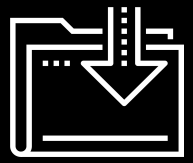
Initial Access and Internal Recon

Cybersecurity

Lesson 16.2



Class Objectives

By the end of today's class, you will be able to:

Understand how initial access fits into the MITRE matrix.

Recognize phishing emails and understand why attackers so commonly use them in order to obtain initial access.

Perform advanced Nmap scans with NSE scripts.

Exploit a machine with a Python script.


Day 1
Recap

Penetration testing, often referred to as **pen testing** or **ethical hacking**, is the offensive security practice of attacking a network using the same techniques that a malicious hacker would use, in an effort to identify security holes and raise awareness in an organization.

Day 1 Recap

The five phases of a pen testing engagement include:

01A	**Planning**	Define the purpose and scope of the test, and sign all legal contracts.
01B	**Reconnaissance**	Obtain publicly available information about your target.
02	**Scanning**	Use tools to run a scan against your target to gather information, such as open ports, and run services to determine potential vulnerabilities.
03	**Exploitation**	Attack the vulnerabilities discovered in the previous steps in order to gain access to the target.
04	**Post exploitation**	Gather valuable information from the compromised systems.
05	**Reporting**	Report on the previous five steps to provide a summary of actions taken, findings, and recommended mitigations.

Reconnaissance consists of gathering information about your target.

Day 1 Recap

Reconnaissance is divided into two types:

01 Passive Recon

Often refers to open **source intelligence (OSINT)**, which leverages information about the target that is publicly available on the internet.

This includes all domains and hosts belonging to a target that are publicly viewable.

02 Active Recon

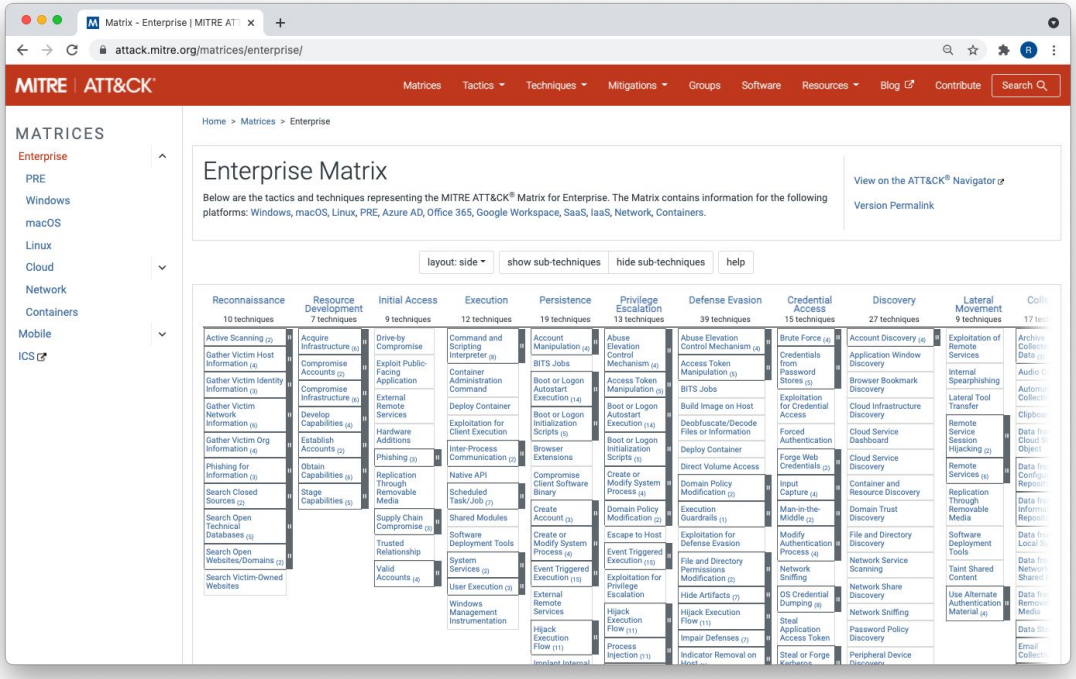
Refers to directly interacting with the target's internal network.

