Penetration Testing Tools

Metasploit

Part 1 (Introduction to Metasploit)

Metasploit is the most popular exploitation framework, and it has two main versions:

- **Metasploit Pro: The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).**
- **Metasploit Framework: The open-source version that works from the command line. This room will focus on this version, installed on the AttackBox and most commonly used penetration testing Linux distributions.**

The main components of the Metasploit Framework can be summarized as follows;

- **msfconsole: The main command-line interface.**
- **Modules: supporting modules such as exploits, scanners, payloads, etc.**
- **Tools: Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern_create and pattern_offset.**

Part 2 (Main Components of Metasploit)

Metasploit can be open from the terminal using the *msfconsole* command. This will b e your main interface to interact with the different modules which Metasploit consists of. These modules are small components which each are built for a specific task.

Before moving on it is important to understand the following three concepts:

- **Exploit: A piece of code that uses a vulnerability present on the target system.**
- **Vulnerability: A design, coding, or logic flaw affecting the target system. The exploitation of a vulnerability can result in disclosing confidential information or allowing the attacker to execute code on the target system.**
- **Payload: An exploit will take advantage of a vulnerability. However, if we want the exploit to have the result we want (gaining access to the target system, read confidential information, etc.), we need to use a payload. Payloads are the code that will run on the target system**

Let's briefly convert the different modules of Metasploit:

Auxiliary: Any supporting module, such as scanners, crawlers and fuzzers, can be found here.

Encoders: Encoders will allow you to encode the exploit and payload in the hope that a signature-based antivirus solution may miss them.

Evasion: While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

Exploits: Exploits, neatly organized by target system.

NOPs: NOPs (No OPeration) do nothing, literally. They are represented in the Intel x86 CPU family they are represented with 0x90, following which the CPU will do nothing for one cycle. They are often used as a buffer to achieve consistent payload sizes.

Payloads: Payloads are codes that will run on the target system. Example payloads could be: getting a shell, load malware, or opening a backdoor.

You will see three different directories under payloads: singles, stagers and stages.

- **Singles: Self-contained payloads (add user, launch notepad.exe, etc.) that do not need to download an additional component to run.**
- **Stagers: Responsible for setting up a connection channel between Metasploit and the target system. Useful when working with staged payloads. "Staged payloads" will first upload a stager on the target system then download the rest of the payload (stage). This provides some advantages as the initial size of the payload will be relatively small.**
- **Stages: Downloaded by the stager. This will allow you to use larger sized payloads.**

Post: Post modules will be useful on the final stage of the penetration testing process listed above, post-exploitation.

Questions????

What is the name of the code taking advantage of a flaw on the target system?

***Answer*: Exploit**

What is the name of the code that runs on the target system to achieve the attacker's goal?

***Answer*: Payload**

What are self-contained payloads called?

***Answer*: Singles**

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

***Answer:* singles**

Part 3 (Msfconsole)

As mentioned earlier, you can launch Metasploit with the *msfconsole* command. Many of the regular command line commands that you know will work in the metasploit console. Examples of this are ls, ping, clear, history and much more. It is important to realize however that some features won't work, such as output redirection. It does however feature tab completion!

Msfconsole is managed by context. If you a parameter setting, and afterwards change module, you will lose your settings! This is unless you specific the variable as a global type.

You select a module by giving the *use* command, followed by the name of the module. You can afterwards see the available options in the context by writing *show options*. It also shows the variables we can or are required to set.

The *show* command can be used followed by the module type (auxiliary, payload, exploit) to list available modules. If used from the msfconsole prompt, the show command will list all modules.

Further information on any module can be obtained by typing the *info* command within its context.

