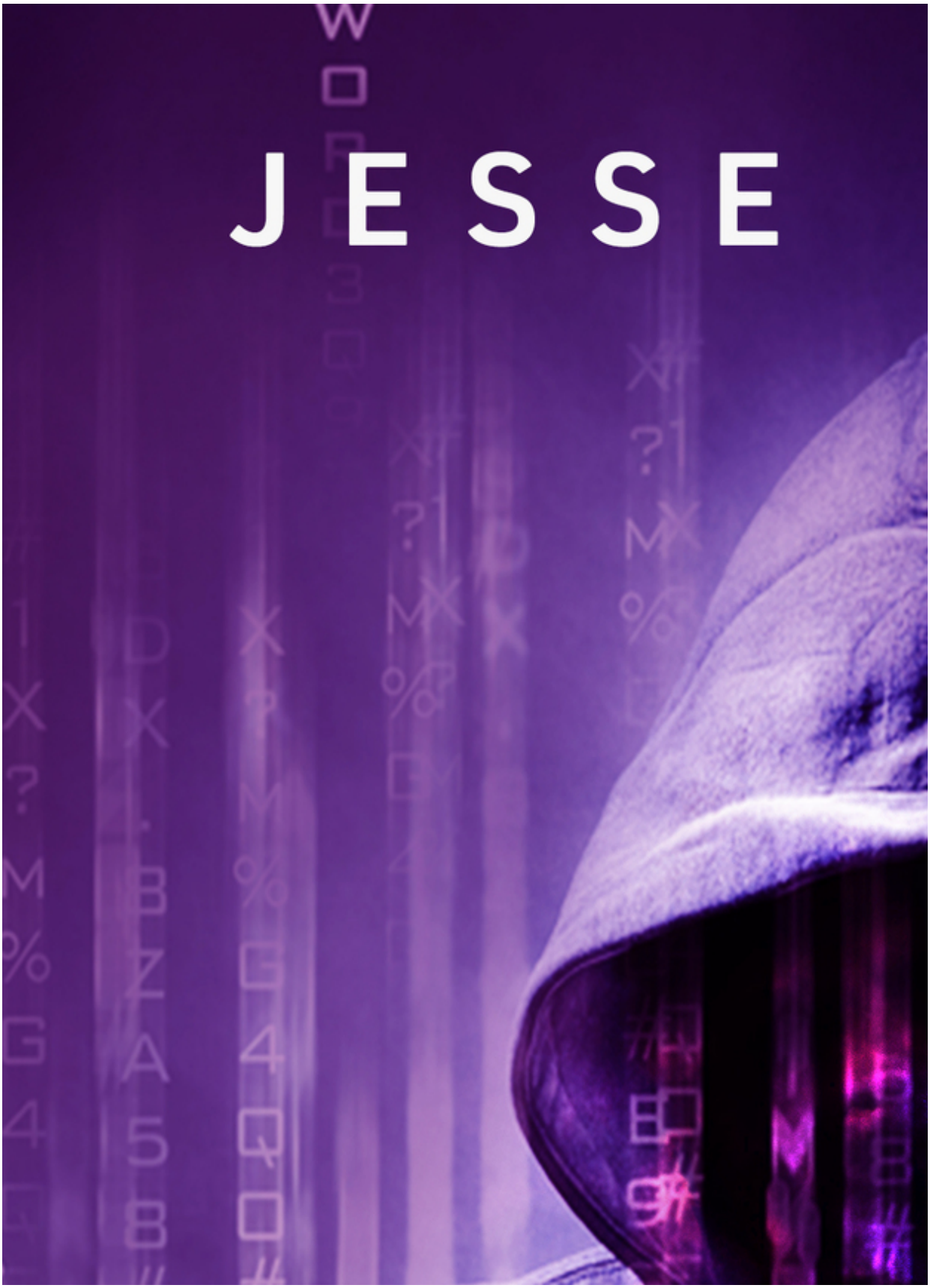
JESSE CANNON

ETHICAL HACKING


JESSE

Ethical Hacking

A Complete Guide With Tips and Tricks. Find out about penetration testing and cyber security by studying advanced ethical hacking methods and techniques (2022 for Beginners)

Jesse Cannon

Table of Contents

Table of Contents

RECONOISSANCE FOR HACKERS

Chapter One: How to Discover a Host

Chapter Two: Active scanning

Chapter Three: Domain name

Chapter Four: Dnsenum tool

Chapter Five: Notion of ports

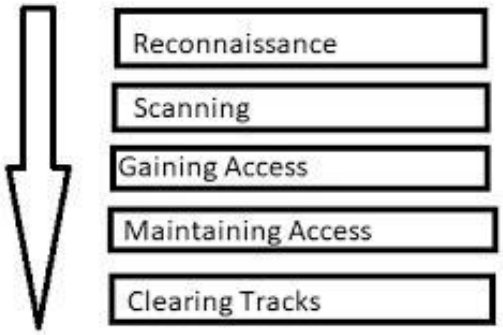
Chapter Six: Recognizing the operating system

Chapter Seven: NMAP tool

Chapter Eight: Maltego Configuration

RECONOISSANCE FOR HACKERS

Introduction



The preceding module of this book presented Kali Linux, as well as its features and installation instructions. This session examines the most crucial skill that all hackers and pen testers must master: reconnaissance. We will discuss many tools and present numerous examples to help you grasp the substance of the topic.

What equipment do you require?

There are hundreds of tools designed specifically for reconnaissance since it is an integral part of the hacking process. This book concentrates on two tools, Nmap and Dmitri, for a basic level introduction. If you are using Windows or a Mac, we recommend installing both programs before beginning this book. If you already have Kali installed, you may quickly access them through the search menu. As previously said, tools are merely there to automate and stream your hacking operation. The approach you use to locate a backdoor to the host is always the secret of hacking. Don't be distracted by tool features and lose sight of your core goal.

How should you handle this module?

Comprehending the strategy to information collection is more important than understanding the tools or commands utilized. Every target necessitates a different method, and as a hacker, you must exclusively build a technique to attack a target based on the survey's findings. As a consequence, make sure that you thoroughly examine the log files and conclusions.

Note & Disclaimer: This book has been meticulously written. We do not want you to use this book for illicit reasons. Anything the reader does with the book's material is not our responsibility.

Chapter One: How to Discover a Host

This chapter serves as a precondition for pen-testers looking to enhance their reconnaissance abilities. We will talk about Networking issues to help you see things in a different light. Continue reading!

```
#nmap -sn --traceroute google.com microsoft.com
   Nmap scan report for google.com (216.58.193.46)
   Host is up (0.16s latency).
   Other addresses for google.com (not scanned):
   2607:f8b0:4012:805::200e
   rDNS record for 216.58.193.46: qro01s13-in-f14.1e100.net

   TRACEROUTE (using port 443/tcp)
   HOP RTT       ADDRESS
   1   1.28 ms   192.168.0.1
   2   ...
   3   158.85 ms 10.165.1.9
   4   ... 5
   6   165.50 ms 10.244.158.13
   7   171.18 ms 10.162.0.254
   8   175.33 ms 200.79.231.81.static.cableonline.com.mx
       (200.79.231.81)
   9   183.16 ms 10.19.132.97
   10  218.60 ms 72.14.203.70
```

How to Discover a Host?

The discovery host detects which hosts are active and then retrieves information about the available hosts. Users might find the host via active scanning or passive surveillance. This section will go through these two ways in-depth, along with step-by-step directions.

Confirm network coverage.

Before identifying a target, it is often required to determine the target's likely range. This range might be a particular host, an address range, or even an entire subnet. It typically depends on the range.