(We will do this today.)

Day 1 Recap

A company called **MITRE** developed the **MITRE ATT&CK matrix** to provide a visual representation of all the **techniques, tactics, and procedures (TTPs)** that may be performed throughout an assessment.

We will use this matrix as a reference for the TTPs that we will conduct throughout the next two weeks of class.

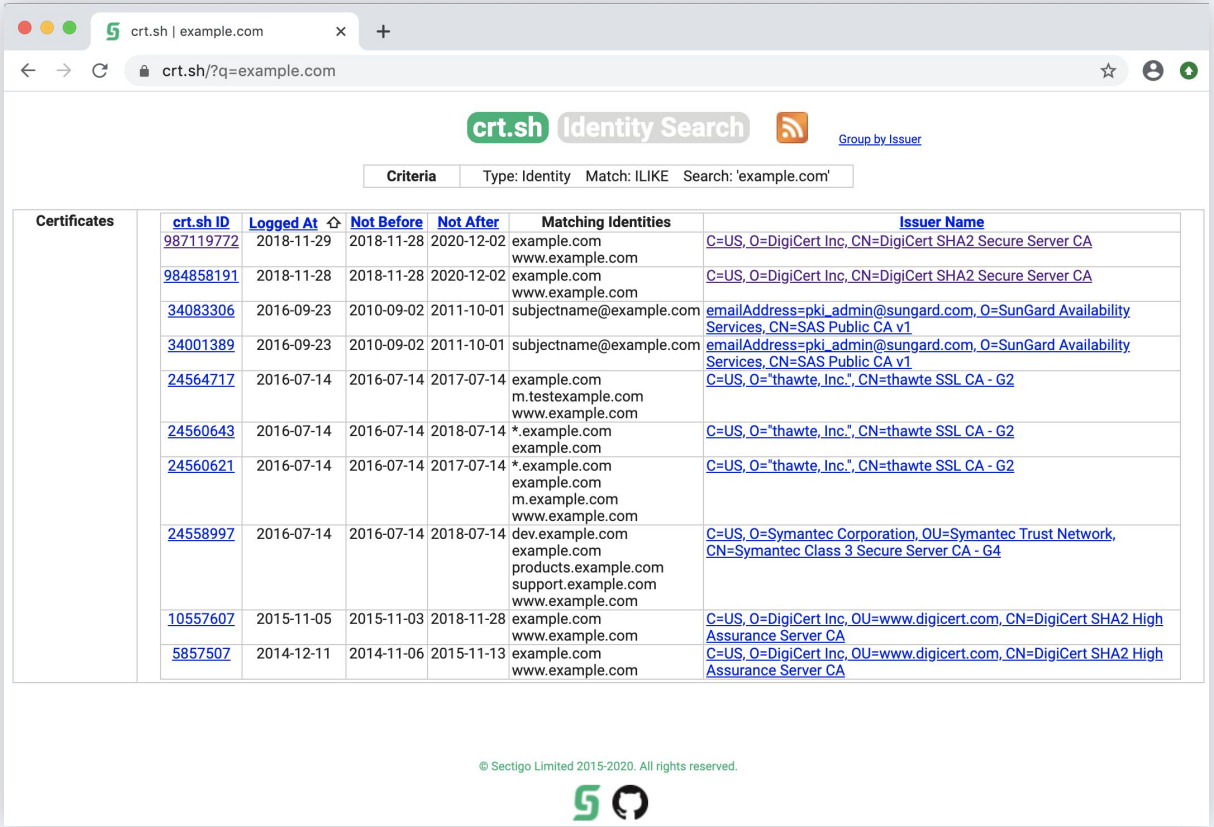


Google Dorking

A reconnaissance tactic in which we manipulate Google searches to narrow down our queries in order to acquire actionable intel.