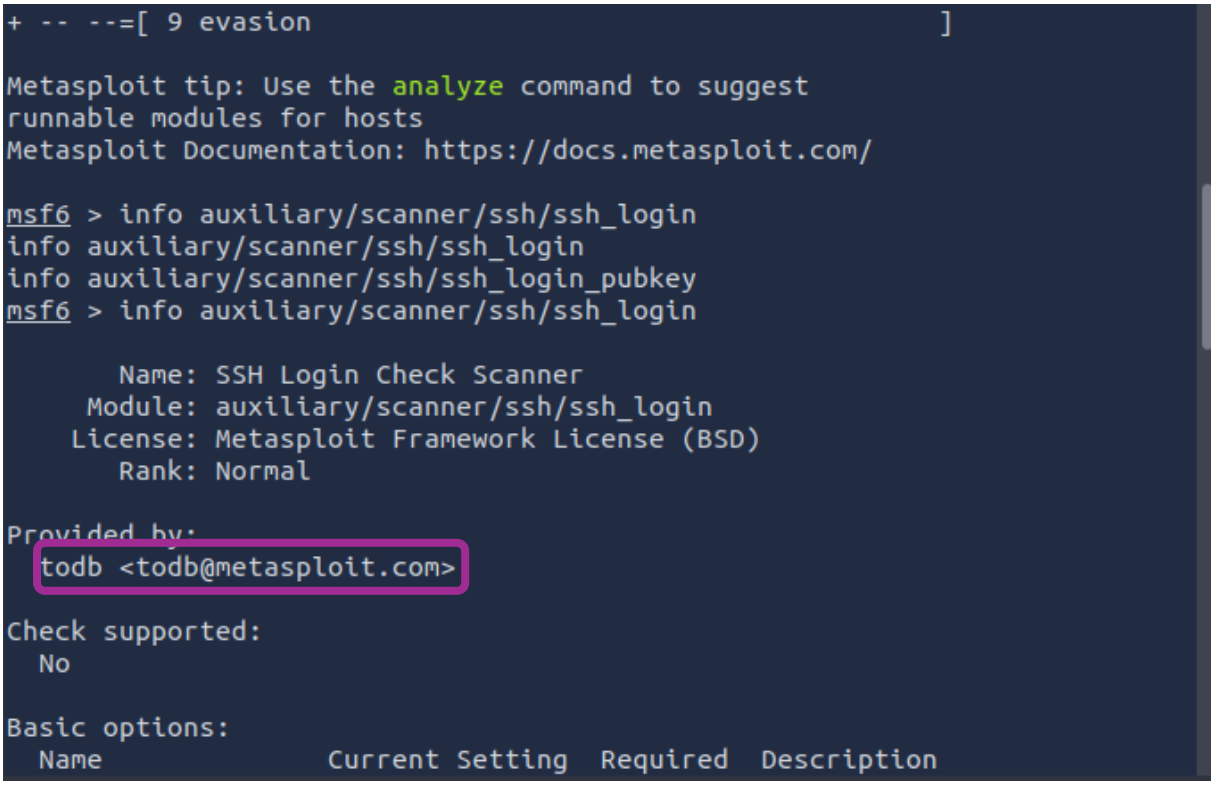
The *search* command is one of the most useful commands available. It will search the Metasploit Framework database for modules relevant to the search query. You can search on both exploit name, CVE numbers and/or target system. An important thing to note is that the search results show a number at the beginning of each result line. This number can be used to to activate a module. You can therefore use *use 0*, instead of *use auxiliary/admin/smb/ms17_010_command* (if this is the first result of your search).

Questions????

How would you search for a module related to Apache?

***Answer*: search apache**

Who provided the auxiliary/scanner/ssh/ssh_login module?



Part 4 (Working with modules)

After using the use command to select a module name, you need to set its parameters. Although many parameters are shared by different modules, additional or different parameters may need to be set. You can list the parameters by entering show options.

You set a parameter by entering set PARAMETER_NAME VALUE. It is important to note that some parameters have default values (make sure these fit your case), and others might be required for the tools to run. You can see this in the show options menu under the "required" column. Once you have set a parameter, you can use the show options command to check the value was set correctly.

Parameters you will often use are:

- **RHOSTS: “Remote host”, the IP address of the target system. A single IP address or a network range can be set. You can also use a file where targets are listed, one target per line using file:/path/of/the/target_file.txt.**
- **RPORT: “Remote port”, the port on the target system the vulnerable application is running on.**
- **PAYLOAD: The payload you will use with the exploit.**
- **LHOST: “Localhost”, the attacking machine (your AttackBox or Kali Linux) IP address.**
- **LPORT: “Local port”, the port you will use for the reverse shell to connect back to. This is a port on your attacking machine.**
- **SESSION: Each connection established to the target system using Metasploit will have a session ID. You will use this with post-exploitation modules that will connect to the target system using an existing connection.**

You can override any set parameter using the set command again with a different value. You can also clear any parameter value using the unset command or clear all set parameters with the unset all command.

The setg command is used to set global values which are used for all modules. When you switch module you will still have the value set. You can clear any value set with setg using unsetg.