The IP address regulations should and will be followed. The target's possible range might be drawn according to the IP regulations. As a result, a penetration tester must understand the IP addressing rules that have been developed.

1. IP address policies

IP addresses (Internet Protocol Addresses) are Internet identification addresses used to identify devices, networks, and even more extensive networks. Your mobile phone, for example, has an IP address, while your modem has a different and distinct IP address. It is a 32-bit binary number divided into four 8-bit binary numbers using dot notation, totaling four bytes. It is critical to realize that IP addresses are often stated in "dotted decimal notation" in the form a.b.c.d. a, b, c, and d are decimal numbers ranging from 0 to 255. The dotted decimal IP address 192.168.12.143, for example, is a 32-bit binary integer.

Workout: Using an internet conversion calculator, determine the binary notation of the above IP numbers.

The IP address is made up of two parts: the network address and the host address. The network address identifies which network on the Internet it belongs to, and the host address identifies which host inside that network. If you look closely, you can see that they are in a master-slave relationship. IP addresses are classified into three types based on their network and host numbers: type A (1.0.0.0 126.0.0.0), type B (128.1.0.0 191.255.0.0), and type C (1.0.0.0 126.0.0.0). (192.0.1.0 223.255.255.0). There are also unique Address classes known as D and E. Furthermore, all 0s and 1s are reserved.

Each group of IP addresses is introduced as follows:

' '

Class A: This set's address range is 1.0.0.0-126.0.0.0, and the subnet mask is 255.0.0.0. The first byte of this address is the network number, while the subsequent three bytes are the host number. Because the front notation of this kind of IP address is 0 and the network number of the address varies from 1 to 126, it is obvious that the network number of the address ranges from 1 to 126.

Class B : addresses range from 128.1.0.0 to 191.255.0.0, with 255.255.0.0 as the specified subnet mask. The first two bytes of this address are the network number, while the final two bytes are the host number. Because the front of this sort of IP address is 10, the network number spans from 128 to 191.

Class C: addresses are 192.0.1.0 to 223.255.255.0, with a subnet mask of 255.255.255.0. The first three bytes of this address are the network number,

while the final byte is the host number. Because the front of this sort of IP address is 110, the network number is between 129 and 223.

It is a multicast address of class D. Because the front of this IP address is 1110, the network number is between 224 and 239. This is often used for multicast users. If you're not already aware, a multicast address is an address that permits a source device to deliver packets to a group of devices. Devices

A multicast group IP address will be allocated to each member of the multicast group, and the multicast address range is 224.0.0.0 to 239.255.255.255.

Because the multicast address represents a group of devices, it can only be used as the packet's destination address. Unicast addresses are always used as the source address. The multicast MAC address begins with the hexadecimal value 01-00-5E, and the subsequent six hexadecimal digits are translated from the IP multicast group address's last 23 digits.

Addresses in Class E are reserved. Because the front of this IP address is 1111, the network number spans from 240 to 255.

There is a unique type of IP address known as a broadcast address among IP addresses. The broadcast address is used to convey data to all hosts on the network at the same time. In a TCP/IP network, the IP address with all 1s in the host identification segment is a broadcast address, and broadcast packets are sent to all machines engaged in the host identification segment.

The subnet mask is used to partition IP addresses into network segments. For example, if the subnet mask corresponding to the IP address 192.168.1.100/24 is 255.255.255.0, the network segment is 192.168.1.0-255, indicating that the network segment has 256 hosts.

When a user finds a host, the mask format allows him to select the network range. For example, among them, for input.

For ease of usage, the CIDR format is often used to define the whole subnet. The CIDR format, for example, is made up of two parts: the network address and the subnet mask, separated by a slash (/).

If the user is unsure about the subnet mask format corresponding to an IP range, the Net-mask utility may help. This program can convert between IP ranges, subnet masks, CIDR, Cisco, and other formats, and between dotted decimal, hexadeci

2. Identify the network structure

Based on the routing information, the user may identify the upper-level network range. By establishing the network topology during a penetration test, you may tell whether the target is a local area or an external network. As a result, penetration testing tools may be chosen in a more focused manner, increasing the efficacy of penetration testing. The following section will explain how to use the Trace-route tool to gather routing records from the target host to establish the network topology.

The syntax for implementing route tracking using this tool is as follows:

[Target] traceroute

In this case, the target is the address of the host network about which we are looking for information.

The scenario of application:

Trace the path of the target host 72.132.234.64 using the Trace-route tool to learn its network topology.

The following is the execution command:

traceroute 72.132.234.64 root@exampleserver

This will provide detailed information about that specific host. If you execute this program, a slew of messages will appear on your computer screen. A lot of this data is about the packets and the path they've taken. Advanced security experts examine these packet tokens during an attack scenario to see whether the hacker has left any fingerprints on the system.

There will be an issue with Trace-route operation in the virtual machine's NAT mode. The top-level route information is not visible. Make sure you are aware of this while working.

Chapter Two: Active scanning

In the last chapter, we learned about a few networking principles critical for comprehending the significance of tools such as Nmap. Networking is a broad subject, but as a hacker, we suggest that you have a solid understanding of it by studying numerous networking ideas and protocols.

Active scanning allows the user to detect whether the target host is dynamic or not. Active scanning is accomplished by sending a probe request packet and then waiting for a response from the target host. If the target host answers to the request, it indicates that the host is alive and well. Otherwise, we might assume that the target host is not available.

The section that follows will go through numerous methods for actively scanning the host.

1) Using the Nmap tool

Nmap is a very effective network scanning and sniping tool. This tool serves three primary purposes. The first of the three is to determine whether or not a group of hosts is online.

The second is to scan host ports and snip the network services supplied, while the third is to infer the host's operating system.

The following examples will demonstrate how to use the Nmap tool to determine whether or not the target host is online.

The syntax of N-map is as follows:

nmap -sP [target]

The -sP option in the above syntax indicates doing a Ping scan on the target host. The choice [target] is used to provide the scan's target address. In rare cases, the target may be a hostname, an IP address (including a single address, multiple addresses, or address ranges), or even network segments.

The scenario of application:

Check to see whether the target host, 72.132.234.64, is online. The following is the execution command:

nmap -sP 72.132.234.64 root@exampleserver

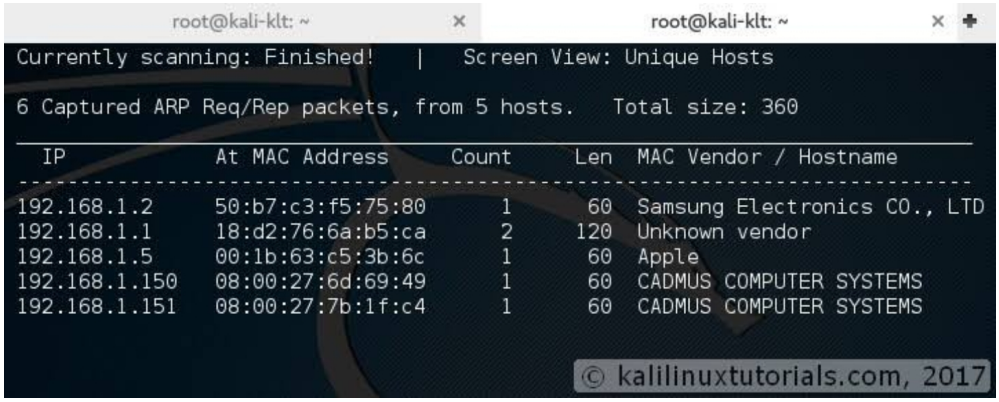
You may also check many hosts at the same time. For your convenience, we've included an illustration of this case below.

