#Lab 02: Information Gathering

## Scenario

In this lab, you will familiarize yourself with commonly used reconnaissance tools and techniques used in the early phases of penetration testing.

You are a penetration tester. Your newest client, Structureality, has hired you to evaluate the security of their network. The client has recently started using 515support as their MSP (managed service provider). However, Structureality is not sure that the technology implemented by 515support is well secured. Therefore, you start your assessment by performing initial reconnaissance and information gathering. This will include reviewing a client's website, extracting information using <tt>whois</tt>, performing DNS reconnaissance, and retaining command history for a pentest report.

## Understand your environment

You will be working from a virtual machine named KALI hosting Kali Linux 2022.2. First, you must discover the remainder of the systems in this lab environment related to your pentest client.

>[!ALERT] The virtual hosting of Kali Linux does not support the ++TypeText++ feature, so you will need to enter all commands for this lab manually. These commands are displayed in a <tt>**\*\*bold terminal font\*\***</tt>.

## Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA PenTest+ objectives:

- 2.1 Given a scenario, perform passive reconnaissance.

- 2.2 Given a scenario, perform active reconnaissance.

- 2.3 Given a scenario, analyze the results of a reconnaissance exercise.

- 5.3 Explain use cases of the following tools during the phases of the penetration test.

===

# Find and explore a client's website

Often the first step a penetration tester performs is to orient themselves as to where they are logically located and then confirm or discover the client's online presence. In this exercise, you will verify your Kali pentester client is connected to the simulated internet of the lab environment, determine if the client's website is online, and discover information about the client from their website.

1. [] Connect to the @lab.VirtualMachine(KALI).SelectLink and sign in as <tt>**\*\*@lab.VirtualMachine(KALI).Username\*\***</tt> using <tt>**\*\*@lab.VirtualMachine(KALI).Password\*\***</tt> as the password.

1. [] Open a Terminal window by selecting the **\*\*Terminal Emulator\*\*** from the Kali Linux toolbar (located at the top of the screen by default). This icon looks like a black computer screen with a cursor.

1. [] Determine the current IP address of the eth0 interface by entering: <BR> <tt>**\*\*ip a s eth0\*\***</tt>.

1. [] The results should indicate the IP address of <tt>203.0.113.66</tt>.

>[!NOTE] In this lab, the IP address range of <tt>203.0.113.0/24</tt> is defined as the internet.

1. [] You have been informed that the FQDN of the client is www.structureality.com. Capture the output of a ping command to see if that FQDN responds to echo-requests by entering the following command:<br> <tt>**\*\*ping www.structureality.com > client\_info.txt\*\***</tt>.

>[!KNOWLEDGE] It is a best practice to always capture the output into a file to create a record of activities during a penetration test.

1. [] Wait for a count of 10 (i.e., approximately 10 seconds), then press <tt>**\*\*CTRL+C\*\***</tt> to terminate the operation.

1. [] Confirm that the output file exists and contains data by entering the command: <tt>**\*\*ls -l\*\***</tt>.

>[!NOTE] You should see the file <tt>client\_info.txt</tt> with a size of at least 100 bytes. This confirms that the output file was created and collected some information.

1. [] Display the contents of the output file by entering the command:<br> <tt>**\*\*cat client\_info.txt\*\***</tt>.

>[!NOTE] The display should show that the FDQN of <tt>www.structureality.com</tt> resovles to <tt>203.0.113.1</tt>. You should also see that while 4 packets were sent (i.e., echo-requests), that no packets were received in response.

>[!KNOWLEDGE] Not getting any results from an echo-request from a ping command may indicate that the target is either protected by a firewall or otherwise configured to ignore echo-requests.

Validate this task <!--- use a script to confirm the existence of /home/kali/client\_info.txt --->

1. [] Open Firefox by selecting its icon from the Kali Linux toolbar.

1. [] In the address field of Firefox, enter <tt>**\*\*www.structureality.com\*\***</tt>.

<!--- Sometimes, this activity shows an error related to a self-signed certificate or unknown issuer - this needs to be resolved to avoid this issue. --->

<!--- A basic company Web page needs to be created. A simple logo, graphics, a link to a contact us page, with some basic but false company info, like address, phone, email, fax, employee names, leadership names, etc. --->

1. [] Select the <tt>**\*\*Contact Us\*\***</tt> link. Notice that a company name, address, phone number, and email address are presented.