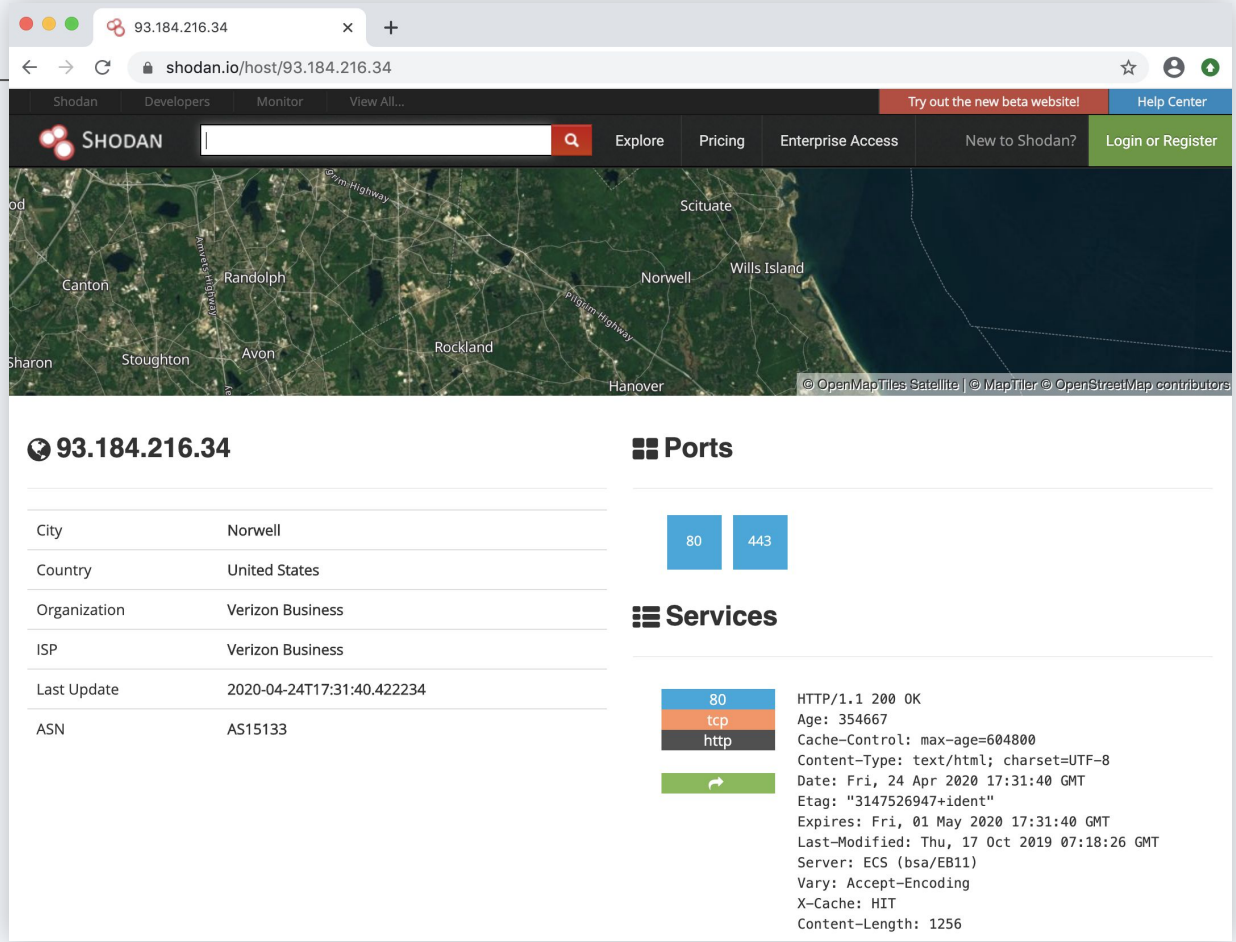
Day 1 Recap

Certificate transparency is another reconnaissance tactic where a penetration tester gathers information from certificate issuers, which publish logs of the SSL/TLS certificates that they issue to organizations.