Scenario of application

Nmap may be used to determine if the hosts 72.132.234.64, 72.132.234.65, and 72.132.234.66 are up and running.

The command to execute is as follows: root@exampleserver: # nmap -sP 72.132.234.64-66

This result displays the availability of these three servers.



2) Employ the Netdiscover tool.

Netdiscover is a tool for ARP inquiry that works in both active and passive modes. This program may be used to scan IP addresses on the network and check for online hosts.

The part that follows will go through how to utilize the Netdiscover utility to implement ARP active scanning.

The following is the syntax format:

netdiscover -r [restricted]

In the above syntax, the option -r [range] specifies the network range to be scanned. If the user does not designate a target, the target network will be chosen for scanning automatically.

The scenario of application:

Scan online hosts in the 72.132.234.64/94 network sector using the Netdiscover utility.

The following is the execution command:

netdiscover -r 72.132.234.64/94 root@exampleserver

You can determine the currently active host IP address, MAC address, and MAC address by analyzing the collected packets.

Manufacturer in today's LAN The IP column displays the address of the web host. When the scanning is finished, all of the information acquired will be shown. If you pay close attention, you may learn a lot about the host you're attempting to attack. After carefully reviewing the results, hit the Ctrl+C key combination to quit the Netdiscover tool's scanning interface.

Users may also locate as many online hosts as feasible if they do not specify the scan range.

The command to execute is as follows: root@exampleserver: # netdiscover

However, we recommend that you do not do this since it may result in a large number of hosts that are typically not worth your effort to attack. Before attacking the host networks, always do extensive study. If you do not, intrusion detection systems will notice your answer and may ban you for an extended period.

Monitor Discovery Host

Snooping is the process of passively observing data packets in a network rather than actively transmitting data packets to the destination. Some protocols, such as ARP broadcast and DHCP broadcast, will automatically broadcast data packets on a local area network. A broadcast packet is a data package that all LAN users may receive. As a result, by watching these packets, users may discover active hosts on the network. The next part will go through how to find the host via monitoring.

1) ARP tracking

ARP (Address Resolution Mechanism) is a TCP/IP protocol that uses IP addresses to acquire physical addresses. When a host delivers data, it broadcasts an ARP request with the target IP address to all hosts in the network and waits for a response message to discover the target's physical address. As a result, active hosts in the LAN may be detected by using ARP monitoring.

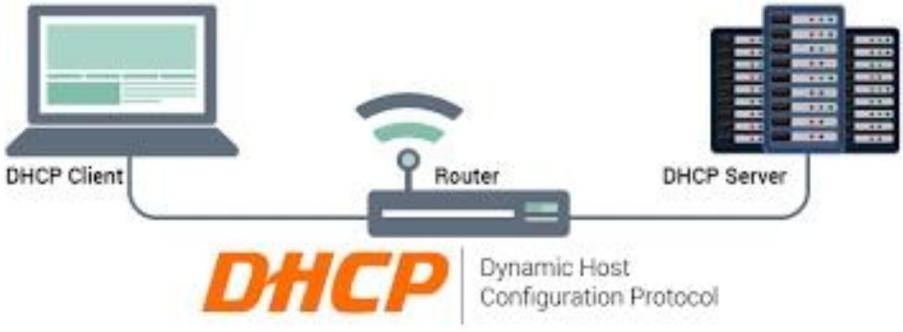
The following section will describe the passive mode implementation of ARP monitoring using the Netdiscover utility to find online hosts.

The syntax structure for Netdiscover's passive scanning tool is as follows:

netdiscover -p

The option -p in the above grammar indicates that passive mode is to be used, which implies that no data packets must be delivered and that just sniffing is permitted.

The scan is being done in passive mode, based on the first line of information output. The second line of data shows the number of snied packets, the number of hosts, and the packet size. The data following line 3 will pertain to the snied packet information. The IP column displays the discovered online hosts. This command in the net find utility may be used to conduct a variety of additional activities. We propose that you try with these instructions to have a better knowledge of the subject.



2)

DHCP eavesdropping

DHCP (Dynamic Host Configuration Protocol, dynamic host configuration protocol) is a network protocol that allows internal networks or network service providers to allocate IP addresses automatically. A broadcast packet is sent when a client wants to get an IP address. The DHCP server that received the request will then give the client an available IP address. As a result, users may utilize DHCP snooping to identify which hosts are up on the network. The following section will explain how to create DHCP snooping using Nmap's broadcast-DHCP-find script to discover hosts.

Nmap's broadcast-DHCP-discover script may be used to transmit a DHCP Discover broadcast packet and effectively show the return packet's unique information. The assignable IP address may be determined by analyzing the information in the answer packet.

This script's syntactic structure for passive scanning is as follows:

Nmap —script broadcast-DHCP-discover root@exampleserver

The —script option in the above syntax specifies that a script will be used for the assault.

In the next chapter, we will begin addressing Domain analysis, which is vital for the information collecting technique. Continue reading!

Chapter Three: Domain name

We examined the processes that may be used to scan a host in the previous chapter. While scanning is thought to be a simple technique, it is frequently not possible these days owing to the intrusion detection systems that are fast being created to identify malicious scanning requests. To address this issue and analyze our target more thoroughly, we must first comprehend the significance of domain analysis. Follow along with this chapter to obtain a clear understanding of it.

What exactly is a domain name?

A domain name is a string of words separated by dots that are often used to denote the name of an Internet computer or computer group. It can determine the computer's electrical location during data transfer. Domain names are often used to identify hosts on the external network. If you wish to execute a penetration test on a host on an external network, you must first analyze the domain name to gather complete information about Different sensitive factors, such as domain name owner information, subdomain name, and server address, may be found. With a handful of examples, this section will explain how to analyze domain name information.

Basic Domain Name Details

When a domain name is registered, basic information such as whether the domain name has been registered or not, the domain name registrar, the domain name owner, and so on are included. You may get basic domain

name information by checking the WHOIS information of the domain name. The following section will explain how to retrieve basic domain name information using WHOIS and other standard tools.

It is often said that domain analysis is the first step that pentesters do before analyzing the target.

1) Make use of WHOIS tools.

The WHOIS tool is used to locate and display user-specific information for a given account (or domain name).

This tool's syntax for querying domain name information is as follows:

[Domain Name] whois

Scenario of application:

To find out more about the domain name wikipedia.com, use the WHOIS tool.

The following is the execution command:

whois wikipedia.com root@exampleserver

After executing the above command into the terminal, you may view the appropriate WHOIS information for the domain name wikipedia.com.

2) Employ the Dmitry tool.

Dmitry is a comprehensive information-gathering tool. Pentesters often use this tool to gather WHOIS host IP and domain name information, subdomains, email addresses included in domain names, and so on.

The syntax format used to obtain WHOIS information using this tool is one of them:

[domain] Dmitry -w

In this case, -w: Execute a WHOIS lookup on the specified domain name. On the other hand, Domain is the host that we are attempting to attack and gather information about.

Scenario of application:

To find out more about the WHOIS information for the domain name wikipedia.com, use the Dmitry tool.

The following is the execution command:

dmitry -w wikipedia.com root@exampleserver

The WHOIS information for the domain name may be obtained by using the above command in the Linux terminal.

～ \s ～

The domain name wikipedia.com will be acquired successfully.

A penetration tester will handle a subdomain as if it were a domain. It generally corresponds to a higher domain in the domain name system hierarchy. For example, www.wikipedia.com and forum.wikipedia.com are two subdomains of wikipedia.com, while forum.wikipedia.com is a subdomain of the top-level Domain wikipedia.com.