1. [] Close Firefox, but leave the Terminal window open.

### Check your work

- [] Confirm that you determined your pentest client's IP address.

- [] Confirm that you attempted to ping the client's FQDN and recorded the results into a file.

- [] Confirm that you visited the client's FQDN using a browser.

- [] Confirm that you discovered details about the client from their website.

===

##Whois reconnaissance

Another common practice of a penetration tester is determining the ownership of the client's registered domain name using <tt>whois</tt>. This can provide details about the company name, address, phone, email addresses, and personnel set as contact points. You will capture the whois output to a file to use in your pentest report.

1. [] Connect to the @lab.VirtualMachine(KALI).SelectLink and, if needed, sign in as <tt>**\*\*@lab.VirtualMachine(KALI).Username\*\***</tt> using <tt>**\*\*@lab.VirtualMachine(KALI).Password\*\***</tt> as the password.

1. [] Return to the terminal window.

1. [] Perform a <tt>whois</tt> query using the whois database host of 192.0.2.10 against the client's registered domain name and captuer the output to a file by entering: <tt>**\*\*whois -h 192.0.2.10 structureality.com > client\_whois.txt\*\***</tt>.

>[!NOTE] The host of <tt>192.0.2.10</tt> is the whois database host and server for this lab environment.

1. [] View the captured output of the <tt>whois</tt> operation by entering: <tt>**\*\*cat client\_whois.txt\*\***</tt>.

1. [] Read over the output of the whois command. You may need to scroll up to view the entire presentation.

Q: Who is the owner of the structureality.com registered domain name?

515web

515support

Structureality

IROOT INC <!--- correct --->

1. [] Notice the *\*Name Server\** line near the end of the whois output. This line displays the name server as <tt>ns.515web.net</tt>.

>[!NOTE] The Name Server line of the whois output confirms that the client's website's FDQN is hosted by a DNS server run by the ISP 515web.

Validate this task <!--- use a script to confirm the existence of /home/kali/client\_whois.txt --->

1. [] Leave the Terminal window open.

### Check your work

- [] Confirm that you performed a whois query and captured the output to a file.

- [] Confirm that you discovered information about the client from whois output.

===

##DNS reconnaissance

Another common penetration testing task is to enumerate information from DNS about the client. This can often be used to discover other related FQDNs, name servers, email servers, and more. In this exercise you will be using the CLI tools of <tt>nslookup</tt> and <tt>dig</tt>.

1. [] Connect to the @lab.VirtualMachine(KALI).SelectLink and, if needed, sign in as <tt>**\*\*@lab.VirtualMachine(KALI).Username\*\***</tt> using <tt>**\*\*@lab.VirtualMachine(KALI).Password\*\***</tt> as the password.

1. [] Return to the terminal window.

1. [] Open nslookup in interative-mode by entering: <tt>**\*\*nslookup\*\***</tt>.

>[!KNOWLEDGE] Nslookup is a program to query the Internet Domain Name System (DNS) via submitting requests to domain name servers. Nslookup operates in one of two modes: **\*\*interactive or non-interactive\*\***.<br><UL><LI>**\*\*Interactive mode\*\*** allows a user to search domain name servers for IP and name information on various hosts or domains. It can also be used in this mode to display a list of hosts in a domain. <br> <LI> **\*\*Non-interactive mode\*\*** just returns the name or IP information requested for an individual host or domain. </UL>

>[!TIP] Windows also has a native <tt>nslookup</tt> command, which operates for the most part like the version in Linux or macOS.

1. [] Check the lookup server being used by nslookup by entering: <tt>**\*\*server\*\***</tt>.

1. [] The results should indicate <tt>203.0.113.226</tt> is being used as the default server.

>[!KNOWLEDGE] By default, nslookup uses the same DNS server to perform queries as the host. However, the <tt>server</tt> sub-command can be used to change the DNS server used to perform lookups.

1. [] View the address resource records of the FQDN of the client by entering: <tt>**\*\*www.structureality.com\*\***</tt>.

1. [] The results should show an IPv4 address of <tt>203.0.113.1</tt>. This is the same address discovered through the <tt>ping</tt> operation in an earlier exercise.