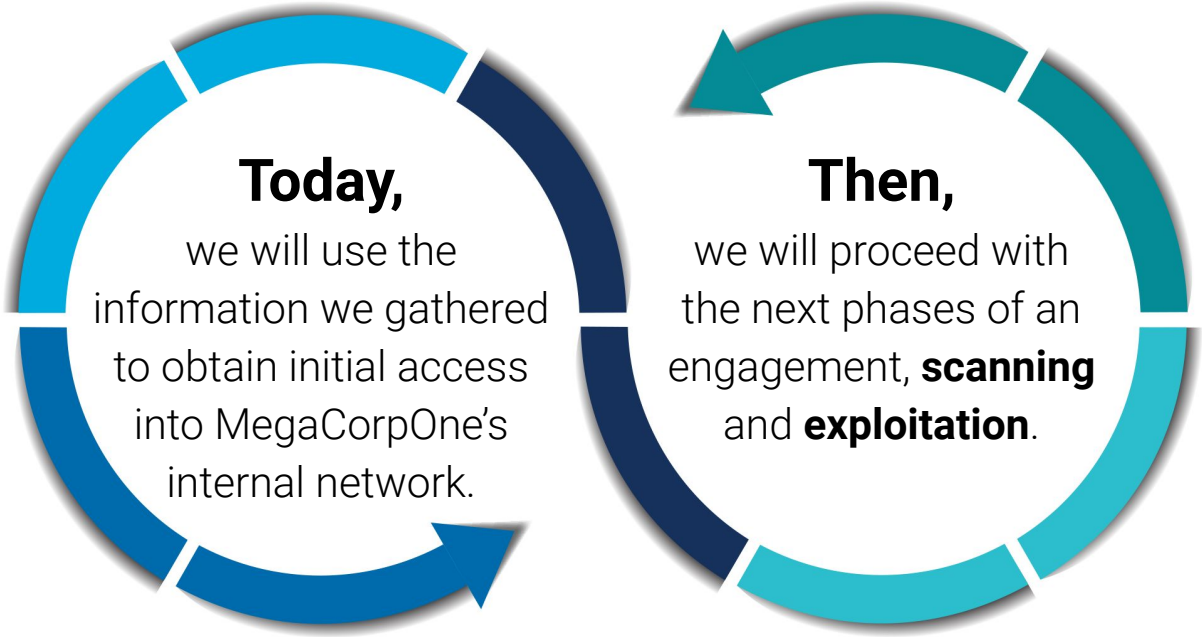
Day 1 Recap

Shodan.io is a reconnaissance website that conducts port scanning across the entire internet and catalogs the results for quick searching.



Day 1 Recap

We ended Day 1's lesson by using Shodan and Recon-ng in the **reconnaissance** phase to identify subdomains and other related domains belonging to MegaCorpOne.



Every method we use this week will tie back to a specific tactic and technique found on the MITRE ATT&CK matrix.