Typically, a subdomain name will include the hostname. For example, in the domain name www.wikipedia.com, the top-level domain name is.com, and the first-level domain name is wikipedia.com. The hostname used to identify the server is www. As a result, wikipedia.com's WWW server address is www.wikipedia.com. It is well known that the relevant host may be located by checking up the subdomain name. The process for finding subdomains will be outlined in full below, with examples.

1) Make use of Dmitry's tool.

Find Subdomains

Subdomains may be discovered using the Dmitry tool. However, the program searches for subdomains using the Google search engine. It may be unreliable at times if you visit websites that Google has delisted. As a result, be sure that your Domain is compatible with Google search.

The following is the syntax for using the Dmitry tool to discover a subdomain name:

Dmitry -s -o

The following are the alternatives and meanings in the grammar above: -S: Enables subdomain querying. -O: Specifies the file to which the output result should be saved.

Scenario of application:

To get the subdomain name of the domain name wikipedia.com, use the Dmitry tool.

The following is the execution command:

dmitry -s wikipedia.com root@exampleserver -o domain subdomain

When you run the above command in the Linux terminal, you will notice that all subdomains and related IP addresses of the domain name wikipedia.com are shown. You may precisely attack your target by using their IP addresses and sub-domains.

3) 

Internet search

Users may also use internet query methods to look for subdomains. The most common address for online subdomain name querying is the following website (https://phpinfo). When the user successfully navigates to the URL in the browser, the interface that prompts for the domain name is shown.

In the text box, enter the domain name to be queried. Then, click the "Start" button to locate the appropriate subdomain. For instance, we may discover several subdomain names of the domain name wikipedia.com.

All accessible subdomains for wikipedia.com will be shown immediately.

~

What Comes Next?

You are now well-versed in the procedures for locating subdomains and comprehending the attributes of a specific domain. However, it is crucial to note that administrators and developers often prohibit their information from being viewed by anonymous people (i.e., penetration testers). As a result, it is critical not to depend just on domain analysis.

In the next chapter, we will address this issue by proposing a method for locating servers for your hacking technique. Continue reading!

Chapter Four: Dnsenum tool

Although the domain name is accessible for people to remember, the machines in the network can only communicate via their IP addresses. As a result, you must query the matching host using the domain name. Different hosts are recognized in the domain name server by domain name records such as A records, MX records, and NS records. A record represents a host, an MX record represents a mail server, and an NS record represents a DNS

server. An IP address is included in each domain name record. By identifying the domain name server, the user may discover the IP address associated with the domain name. The procedure for locating the server will be discussed in detail below, along with proper directions for your comprehension. Continue reading!

1) Use the Dnsenum tool.

Dnsenum is a utility for collecting domain name information. It may effectively run reverse searches on a network segment and predict plausible domain names using Google or dictionary files. It may also lookup the host address.

The website's information, domain name server, and mail exchange records

This tool's syntax for collecting domain name information is as follows:

dnsenum -w

The -w option in the above syntax specifies that the WHOIS query is run inside the scope of the network.

Scenario of application:

To enumerate the information of the subdomain name wikipedia.com, use Dnsenum.

The following is the execution command:

dnsenum -w wikipedia.com root@exampleserver

When you enter the preceding code into a terminal, you will see that the IP address of the subdomain www.wikipedia.com has been retrieved.

2) Employ the Nslookup tool.

Nslookup is a Microsoft command utility for discovering and debugging DNS servers. This utility can query DNS records to see whether the domain name resolution is standard. The program may also be used to troubleshoot network faults in the case of a network breakdown. The IP address of the matching server may be retrieved by performing domain name resolution.

The tool's syntactic format is as follows:

domain nslookup

The argument domain is used in the command to provide the domain name to be queried.

Scenario of application:

To resolve the domain name www.wikipedia.com, use Nslookup.

The following is the execution command:

nslookup www.wikipedia.com root@exampleserver

192.123.8.1 Server Address: 192.342.43.2 #53

Non-authoritarian response: Name:www.wikipedia.com 54.123.131.876 is the address.

We can see from the output information that the domain name www.wikipedia.com was successfully resolved. We can see from the findings that the addresses associated with this domain name are 192.123.8.1 and 192.342.43.2.

The default query when using Nslookup to make a domain name inquiry is A record. In the interactive mode, users may also use settype=value to define the value of the domain name record. The supplied domain name record may be A, NS, MX, CNAME, PTR, and so on.

For example, to acquire the NS name server record for the domain name wikipedia.com, use Nslookup as follows:

(1) To access interactive mode, use the Nslookup utility.

The following is the execution command:

nslookup> root@exampleserver

If the command line prompt is presented as >, you have successfully entered the interactive mode of Nslookup.

(2) Select NS record as the query type. The following is the execution command:

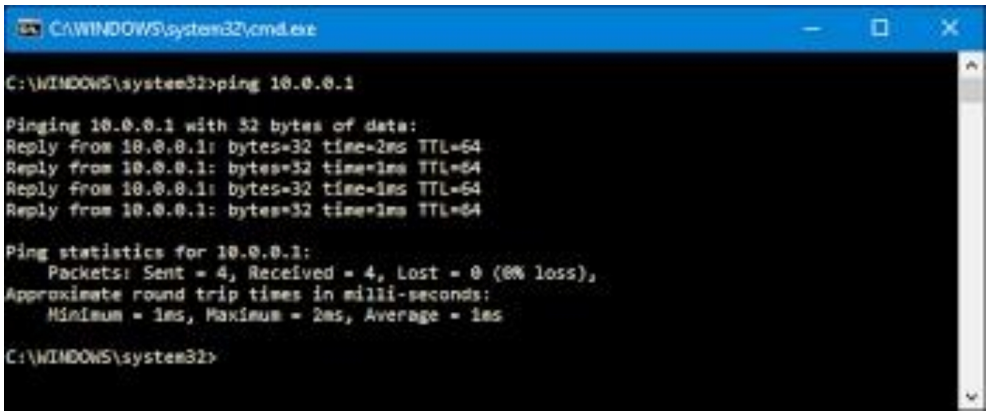
set type to ns

(3) Type in the domain name to be searched. The following is the execution command:

wikipedia.com

192.123.8.1 Server Address: 192.342.43.2 #53 Answer that is not authoritative: Name: www.wikipedia.com Address: 54.123.131.876 = ns7.wikipedia.com ns2.wikipedia.com is the nameserver.

If the user does not want to query other records, he may quit the interactive mode using the exit command. as seen below:

3) 

Use the Ping command to exit root@exampleserver:

The ping command may be used to determine whether or not a network is connected. This may generally assist users in analyzing and judging network faults. You may generally provide multiple IP addresses for a domain name. As a result, when users use various tools to query domain name information, they will get several addresses. The user cannot tell which address the target server is using at this moment. Using the Ping command, the user may detect the IP address presently in use and subsequently find the destination host.

The ping command has the following syntax:

ping -c [number]

[target]

In the above syntax, the option -c specifies the number of Ping packets to be sent, and the argument [target] specifies the address of the target host, which may be a hostname, IP address, or domain name. To halt Ping, the Windows system only transmits and replies to four packets. The ping command is always performed by default on the Linux system, and the user must hit the Ctrl+C key combination to stop it.

Scenario of application:

To determine the IP address of the domain name www.wikipedia.com, use the Ping command and request that just four detection packets be sent.