>[!KNOWLEDGE] This lab environment is limited to using only IPv4. If IPv6 were available, you would also see any defined IPv6 address associated with this FQDN. You can also set the lookup type to <tt>A</tt> for IPv4 addresses or <tt>AAAA</tt> for IPv6 addresses or <tt>ANY</tt> for any/all addresses.

1. [] Notice the caveat statement above the results of &quot;<tt>Non-authoritative answer:</tt>&quot;. This indicates the results are being returned from a caching DNS server instead of directly from an authoritative server. It is good practice to work directly against an authoritative server.

1. [] Resolve the nameserver discovered from the prior <tt>whois</tt> exercise of <tt>ns.515web.net</tt> into its IP address by entering: <tt>**\*\*ns.515web.net\*\***</tt>

1. [] Change the lookup server for nslookup to the IP address of ns.515web.net by entering: <tt>**\*\*server 203.0.113.225\*\***</tt>

1. [] Perform the client's FQDN address query again by entering: <tt>**\*\*www.structureality.com\*\***</tt>.

1. [] Notice the results no longer have the caveat line. Therefore, the results are coming directly from an authoritative DNS server.

1. [] Change the resource record type to view the authoritative DNS servers related to the registered domain name by entering: <tt>**\*\*set type=ns\*\***</tt> followed by <tt>**\*\*structureality.com\*\***</tt>.

1. [] The results should show the nameserver of <tt>ns.structureality.com</tt> with an IPv4 address of <tt>203.0.113.225</tt>

1. [] Change the resource record type to view the SMTP email servers related to the registred domain name by entering: <tt>**\*\*set type=mx\*\***</tt> followed by <tt>**\*\*structureality.com\*\***</tt>.

1. [] The results should show the mail exchanger FQDN of <tt>mail.structureality.com</tt> with an IPv4 address of <tt>203.0.113.1</tt>

<!--- if PTR records are added, then reverse lookups could be performed against these IP addresses --->

1. [] Change the resource record type to view the SOA record related to the registred domain name by entering: <tt>**\*\*set type=soa\*\***</tt> followed by <tt>**\*\*structureality.com\*\***</tt>.

1. [] The results should be similar to the following:

```PowerShell-nocode

origin = structureality.com

mail addr = hostmaster.structureality.com

serial = 2002060901

refresh = 3600

retry = 600

expire = 86400

minimum = 600

```

>[!NOTE] The <tt>serial</tt> value may be different in your display as any edits to a DNS zone file causes an incrementation of the serial number.

>[!KNOWLEDGE] The <tt>mail addr</tt> line in the SOA record is the email address to be used when needing to contact someone about the registered domain. However, notice that it does not currently look like a standard email address. That is because the @ symbol is not an allowed character in DNS. So, the convention is to replace the @ symbol with a period. Therefore, you must replace the first period with an @ symbol to return it to the proper structure of an email address.

1. [] Exit interactive-mode nslookup by entering: <tt>**\*\*exit\*\***</tt>.

The tool of <tt>nsloolup</tt> is a powerful DNS utility, but it does not lend itself easily to recording its operations and results (at least not in interactive mode). So while you can use <tt>nslookup</tt> in non-interactive command mode, in this exercise, you will use <tt>dig</tt> to perform the same queries and capture the output into a file to retain this information for your pentest report.

1. [] Use the <tt>dig</tt> utility to extract DNS information from an authoritative DNS server related to the registered domain name of structureality.com and capture the output into a file by entering: <tt>**\*\*dig @203.0.113.225 structureality.com > client\_dns.txt\*\***</tt>.

1. [] View the captured output of the <tt>dig</tt> operation by entering: <tt>**\*\*cat client\_dns.txt\*\***</tt>.

1. [] Notice that this operation captured the SOA record for structureality.com. While not labeled in the <tt>dig</tt> output, the same values of origin, mail addr, serial, refresh, retry, expire, and minimum are present.

1. [] Capture the <tt>dig</tt> output from <tt>www.structureality.com</tt> into the same output file, but don't loose the existing content by entering: <tt>**\*\*dig @203.0.113.225 www.structureality.com >> client\_dns.txt\*\***</tt>.

>[!KNOWLEDGE] The use of double greater-than symbols (i.e., &gt;&gt;) performs an append rather than a replace function when capturing output into a file.

1. [] View the captured output of the <tt>dig</tt> operation by entering: <tt>**\*\*cat client\_dns.txt\*\***</tt>.