Once all module parameters are set, you can launch the module using the exploit command. Metasploit also supports the run command, which is an alias created for the exploit command.

Some modules support the check option. This will check if the target system is vulnerable without exploiting it.

Once a vulnerability has been successfully exploited, a session will be created. This is the communication channel established between the target system and Metasploit.

You can use the background command to background the session prompt and go back to the msfconsole prompt. Alternatively, CTRL+Z can be used to background sessions.

Questions????

How would you set the LPORT value to 6666?

***Answer*: SET LPORT 6666**

Hydra

Part 1 (Hydra Introduction)

Hydra, a potent online password-cracking tool, operates as a swift system login hacking program by employing brute force techniques. In essence, it automates the arduous task of manually guessing passwords for various authentication services like SSH, FTP, and web applications. Hydra accelerates this process by systematically running through a password list to pinpoint the correct password.

With an extensive range of supported protocols, including but not limited to FTP, HTTP, SMTP, and SSH, Hydra stands as a versatile tool for penetrating a myriad of systems. Its capabilities extend to deciphering passwords for services like SNMP, Oracle, MySQL, and even popular communication platforms such as IRC and XMPP.

This underscores the critical need for robust passwords, as Hydra can swiftly crack weak passwords lacking complexity, such as those under eight characters or devoid of special characters. The ubiquity of default credentials like 'admin:password' in devices such as CCTV cameras and web frameworks further emphasizes the necessity of promptly altering default login information. As a cautionary measure, users are urged to adopt secure, unique passwords to fortify their digital defenses against potential brute force attacks.

Part2(Using Hydra)

Hydra, a robust password-cracking tool, empowers users with formidable capabilities, the utilization of which hinges upon the specific service or protocol under attack. The flexibility of Hydra is exemplified through commands tailored for distinct scenarios, such as FTP, SSH, and web form assaults.

For FTP, a command example reveals the simplicity of the syntax:

hydra -l user -P passlist.txt ftp://MACHINE_IP.

Here,

the -l flag designates the username (user),

-P denotes the password list (passlist.txt),

and the FTP service on the specified machine is targeted.

When dealing with SSH, the command structure adapts to the particulars of the scenario:

hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh.

Noteworthy options include -l for specifying the SSH username, -P for indicating the path to the password list, and -t to set the number of concurrent threads.

Web form attacks via Hydra involve intricate commands. For instance, to brute force a POST login form, the command is:

sudo hydra <username> <wordlist> MACHINE_IP http-post-form <path>:<login_credentials>:<invalid_response>.

Here, the -l flag designates the web form username, -P indicates the password list, and http-post-form specifies the form type as POST. The command includes specifics like the login page URL, the login credentials format, and the server's response when login fails.

A concrete example further illustrates Hydra's potency:

hydra -l <username> -P <wordlist> MACHINE_IP http-post-form /:username=^USER^&password=^PASS^:F=incorrect-V.

In this command, the login page is denoted by "/", the username and password fields are defined, and the server's response to failed logins is specified as "F=incorrect."

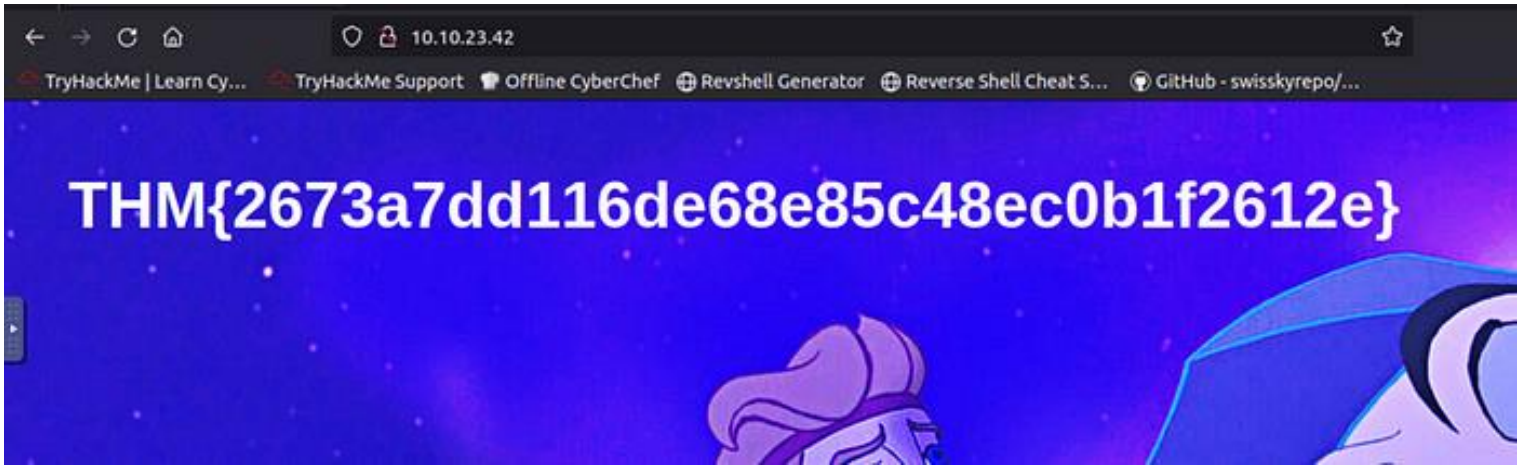
Armed with this knowledge, users gain the prowess to wield Hydra effectively, be it for FTP, SSH, or web form attacks. This tool serves as a double-edged sword, emphasizing the importance of robust security measures to thwart potential brute force endeavors.