The following is the execution command:

ping -c 4 www.wikipedia.com root@exampleserver

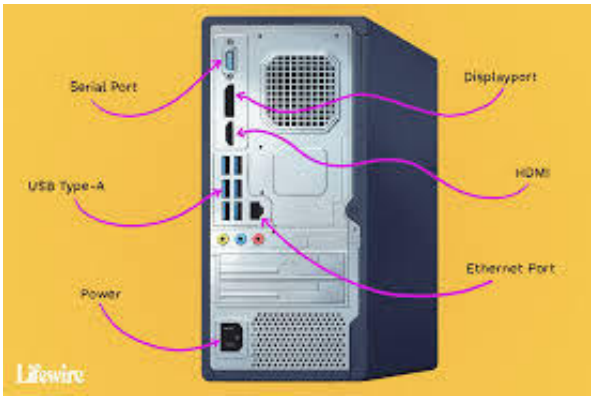
Following the above command's execution, we can observe that the response packet from the target host was successfully received. The IP address issued by the target may be determined from the response packet information.

What comes next?

With a thorough knowledge of the Domain and server analysis, you are now prepared to discuss the significance of port analysis. Nmap, a well-known information collecting tool, is renowned for its superior approach to port analysis. Continue reading to learn how to do port analysis using Nmap.

Chapter Five: Notion of ports

You may find the applications running on the target host by scanning the port. After that, we may gather information on these apps to identify vulnerabilities and effectively execute penetration testing. This section will explain the notion of ports and how to do port scanning.



Ports Introduction

The port is regarded as a crucial concept in computers. Ports have numerous meanings in network technology. The port in question here is not a physical sport but rather a TCP/IP port. In a logical sense, it is a port. TCP and UDP are two of the most extensively used TCP/IP protocols. Because TCP and UDP are distinct protocols, their corresponding port numbers are likewise independent of one another. TCP, for example, has port 235; UDP may also have port 235; the two do not frequently clash.

The following are descriptions of port functionalities and widely used ports:

1) The port's function

Users understand that a host corresponds to an IP address and may offer various services, including Web services and FTP services. Different network services cannot be recognized if there is just one IP address; thus, utilize "IP+port number" to distinguish between them.

2) Port definition

The port number identifies the single process on the host, while the "IP+port number" identifies the only method on the network. During network development, the socket is defined as IP + port number. The port number is represented as a 16-bit binary number with a range of 0 to 65535.

These ports, however, cannot be utilized carelessly, and some may already be occupied. For example, the Web server's port is 80, the FTP service's port is 21, etc. As a result, ports are categorized, and the range of ports that users may use is tightly regulated for pen-testers. Always be well-versed in the ports available to your goal.

3) Classification of ports

Ports may be classified in a variety of ways. Typically, they will be categorized based on whether the server or the client utilizes them.

The server's port number may be separated into two categories: reserved port numbers and registered port numbers, as shown below:

Port number reserved:

This kind of port has a value range of 0 1023. These ports, which are needed by specific applications, cannot be used during user programming. Only apps with superuser privileges may be allocated a reserved port number. The default port of the WWW service, for example, is 80, whereas the default port of the FTP service is 21. Users may, however, define other port numbers for these network services. Some system protocols use a fixed port number that cannot be altered. Port 139, for example, is reserved for communication between NetBIOS and TCP/IP and cannot be modified manually.

A number of the registered port:

This port has a range of 1024 49151, which is the port number range used by the user to write to the server. When server resources do not occupy these ports, the client may pick them dynamically. The client's port number is also known as a temporary port number, and it has a value range of 49152 65535.

Port scan implementation

Port scanning may be applied after the user has a firm grasp of the port idea. The next part will go through how to utilize the Nmap and Dmitry tools to do port scanning.

1) Employ the Nmap tool.

It is common to practice using the Nmap program to do port scanning.

Nmap can detect six port states: open (open), closed (closed), filtered (filtered), unfiltered (unfiltered), and open/filtered (open or filtered) as well as closed/filtered (closed or filtered). If you wish to utilize the Nmap program to do port scanning, you must first understand each port status.

The section that follows will explain the exact significance of these six-port statuses.

Open:

On this port, the program usually receives TCP connections or UDP packets. Security-conscious individuals understand that any open port is an entrance point for an attack. Attackers or intrusion testers aim to find open ports, whereas administrators strive to block them or secure them with firewalls so that legitimate users may use them. Open ports may also be of interest to non-security scanning since they reveal which services are accessible on the network.

Closed: The closed port is also available to Nmap (it receives and reacts to Nmap detection signals), but it is clear that no application is listening to it. They can demonstrate that the host of the IP address is running (host discovery or ping scan), and they can also assist in detecting specific operating systems. Because the blocked ports are still accessible, some of them may be reopened after a period. The system administrator may use a firewall to restrict such ports. They will be shown as filtered in this manner.

Filtered (reduced):

Nmap cannot identify whether a port is open because packet filtering stops probing packets from reaching it. Filtering may be provided by professional firewall equipment, router rules, or host-based software firewalls. They sometimes react to ICMP error signals, such as type 3 code 13 (target cannot be reached: contact is disallowed by the administrator), but more often than not, the filter just discards the probe frame without responding. Nmap will attempt multiple times to determine if the probe packet was dropped due to network congestion. The scanning pace will be significantly slowed as a result of this.

Unfiltered: The unfiltered state indicates that the port is reachable, but Nmap cannot tell whether it is open or closed. The user will only classify the port into this state through the mapping firewall rule set's ACK scan.

Scanning unfiltered ports with other scanning methods (such as window scanning, SYN scanning, or FIN scanning) may assist in identifying whether the port is open.

Open/filtered (open or filtered): Nmap splits a port into this state when it is difficult to identify whether it is available or filtered. When the open port does not react, this is the situation. The absence of response may also indicate that the message filter disregarded the probe message and subsequent response messages. As a result, Nmap is unable to tell whether the port is open or filtered. This category may include UDP, IP protocol, FIN, Null, and Xmas scanning.

Closed/filtered (closed or filtered): This state is utilized when Nmap cannot detect whether the port is closed or filtered. It will only be seen in the IPID Idle scan.

The following is the syntax for port scanning with Nmap:

[target] Nmap -p

The option -p is used in the preceding syntax to indicate the port to be searched. A single port, many ports, or a range of ports might be defined. When providing multiple scanning ports, use commas to separate them. Nmap scans ports in a range of 1 to 1000 by default.

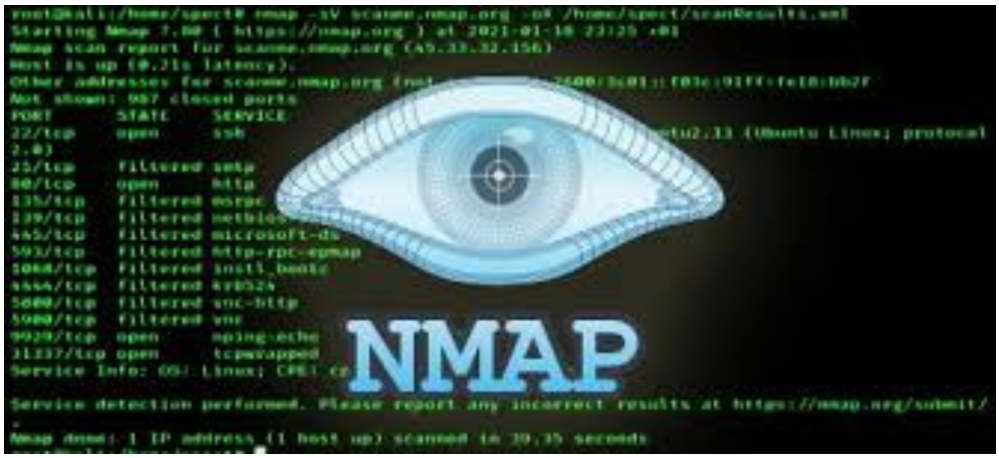
Scanning ports on the target host 192.243.176.84 is a use-case scenario. The following is the execution command:

nmap 192.243.176.84 root@exampleserver

By default, when this command is performed on the terminal, the Nmap utility searches 1000 ports.