Gaining Initial Access

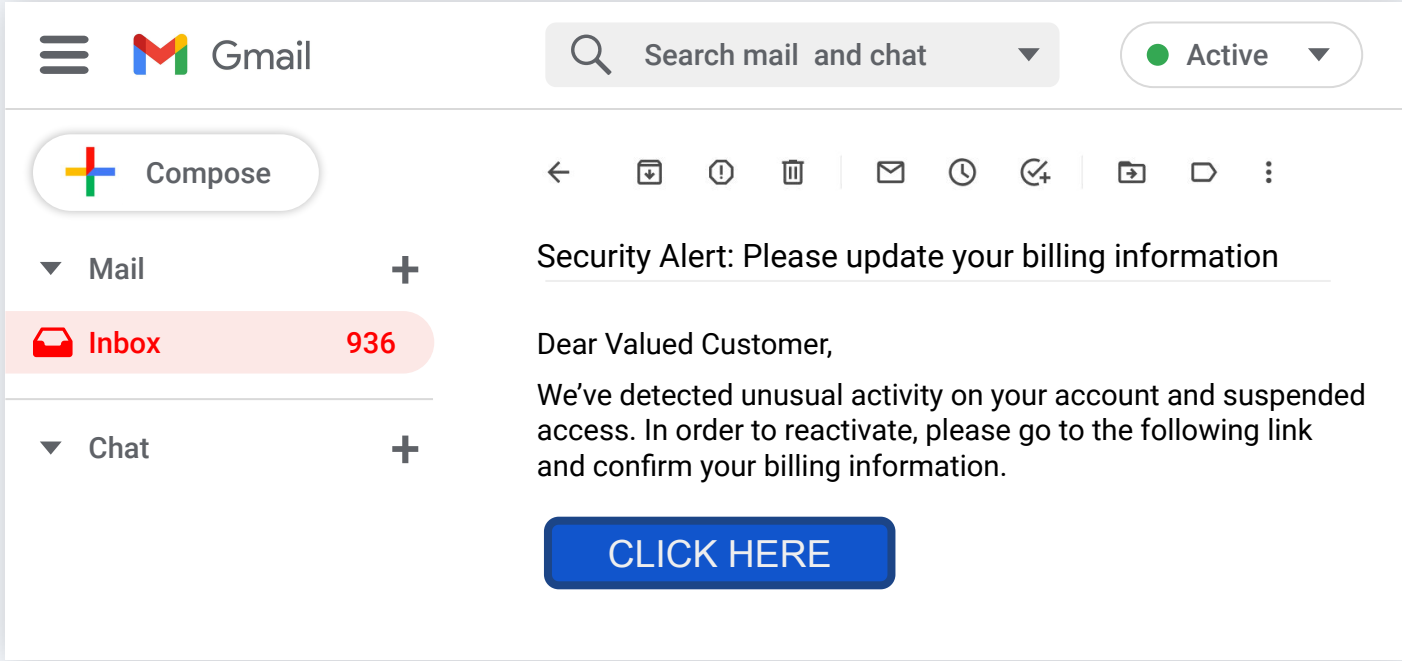
Gaining Initial Access

The information that we gathered in the previous class can be used to gain **initial access** into our target.

For example:

Through Google dorking, you may find an employee's name, job title, direct reports, and email address.

You could use that information to craft a deceptive email to try and obtain the employee's credentials for their private network.



Initial Access

MITRE defines “initial access” as follows:

Initial access consists of techniques that use various entry vectors to gain their initial foothold within a network.

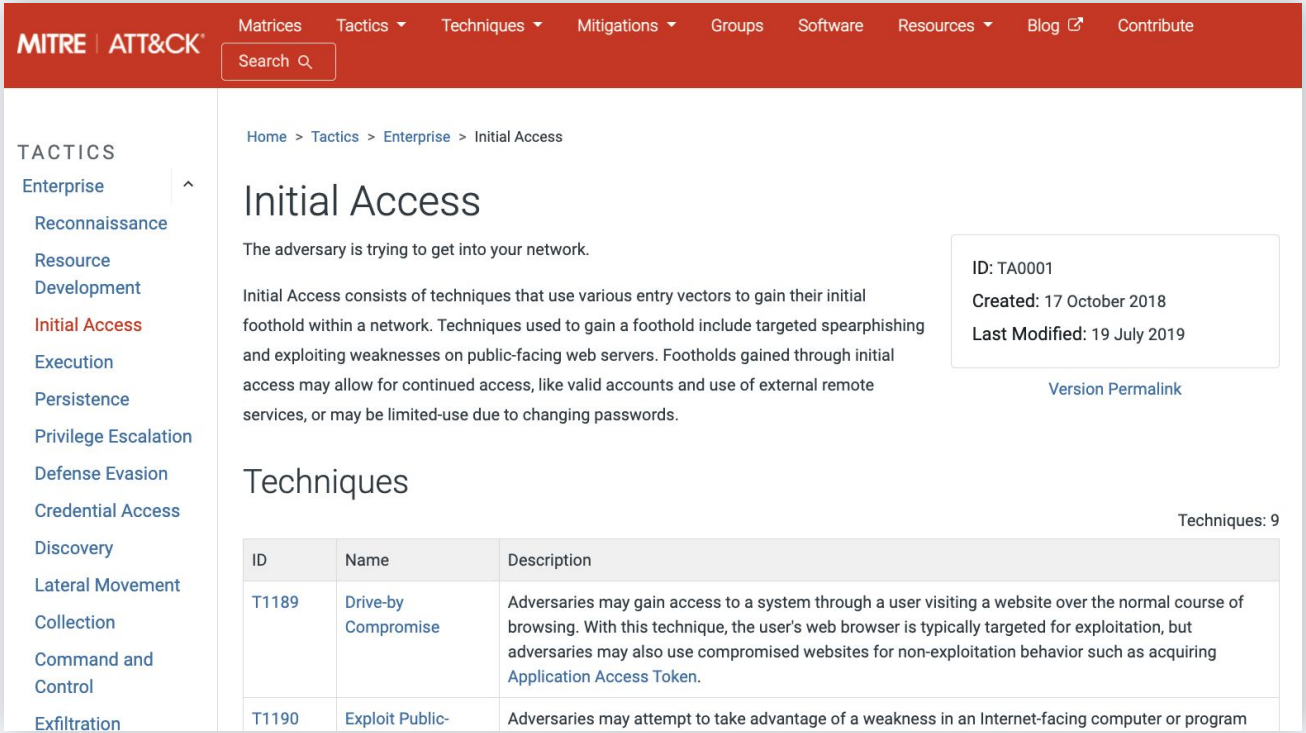
Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers.

Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Source: https://attack.mitre.org/tactics/TA0001/

Gaining Initial Access

Initial Access is [Tactic ID TA0001](#).



Gaining Initial Access

We will cover two methods of gaining initial access on a target machine or network:

Phishing

The most common method, in which the attacker crafts a fraudulent email that misleads the recipient into clicking on a link in the email.

Remote Services through Valid Accounts

This method involves gaining access to the target by guessing credentials on a VPN login portal. These techniques are categorized by MITRE as Valid Accounts and External Remote Services.

Phishing

Phishing is the most common way an attacker gains access to the internal network.

Phishing

The goal of phishing can vary.

Sometimes,
a phishing email is sent only to obtain credentials.

Other times,
the email contains a malicious link that will install malware or a backdoor on the victim's computer.

Phishing

Phishing is more like a social engineering exercise than a technical abuse.

- Unlike other attacks, phishing leverages human error by crafting misleading and convincing fraudulent emails.
- Therefore, there is no “patch” to prevent phishing.
- An organization’s best defense is to require users to complete security awareness training in which they’re taught how to identify phishing emails.

Can you name any telltale signs that an email is a phishing attempt?

Phishing

Telltale signs of a phishing attempt:

Typos	In the body of the email and the sender's email address are common flags.
Typosquatting	A common tactic in which an attacker will register a fraudulent domain similar to a legitimate one. **For example:** `Google.com` vs. `GoogIe.com` (with a capital "i" instead of a lowercase "l")
Subdomains	Are often registered to mimic real domains. **For example:** `payments.google.com` vs. `paymentsgoogle.bogusdomain.com` Remember that domains can be spoofed if proper DNS protections are not in place.