Questions????

Use Hydra to bruteforce molly's web password. What is flag 1?

```
root@ip-10-10-173-166:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.23.42 http-post-form "/login:username=^USER^&password=^PASS^:Your
username or password is incorrect."
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-02-26 03:29:58
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hyd
ra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://10.10.23.42:80//login:username=^USER^&password=^PASS^:Your username or password is incorrect.
[80][http-post-form] host: 10.10.23.42   login: molly   password: sunshine
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2024-02-26 03:30:14
root@ip-10-10-173-166:~#
```



Use Hydra to bruteforce molly's SSH password. What is flag 2?

```
root@ip-10-10-173-166:~# ssh molly@10.10.23.42
The authenticity of host '10.10.23.42 (10.10.23.42)' can't be established.
ECDSA key fingerprint is SHA256:9Kd5Bknzh2hC/sNQnmmIvOPjCgQaFgESrkdvdmyyIAM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.23.42' (ECDSA) to the list of known hosts.
molly@10.10.23.42's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-23-42:~$ ls
flag2.txt
molly@ip-10-10-23-42:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-23-42:~$
```

Nmap

Part 2 Introduction

When it comes to hacking, knowledge is power. The more knowledge you have about a target system or network, the more options you have available. This makes it imperative that proper enumeration is carried out before any exploitation attempts are made.

Say we have been given an IP (or multiple IP addresses) to perform a security audit on. Before we do anything else, we need to get an idea of the "landscape" we are attacking. What this means is that we need to establish which services are running on the targets. For example, perhaps one of them is running a webserver, and another is acting as a Windows Active Directory Domain Controller. The first stage in establishing this "map" of the landscape is something called port scanning. When a computer runs a network service, it opens a networking construct called a "port" to receive the connection.

Questions????

What networking constructs are used to direct traffic to the right application on a server?

Ports

How many of these are available on any network-enabled computer?

65535

[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024

Part 3 Nmap Switches

Nmap can be accessed by typing *nmap* into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do different things) we will be covering below.

Questions????

What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS

Which switch would you use for a "UDP scan"?

-sU

If you wanted to detect which operating system the target is running on, which switch would you use?

-O

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?
(Note: it's highly advisable to always use at least this option)

-vv

What switch would you use to save the nmap results in three major formats?

-oA

What switch would you use to save the nmap results in a “normal” format?

-oN

A very useful output format: how would you save results in a “grepable” format?

-oG

How would you activate this setting?

-A

How would you set the timing template to level 5?

-T5

How would you tell nmap to only scan port 80?

-p 80

How would you tell nmap to scan ports 1000–1500?

-p 1000–1500

How would you tell nmap to scan all ports?

-p-

How would you activate a script from the nmap scripting library (lots more on this later!)?

— script

How would you activate all of the scripts in the “vuln” category?

— script=vuln

Part 4 Scan Types Overview

When port scanning with Nmap, there are three basic scan types. These are:

- **TCP Connect Scans (-sT)**
- **SYN "Half-open" Scans (-sS)**
- **UDP Scans (-sU)**

Additionally there are several less common port scan types, some of which we will also cover (albeit in less detail). These are:

- **TCP Null Scans (-sN)**
- **TCP FIN Scans (-sF)**
- **TCP Xmas Scans (-sX)**

Most of these (with the exception of UDP scans) are used for very similar purposes, however, the way that they work differs between each scan. This means that, whilst one of the first three scans are likely to be your go-to in most situations, it's worth bearing in mind that other scan types exist.