The open ports will be shown in the output.

Use-case scenario: Set the port range to 1 to 50 and scan the target host for ports.



The following is the execution command:

nmap -p 1-50 root@exampleserver 192.243.176.84

We can see from the output result after entering the above terminal that the ports 1 through 50 are scanned. All available ports will be listed.

Use-case Scenario:

Specify the scan target host's ports 21 and 23. The following is the execution command:

nmap -p 21,23 192.243.176.84 root@exampleserver

This provides considerably more precise information about the two sections that were expressly requested by the command. You may reduce the time it takes to scan the ports by employing these strategies.

2) Employ the Dmitry tool.

The Dmitry program has a -p option for port scanning.

The following syntax is used to accomplish port scanning:

[host] Dmitry -p

In this case, the host is the IP address of the target for which we are attempting to scan the ports.

Example of a Use-Case Scenario:

Dmitry should be used to scan the open ports on the target host 192.243.176.84.

The following is the execution command:

dmitry -p 192.243.176.84 root@exampleserver

All of the ports open on the target host may be seen in the output information. The number of scanned ports and the number of closed ports may be seen in the penultimate line of output.

What Comes Next?

Despite how vital ports are, they remain challenging to install. Administrators nowadays use intrusion detection systems, but it is not intelligent to depend only on them. Furthermore, with ports, we may not locate the extra information necessary to construct exploits. It would be beneficial if we could learn more about the target's operating system. Continue reading to learn more about OS system identification in the next chapter.

Chapter Six: Recognizing the operating system

The system type of the target host may be established by identifying the operating system. In this technique, penetration testers may do vulnerability detection on the target system's application in a planned manner, saving unneeded lost time. With significant examples, this section will introduce the way of recognizing the operating system.

TTL (Time To Live) recognition: This information indicates the maximum number of network segments that an IP packet may cross before being

rejected by the router. Different kinds of operating systems react with varying values of TTL. As a result, users may use the Ping command to identify the technique. A list of starting TTL values for each operating system will be required to allow users to rapidly ascertain the nature of a target system. A fast Google search will lead you right to them.

Scenario of application:

Ping may be used to determine the operating system type of the target host 192.243.176.84. The target host's operating system is Kali Linux. Let's see whether the command can detect it or not.

The following is the execution command:

ping -c 192.243.176.84 root@exampleserver

The TTL value in the answer packet is 64, as shown by the output information. The host is most likely a Linux operating system. You may test this command on your operating system to see how useful it is.

Scenario of application:

Ping may be used to determine the operating system type of the target host 192.243.176.84. The target host's operating system is Windows 7.

The following is the execution command:

ping -c 192.243.176.84 root@exampleserver

According to the output information, the TTL value in the answer packet is 128. This is a Windows operating system, which can be described.

Tip: If there are too many routers between the local host and the target, the judgment result may be off.

Because TTL is simply an imprecise assessment, the outcome may be inaccurate. The NMAP tool has a feature for detecting the operating system. The next part will go through how to utilize NMAP to determine the kind of operating system.

The syntax for identifying the operating system using NMAP is as follows:

[target] Nmap -O

In this case, target refers to the host address that we attempt to attack during our penetration testing.

Scenario of application:

NMAP may be used to determine the operating system type of the target host 192.243.176.84.

The following is the execution command:

nmap -O 192.243.176.84 root@exampleserver

Based on the output information, we can deduce that the target host's operating system is Microsoft Windows 7/2008/8.1. Although it is hard to tell which version it is, the closest system version will be shown.

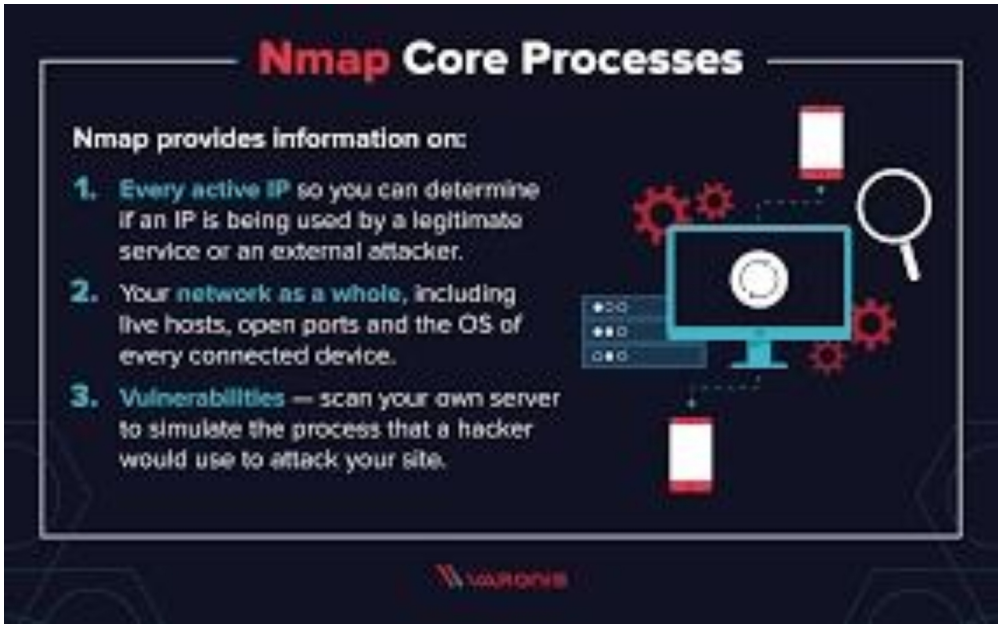
While Dmitri has the same functionality, our experience has shown that it produces more mistakes throughout the scan. We strongly advise you to solely use Nmap to learn about the specifics of the host operating system.

What Comes Next?

We shall go through identification services in depth. Continue reading!

Chapter Seven: NMAP tool

The identification service mainly uses the version information of the detection service. In general, specific older versions may include vulnerabilities. If there are flaws, users may enter the host and gain further valuable information. This section will explain how to discover services for simpler target exploitation.



NMAP tool usage

The Nmap tool has a -SV option that may be used to determine the service's version. The section that follows will provide a Nmap approach for identifying services that makes use of this parameter.

The syntax for identifying the service version using Nmap is as follows:

[host] Nmap -sV

The option -is in the above syntax denotes the implementation of service version detection.

Scenario of application:

Identify all open services and versions on the 192.243.176.84 target host.

The following is the execution command:

nmap -sV 192.243.176.84 root@exampleserver

The output information reveals the specified service-related information. The output data has four columns: PORT (port), STATE (state), SERVICE (service), and VERSION (version). You may gather helpful information about the respective service by analyzing each column of data. FTP, for example, corresponds to TCP port 21, and the version is FileZilla ftpd. The final line also shows that the target host's hostname is TEST-PC and the operating system type is Windows.

A map is a collection of penetration testing tools for discovering network services, which includes two programs: amap and amapcrap. The amap tool, for example, is used to attempt to detect apps operating on atypical ports. In contrast, the amapcrap device discovers applications based on non-ASCII encoding by sending trigger packets and searching the response string list for the response.

The part that follows will go through how to utilize Amap tools to find service information.

1) Make use of the amapcrap tool.

The amapcrap utility may transmit random data to UDP, TCP, or SSL ports to acquire unlawful response information. The information gathered will be written to the appdefs. trig and appdefs.resp files to aid in the next stage of Amap detection.

This tool's syntax for identifying service information is as follows:

0ab> amapcrap -n -m [host] -v [port]

The -V denotes the verbose mode.