1. [] Notice the output shows the same <tt>A</tt> record result seen previously when using <tt>nslookup</tt>.

1. [] Capture the <tt>dig</tt> output from <tt>structureality.com</tt> for the resource record type of <tt>MX</tt> into the same output file, but don't loose the existing content by entering: <tt>**\*\*dig @203.0.113.225 structureality.com -t mx>> client\_dns.txt\*\***</tt>.

1. [] Capture the <tt>dig</tt> output from tt>structureality.com</tt> for the resource record type of <tt>NS</tt> into the same output file, but don't loose the existing content by entering: <tt>**\*\*dig @203.0.113.225 structureality.com -t ns>> client\_dns.txt\*\***</tt>.

1. [] View the captured output of the <tt>dig</tt> operation by entering: <tt>**\*\*cat client\_dns.txt\*\***</tt>.

1. [] Notice the output shows the same <tt>MX</tt> and <tt>NS</tt> record results seen previously when using <tt>nslookup</tt>.

Validate this task <!--- use a script to confirm the existence of /home/kali/client\_dns.txt --->

1. [] Leave the Terminal window open.

### Check your work

- [] Confirm that you used <tt>nslookup</tt> in interactive mode.

- [] Confirm that you retrieved results from an authoritative DNS server.

- [] Confirm that you enumerated the IP addresses of the client's FQDN, name server (NS), and email server (MX)

- [] Confirm that you viewed the client's SOA record.

- [] Confirm that you used <tt>dig</tt> to capture DNS information into a file.

===

##Export command history for pentest report

After each significant step or phase in a penetration test, it is essential to update the documentation regarding the tasks performed by the penetration tester. This includes exporting commands entered into Terminal windows into a file.

1. [] Connect to the @lab.VirtualMachine(KALI).SelectLink and, if needed, sign in as <tt>**\*\*@lab.VirtualMachine(KALI).Username\*\***</tt> using <tt>**\*\*@lab.VirtualMachine(KALI).Password\*\***</tt> as the password.

1. [] Return to the terminal window.

1. [] Export the Terminal window command history and capture it in a file by entering: <tt>**\*\*history > pentest\_commands.txt\*\***</tt>

1. [] View the captured command history by entering: <tt>**\*\*cat pentest\_commands.txt\*\***</tt>

Validate this task <!--- use a script to confirm the existence of /home/kali/pentest\_commands.txt --->

The various output and command history capture files can be copied to a central location for storage and preservation. This is not performed in this lab, but is a good practice in a real-world penetration testing event.

### Check your work

- [] Confirm that you exported your command history to a file.

===

## Comprehensive questions

Each assisted lab ends with a set of comprehensive questions. Answer these to ensure that you recognize the importance of the activity steps and the uses for the information you have learned.

1. What are the tools nslookup and dig used for?

Searching DNS records <!--- correct --->

Searching Domain registration records

Searching Email records

Searching Dark Web records

All answers are correct.

1. What is the tool whois used for?

Searching DNS records

Searching Domain registration records <!--- correct --->

Searching Email records

Searching Dark Web records

All answers are correct

1. Which option in dig will let you select the DNS record type to return?

-r

-t <!--- correct --->

-d

-z

None of these are correct

1. The Whois tool can provide which of the following information on a domain?

Creation and Expiration dates

Registrant Contact Information

List the DNS servers of the Domain

Registrar's Whois server

All answers are correct <!--- correct --->

1. If no response is received when pinging a FQDN, this indicates what?

The site is under DDOS attack.

The site may be behind a firewall. <!--- correct --->

The site is running Windows.

The site may be in a foreign language.

===

## Grade lab

That concludes this lab. Please ensure you end it properly rather than just closing the browser window.

Once you select **\*\*Submit\*\***, you will not be able to return to this lab instance. If you want to repeat the lab, you can launch a new instance from your lab portal.

1. Check the step boxes to mark all tasks as complete and make sure you have submitted responses to all the activities.

1. Select **\*\*Submit\*\*** below to grade the lab.

>[!TIP] You can use the **\*\*Menu\*\*** button !IMAGE[Screenshot of Menu icon](lod%20icon%20menu.png) to save the lab state and return to it later. Note that you can only have a limited number of labs in a save state at any one time. You can also use the **\*\*Menu\*\*** to end (cancel) a lab. This means that no score will be recorded and that the next time you launch the lab it will be reset to its starting conditions.