In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Part 5 Scan Types TCP Connect Scans

To understand TCP Connect scans (-sT), it's important that you're comfortable with the *TCP three-way handshake*. If this term is new to you then completing Introductory Networking before continuing would be advisable.

As a brief recap, the three-way handshake consists of three stages. First the connecting terminal (our attacking machine, in this instance) sends a TCP request to the target server with the SYN flag set. The server then acknowledges this packet with a TCP response containing the SYN flag,

as well as the ACK flag. Finally, our terminal completes the handshake by sending a TCP request with the ACK flag set.

Questions????

Which RFC defines the appropriate behaviour for the TCP protocol?

RFC 793

If a port is closed, which flag should the server send back to indicate this?

RST

Part 6 Scan Types SYN Scans

As with TCP scans, SYN scans (-sS) are used to scan the TCP port-range of a target or targets; however, the two scan types work slightly differently. SYN scans are sometimes referred to as "Half-open" scans, or "Stealth" scans.

Where TCP scans perform a full three-way handshake with the target, SYN scans sends back a RST TCP packet after receiving a SYN/ACK from the server (this prevents the server from repeatedly trying to make the request).

Questions????

There are two other names for a SYN scan, what are they?

Half-Open, Stealth

Can Nmap use a SYN scan without Sudo permissions (Y/N)?

N

Part 7 Scan Types UDP Scans

Unlike TCP, UDP connections are *stateless*. This means that, rather than initiating a connection with a back-and-forth "handshake", UDP connections rely on sending packets to a target port and essentially hoping that they make it. This makes UDP superb for connections which rely on speed over quality (e.g. video sharing), but the lack of acknowledgement makes UDP significantly more difficult (and much slower) to scan. The switch for an Nmap UDP scan is (-sU)

Questions????

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

open|filtered

When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?

ICMP

Part 8 NULL, FIN and Xmas

NULL, FIN and Xmas TCP port scans are less commonly used than any of the others we've covered already, so we will not go into a huge amount of depth here. All three are interlinked and are used primarily as they tend to be even stealthier, relatively speaking, than a SYN "stealth" scan

Questions????

Which of the three shown scan types uses the URG flag?

xmas

Why are NULL, FIN and Xmas scans generally used?

Firewall Evasion

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Microsoft Windows

Part 9 Scan Types ICMP Network Scanning

On first connection to a target network in a black box assignment, our first objective is to obtain a "map" of the network structure — or, in other words, we want to see which IP addresses contain active hosts, and which do not.

One way to do this is by using Nmap to perform a so called "ping sweep". This is exactly as the name suggests: Nmap sends an ICMP packet to each possible IP address for the specified network. When it receives a response, it marks the IP address that responded as being alive. For reasons we'll see in a later task, this is not always accurate; however, it can provide something of a baseline and thus is worth covering.

Questions????

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

nmap -sn 172.16.0.0/16

Part 10 NSE Scripts Overview

The Nmap Scripting Engine (NSE) is an incredibly powerful addition to Nmap, extending its functionality quite considerably. NSE Scripts are written in the *Lua* programming language, and can be used to do a variety of things: from scanning for vulnerabilities, to automating

exploits for them. The NSE is particularly useful for reconnaisance, however, it is well worth bearing in mind how extensive the script library is.

There are many categories available. Some useful categories include:

- **safe:- Won't affect the target**
- **intrusive:- Not safe: likely to affect the target**
- **vuln:- Scan for vulnerabilities**
- **exploit:- Attempt to exploit a vulnerability**
- **auth:- Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)**
- **brute:- Attempt to bruteforce credentials for running services**
- **discovery:- Attempt to query running services for further information about the network (e.g. query an SNMP server).**

Questions????

What language are NSE scripts written in?

LUA

Which category of scripts would be a very bad idea to run in a production environment?

Intrusive

Part 11 NSE Scripts Working with the NSE

Questions????

What optional argument can the ftp-anon.nse script take?

Maxlist

Part 12 NSE Scripts Searching for Scripts

Ok, so we know how to use the scripts in Nmap, but we don't yet know how to *find* these scripts.