Scenario of application:

To probe port 90 apps, use the amapcrap program. The following is the execution command:

amapcrap -n 20-ma 192.198.153.84 90 root@exampleserver -v

We may deduce from the given results that the gathered data is written into the appdefs.trig and appdefs. resp trigger files. These two files will be used to acquire information when users use the Amap tool to identify services.

2) Make use of the map tool.

The amap utility may attempt to discover apps that are running on unusual ports.

This tool's syntax for identifying service information is as follows:

[host][port] amap -bqv

Scenario of application:

Scan the port 80 services on the target host 192.243.176.84 using the map tool.

The following is the execution command:

amap -bqv 192.243.176.84 80 root@exampleserver

According to the output information, the service matching port 80 is HTTP or HTTP-apache2. According to the presented identifying information, the web service operating on the target host is Apache, and the version is 2.2.8. The amap tool employs two trigger files and a response file, as seen by the first three lines of output. Appdefs.trig, appdefs.resp, and appdefs.rpc are some of the file names.

Service Information Collection

Some specialized services may be able to give extra information. SMB service, for example, may provide file system structure, while SNMP service can provide target host information. This section will describe how to utilize these services to acquire vital information on the target for your pen-testing.

SMB Support

SMB (Server Message Block) is an IBM protocol that allows computers to share files, printers, serial ports, and other resources. The SMB protocol may be used with the TCP/IP protocol or with other network protocols (such as NetBEUI). You may learn about the file system structure of the target host by collecting the SMB service's shared folder metadata. The shared folder information for utilizing the smbclient program to access the SMB service will be introduced in the next section.

smbclient is an SMB client program that may be used to access shared files in the SMB service.

The following is the grammatical format of the smbclient tool:

smbclient -L -U username>/username> root@exampleserver

The following are the alternatives and meanings in the grammar above: -L: This option defines the SMB server address. -U: This option is used to define the user name for login into the SMB service.

Use

-Case scenario: Use the Linux system's SMB service. The following is the execution command:

smbclient -U root -L 192.243.176.84 Enter the password for WORKGROUProot:

Entering the password for the SMB service user login will reveal the data that requires further investigation.

The files shared in the target SMB may be seen in the output information. Sharename is the name of the shared file, kind is the type of hard drive, and Comment is a description of the shared file. It may be mentioned that the target host's operating system is Linux, and the shared file is of the Linux file system type.

If the destination host's operating system is Windows, the file name column will show the shared folder's drive letter.

smbclient -L 192.243.176.84-U root@exampleserver

As shown by the file name of the above output result, the default shared discs are C disc and E disc. Only in the Windows operating system are folders separated into discs by drive letters. It is possible to conclude that the shared folder is of the Windows system type.

SNMP Service SNMP (Simple Network Management Protocol) is a set of network management standards that includes an application layer protocol and a collection of resource objects. The network management system uses this protocol to monitor any circumstance on network equipment that requires the administrator's attention. This service may be used to retrieve host information. The section that follows will explain how to use the snmpcheck program to acquire host information.

To retrieve target host information, use the snmpcheck program to enumerate SNMP devices.

The tool's syntactic format is as follows:

[target] SNMP-check

Scenario of application:

To acquire 192.243.176.84 host information through the SNMP protocol, use the SNMP-check utility.

The following is the execution command:

SNMP-check 192.243.176.84 root@exampleserver

When the connection is successful, the host's system information may be acquired.

Each section must be understood because of the vast quantity of output information generated by the preceding command. Continue reading!

1) We may collect system information such as the hostname, kind of operating system, and architecture.
2) We have access to user account information.
3) It is possible to retrieve network information such as the TTL value, TCP segment, and data element.
4) It is possible to retrieve network interface information such as interface status, speed, IP address, and subnet mask.
5) Capable of obtaining network IP information.
6) It is possible to retrieve routing information such as the destination address, the next-hop address, the subnet mask, and the path length value.
7) It is possible to acquire the monitored TCP port. .

8) It is possible to receive monitoring UDP port information. For example, UDP ports that are monitored maybe 123, 154, 6300, 300, and 5322.

9) We may collect information about network services such as distributed component object model service, DHCP client, and DNS client.

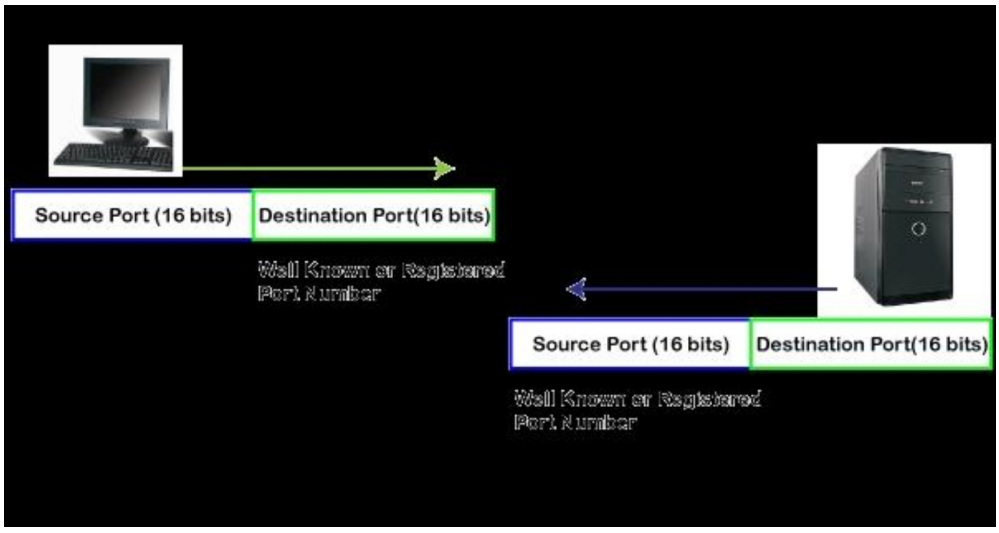
10) We may retrieve process information such as the process ID, name, and type.

11) 11)We can get storage information such as device ID, device kind, and file system type.

12) It is possible to retrieve file system information such as the index, mount point, remote mount point, and access rights.

13) Capable of obtaining device information such as the device ID number, kind, and status.

14) Can get information on software components such as.Net framework, Visual C++2008, and so on.



What Comes Next?

We have now accomplished an essential portion of the information collecting method during penetration testing. With all of this collected data, we must analyze it to get or develop a workable process. To make this approach as simple as possible for you, we will describe the Maltego tool in full. Continue reading!

Chapter Eight: Maltego Configuration

A vast quantity of information about the target host may be gathered using the techniques mentioned above. Users must sort and analyze this data to simplify the later deployment of penetration testing. At this stage, users may utilize Maltego tools to analyze and organize the data.

This part will go through how to utilize Maltego tools to analyze and organize data.

Maltego

Configuration

Maltego is a very effective information collecting tool. It can gather the essential information automatically, but it can also visualize the obtained data and display the findings to users visually. The Maltego program is installed by default in Kali Linux so that users may utilize it right away. However, before using the program, you must first do some basic setup, such as creating an account and logging in.

Choosing a starting mode The Maltego tool will be configured in the section that follows.

1) Create an account.

When using Maltego technologies, customers must first log in to the company's social page. As a result, before using the tool, you must first create an account.

The registered account's address is as follows: https://www.paterva.com/web7/community/community.php

A dialogue box containing field boxes will appear when the user successfully navigates to the location mentioned above in the browser.

Fill out the appropriate information in this dialogue box and check the "Perform human-machine authentication" option. A dialogue window for image verification will appear. Select the relevant image in this dialogue box by following the directions and clicking the "Verify" button. After the verification has been completed successfully, the registration dialogue box will be presented.