Phishing

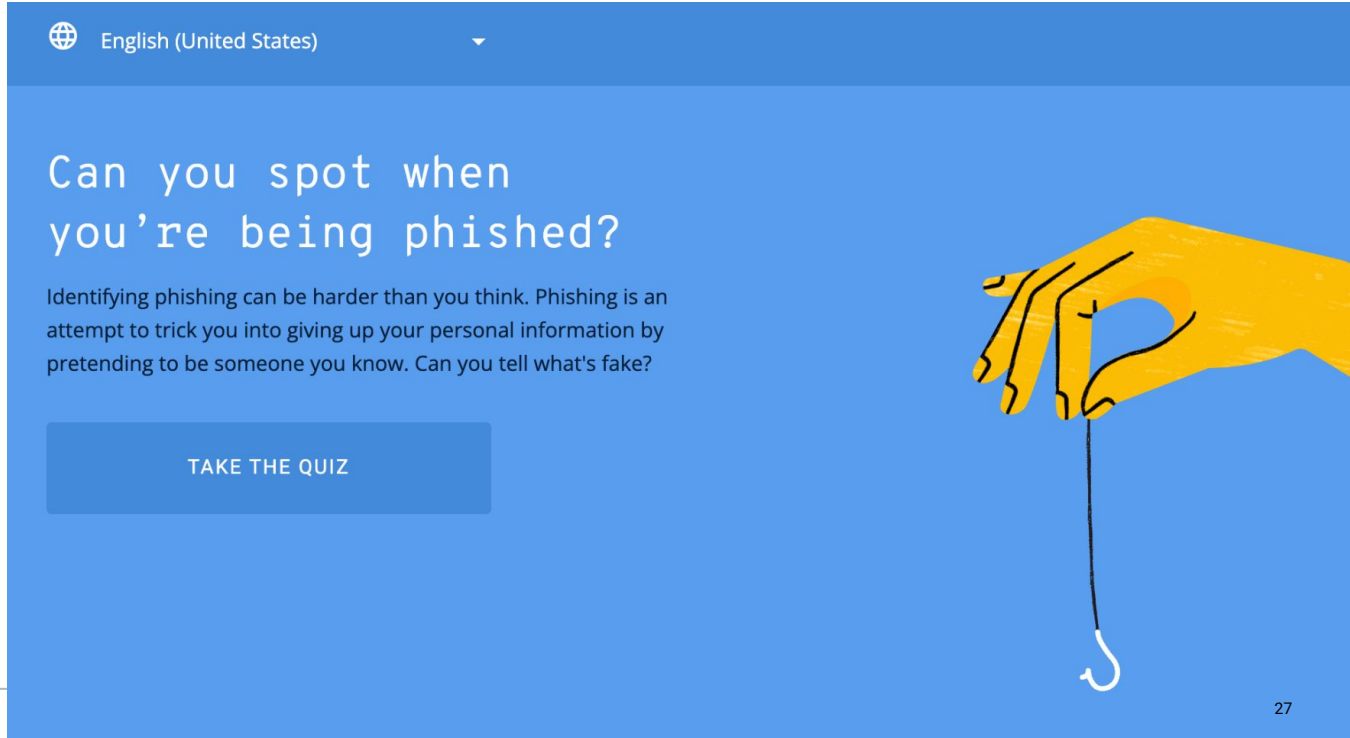
If an email asks you to do something that's not traditionally part of your job or that's possibly risky, it's always better to confirm the task in person or by another means of contact.

Questions?

Phishing Quiz

It is not logistically feasible to perform a phishing campaign in class.
It is also illegal without written consent.

Instead, we'll practice detecting the difference between authentic and phishing emails with an [online activity created by Google](#).



Valid Accounts, External Remote Services, and Password Guessing

Valid Accounts and External Remote Services

Similar to a real attack, many different tactics may be attempted to gain access to a target during a penetration test.

Valid Accounts and External Remote Services

Another way of gaining initial access is by finding a VPN configuration file belonging to the target and logging into the VPN with stolen credentials.

This method leverages two techniques from MITRE:

Valid Accounts

The attacker uses real user accounts to gain access.

Remote Services

The attacker uses remote services such as VPN to try and gain access from outside of the target's network.

Valid Accounts and External Remote Services

In one of our previous OSINT activities, we tried to find subdomains for megacorpone.com.

- Suppose that during this process, we discovered an additional subdomain, vpn.megacorpone.com, that directly handles VPN connections and configurations for the MegaCorpOne domain.
- We accessed this site and determined that it contains a login portal asking for a user id and password.
- If a pen tester is able to supply correct credentials, they will be able to log in to the portal and download the VPN configuration file.