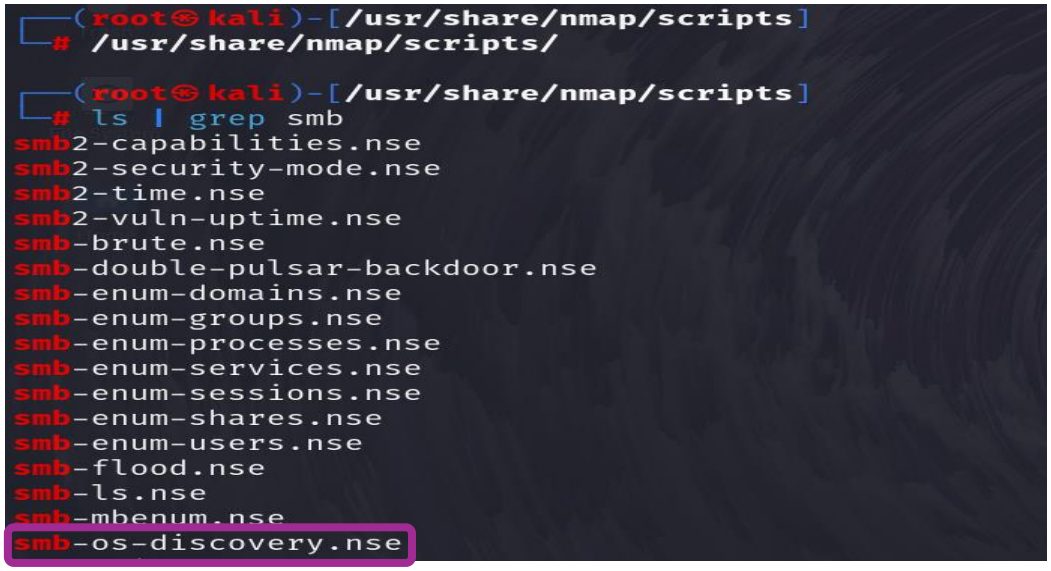
We have two options for this, which should ideally be used in conjunction with each other. The first is the page on the Nmap website (mentioned in the previous task) which contains a list of all official scripts. The second is the local storage on your attacking machine. Nmap stores its scripts on Linux at /usr/share/nmap/scripts. All of the NSE scripts are stored in this directory by default -- this is where Nmap looks for scripts when you specify them.

There are two ways to search for installed scripts. One is by using the /usr/share/nmap/scripts/script.db file. Despite the extension, this isn't actually a database so much as a formatted text file containing filenames and categories for each available script.

The second way to search for scripts is quite simply to use the ls command. For example, we could get the same results as in the previous screenshot by using ls -l /usr/share/nmap/scripts/*ftp*

Questions????

Search for "smb" scripts in the /usr/share/nmap/scripts/ directory using either of the demonstrated methods.
What is the filename of the script which determines the underlying OS of the SMB server?



Read through this script. What does it depend on?

```
--
--@xmloutput
-- <elem key="os">Windows Server (R) 2008 Standard 6001 Service Pack 1</elem>
-- <elem key="cpe">cpe:/o:microsoft:windows_2008::sp1</elem>
-- <elem key="lanmanager">Windows Server (R) 2008 Standard 6.0</elem>
-- <elem key="domain">LAB</elem>
-- <elem key="server">SQL2008</elem>
-- <elem key="date">2011-04-20T13:34:06-05:00</elem>
-- <elem key="fqdn">Sql2008.lab.test.local</elem>
-- <elem key="domain_dns">lab.test.local</elem>
-- <elem key="forest_dns">test.local</elem>

author = "Ron Bowes"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
dependencies = {"smb-brute"}
```

Part 13 Firewall Evasion

We have already seen some techniques for bypassing firewalls (think stealth scans, along with NULL, FIN and Xmas scans); however, there is another very common firewall configuration which it's imperative we know how to bypass.

Your typical Windows host will, with its default firewall, block all ICMP packets. This presents a problem: not only do we often use *ping* to manually establish the activity of a target, Nmap does the same thing by default. This means that Nmap will register a host with this firewall configuration as dead and not bother scanning it at all.

Questions????

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

Icmp

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

data-length

Part 14 Practical

Questions????

Does the target (MACHINE_IP)respond to ICMP (ping) requests (Y/N)?