At this moment, click the Register! Button to finish the registration process. You will now get an email from the email address you used to create your account. To activate your account, log in to your inbox.

2) Enable the Maltego mode.

Maltego has two modes: Regular Privacy Mode (normal privacy mode) and Stealth Privacy Mode (stealth privacy mode) (concealed privacy mode). The Normal Privacy Feature mode, for example, may get more information. Furthermore, users can directly access data on the Internet, such as physical images and website information. Stealth Privacy Mode is more often utilized to analyze data quickly, particularly when the current.

The PC lacks a network. It will not be able to acquire data directly from the Internet when using this model. So, to get more information, it is advised to choose the Normal Privacy Mode. The section that follows will go through how to establish the Maltego mode in detail.

Scenario of application:

Set the Maltego privacy setting to Normal. The following are the particular steps:

1) In the graphical interface's menu bar, choose "Applications"|"Information Collection"|maltego command. The Maltego product selection dialogue box will then appear.

2) This dialogue box displays the various Maltego products, which include Maltego XL, Maltego Classic, Maltego CE (Free), and Maltego CaseFile (Free). Maltego XL and Maltego Classic are paid applications, while Maltego CE and Maltego CaseFile are

free. We will now choose the free Maltego tool and press the run button.

3) The licensing agreement information is shown in this dialogue box. Click the Next button after selecting the Accept check box. The login dialogue box will appear.

4) In this dialogue box, enter the previously registered account information (email address, password, and verification code) to log in to the Maltego server. Then, press the Next button. A dialogue box will be shown.

5) The outcome of the login is shown in this dialogue box. The login user name, email address, and login time may all be found in this dialogue window. Then, after clicking the Next button, a dialogue window for installing Transforms will appear.

6) This dialogue box contains information about the to-be-installed application services, Transforms, entities, and hosts. Then press the Next button to bring up another dialogue box.

7) In this dialogue box, you may choose whether or not to activate the automated error reporting option. Select the Automatically transmit Error Reports option to activate it. Click the Next button if you do not wish to start it. The privacy mode selection dialogue box will appear once you click the Next button.

8) In the dialogue box, click the Next button after selecting Normal mode.

9) From this phase, it is clear that Maltego is ready. At this stage, the user may gather data using the Maltego program. There are three default approaches available here: Open a blank graph and let me play about (open a blank chart), Open an example graph (open an example graph), and Go away; I've done this before! Select the first running technique here. Allow me to experiment with a blank chart, which will launch the interface.

10) The presence of this interface indicates that Maltego has been successfully launched, and a new chart has been opened. The user may then choose any object and drag it on the graph to analyze and organize it.

Maltego Tool Usage

The Maltego utility may be used regularly, thanks to the prior settings. The Maltego program allows users to organize and analyze previously obtained data. You may also acquire additional information by using Maltego's Transforms. Maltego has a wide variety of entities for representing information nodes.

The Domain entity may be used to express domain name information. The part that follows will explain how to use Maltego tools to organize and analyze data.

Organize and analyze host data

We can determine the active hosts in the local area network using prior data gathering. Open ports, services, and operating systems are examples of hosts.

The following section will go over how to utilize IP address entities to organize and analyze host data.

Scenario of application:

To organize and analyze host information, use the Maltego tool. The following are the particular steps:

1) Launch the Maltego utility, and the UI will appear.
2) The interface's left column displays all accessible entities. In this case, the IP address entity will be used to sift through the obtained host-related data. Select the IPv4 Address item and drag it to the chart to show the interface.
3) You can see from this interface that an IP address entity has been added to the chart, using the default IP address of 192.243.176.84. At this time, the user may change the address to the active host address that was found, such as 192.168.29.136. The user may change the entity's address by double-clicking its IP address or changing the value of the attribute IP Address.
4) This interface shows that the value of the IP address entity has been successfully updated. At this time, to sort out the host's vital information, the user drags and drops the Port and Service entities to the chart in the same manner.

5) You can view the newly inserted ports and service entities through this interface. The port default attribute value is 0 among them. The default attribute value for the service is 80/Apache 9. Users may change the values of entity attribute values depending on the data they gather. We can see from the information collected above that the host has 21, 22, 80, 135, and 139 open ports, with the relevant services being FTP, SSH, HTTP, msrpc, and NetBIOS-ssn.

6) At this point, the information gathered is sorted. Users may link the connection between them by connecting lines to make analysis and viewing more straightforward. Use a cable, for example, to link the host IP address and port here. Click the mouse near the IP address entity (192.243.176.84), which will cause a line to be expanded, and then click the port entity. A dialogue window will appear at this point.

7) The information in this dialogue box is used to configure the connecting line's Label, Color, Style, and Thickness. Set the line's label to port and the color to read here, and use the default settings for the remaining variables.

8) Click the OK button to see the newly inserted connecting line.

9) This interface shows that the connection between the IP address entity and the port entity has been formed successfully. Using the same way, users may link other entities' relationships with connecting lines and designate entity information with tags.

10) The gathered information is more naturally displayed and easier to utilize using this interface. At this point, users may additionally utilize Maltego Transforms to acquire more information, such as IP owner information, network information, and history information.

Domain name information should be organized and analyzed.

We may learn about the obtained domain name WHOIS information, subdomain name, and server information by analyzing the previously gathered data. The next part will use Domain entities to organize and analyze domain name information.

To organize and analyze domain name information, use the Maltego tool.

The following are the particular steps:

1) In Maltego, create a new chart to prevent confusion with old data. Select the New Chart option.
2) From this interface, you can see that a new graph has been opened with the name New Graph (2). To organize and analyze domain name information, choose the domain entity (Domain). Drag the Domain entity from the entity panel to the chart, and then change the entity's domain name to wikipedia.com.
3) We can see from the given information that the domain name's WHOIS information, subdomain name, and server information have been retrieved. Here are several subdomains of the domain name wikipedia.com. DNS Name is the entity used to represent the subdomain name. As a result, pick DNS. Drag an entity from the entity list to the chart, then change the entity name to the relevant subdomain name.
4) You may see the organized subdomain information from this interface. Similarly, the user may link them via the cable.
5) From this interface, you can see how the domain names that have been gathered are organized. Furthermore, all subdomains related to the domain name wikipedia.com are visible. At this point, users of Maltego's Transform may also get further information about the domain name and subdomain names, such as the domain name registrar, subdomain name, and WHOIS information.

To gather information, use Transform.

Maltego has a plethora of Transforms that may be used to get more data. To obtain further information, the following will use the domain name entity as an example.

The Transform may be used to get information on the domain name wikipedia.com.

The following are the particular steps:

1) Drag the Domain entity to a new chart and change the domain name to wikipedia.com.
2) Select the domain name object and right-click to get a list of all accessible Transforms.
3) You can examine the Transform sets that may be utilized for domain name entities, such as Shodan, ThreatMiner, and Farsight DNSDB, using this interface. If the user wishes to see. To display all Transforms, choose All Transforms from the drop-down menu. To examine a specific Transform set, click the appropriate Transform. Click the All Transforms button to get a list of all Transforms.
4) At this point, the user may choose any Transform to receive the associated data. To locate additional top-level domains of a domain name, use the To Domain[Find other TLDs] Transform.

With this, we have concluded a quick introduction to Maltego and its novel and practical data analysis capabilities. This chapter brings Module 2 to a close. The next module will help us improve our hacking abilities by teaching us about vulnerability scanning and sniffing attacks. We suggest that you complete the first two courses before moving on to the third.

BEST WISHES and the third module is on its way!