N

Perform an Xmas scan on the first 999 ports of the target — how many ports are shown to be open or filtered?

```
┌──(root㉿kali)-[/]
└─# nmap -p1-999 -sX 10.10.113.1 -vv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-15 15:33 EDT
Initiating Ping Scan at 15:33
Scanning 10.10.113.1 [4 ports]
Completed Ping Scan at 15:33, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:33
Completed Parallel DNS resolution of 1 host. at 15:33, 6.54s elapsed
Initiating XMAS Scan at 15:33
Scanning 10.10.113.1 [999 ports]
Completed XMAS Scan at 15:33, 4.95s elapsed (999 total ports)
Nmap scan report for 10.10.113.1
Host is up, received reset ttl 64 (0.0083s latency).
Scanned at 2024-06-15 15:33:27 EDT for 5s
All 999 scanned ports on 10.10.113.1 are in ignored states.
Not shown: 999 open|filtered tcp ports (no-response)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.72 seconds
           Raw packets sent: 2005 (80.192KB) | Rcvd: 4 (160B)
```

Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Y

Perform a TCP SYN scan on the first 5000 ports of the target — how many ports are shown to be open?

5

Nessus

Part 1 Introduction

This exercise will be based on the TryHackMe red primer series room: Nessus

What is Nessus? Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network

---

Part 3 Navigation and Scan Types!

Questions????

As we log into Nessus, we are greeted with a button to launch a scan, what is the name of this button?

new scan

Nessus allows us to create custom templates that can be used during the scan selection as additional scan types, what is the name of the menu where we can set these?

policies

Nessus also allows us to change plugin properties such as hiding them or changing their severity, what menu allows us to change this?

plugin rules

Nessus can also be run through multiple ‘Scanners’ where multiple installations can work together to complete scans or run scans on remote networks, what menu allows us to see all of these installations?

scanners

Let’s move onto the scan types, what scan allows us to see simply what hosts are ‘alive’?

host discovery

One of the most useful scan types, which is considered to be ‘suitable for any host’?

basic network scan

Following a few basic scans, it’s often useful to run a scan wherein the scanner can authenticate to systems and evaluate their patching level. What scan allows you to do this?

credential patch audit

When performing Web App tests it’s often useful to run which scan? This can be incredibly useful when also using nitko, zap, and burp to gain a full picture of an application.

web applications tests

Part 4 Scanning!

Questions????

Create a new 'Basic Network Scan' targeting the deployed VM. What option can we set under 'BASIC' to set a time for this scan to run? This can be very useful when network congestion is an issue.

schedule

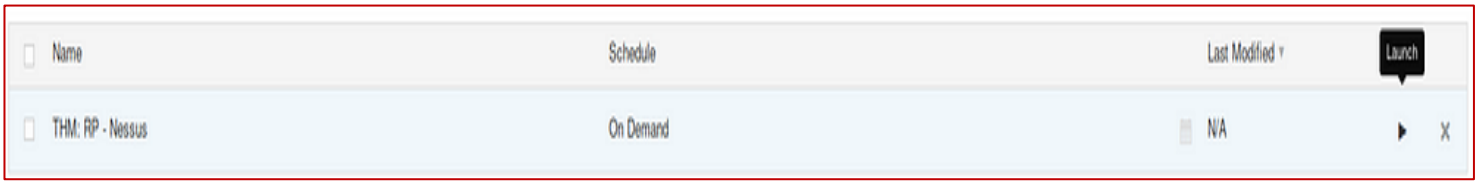
Under discovery set the scan to cover ports 1–65535. What is this type called?

port scan (all ports)

What scan type can we change to under 'ADVANCED' for this lower bandwidth connection?

scan low bandwidth links

With these options set (other than the time to run) save and launch the scan.



After the scan completes, which 'Vulnerability' can we view the details of to see the open ports on this host?

nessus syn scanner

There seems to be a chat server running on this machine, what port is it on?

6667

Looks like we have a medium level vulnerability relating to SSH, what is this vulnerability named?

ssh weak algorithms supported

What web server type and version is reported by Nessus?

apache/2.4.99

Part 5 Scanning a Web Application

Questions????

What is the plugin id of the plugin that determines the HTTP server type and version?

10107

What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php

What is the file extension of the config backup?

.bak

Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/

What vulnerability is this application susceptible to that is associated with X-Frame-Options?

clickjacking

What version of php is the server using?

5.5.9-1ubuntu4.26