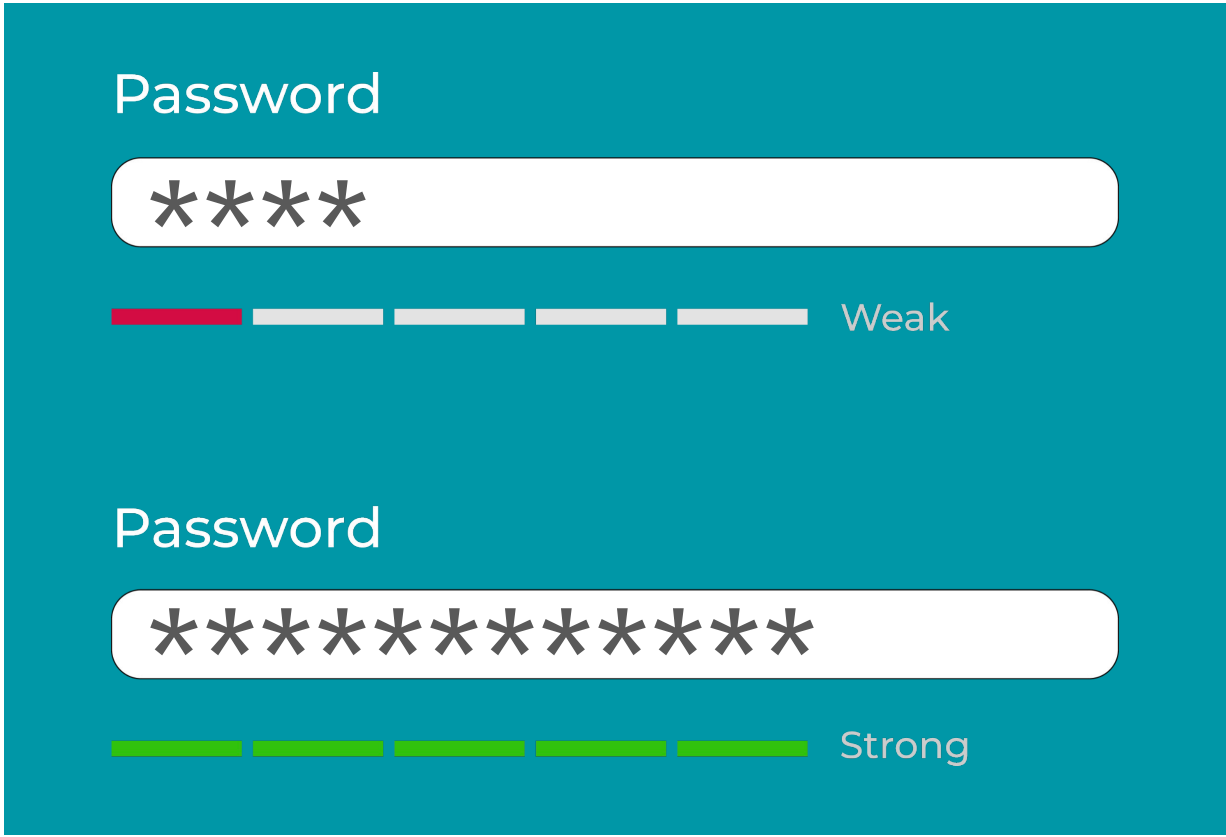
How do we determine what credentials to use to try and gain access to the target?

Valid Accounts and External Remote Services

While it's recommended that users and administrators create complex passwords, they often do not.

Due to this vulnerability, it is not uncommon for pen testers to attempt and succeed at logging into accounts using weak, commonly used passwords.

The method they would apply is called **password guessing**.



Password guessing is the systematic method of guessing passwords to obtain access into a target.

Can you guess the most commonly used password in 2021?

The most common password is

123456

You can visit this website for a list of the other most commonly used passwords.

Password Guessing

Many common passwords include the following:

Variants of “password”	(P@ssw0rd, pa$$w0rd, etc.)
SeasonYear	(Winter2020, Summer2021)
The user’s own username or variants of it	(bob, b0b, a$hl3y, etc.)

This information can help pen testers succeed in correctly guessing a user’s password.

Password guessing has also been used in high profile breaches such as the **SolarWinds hack**.

During this attack, threat actors used password guessing to breach their targets.

Summary

We've covered the following concepts:

Concept	Definition	Tactic Used
Initial access	A MITRE tactic covering methods for gaining access into a target's system.	
Phishing	The most commonly used initial access method. It leverages human error by crafting misleading and convincing fraudulent emails.	**Typosquatting** is a common tactic used with phishing, in which an attacker will register a fraudulent domain similar to a legitimate one.
Remote services through valid accounts	An initial access method where the attacker uses real user accounts to gain access through a remote service, such as VPN.	Can be used in conjunction with **password guessing**, as users often have weak and commonly used passwords.

Questions?

Activity: Accessing Remote Services though Valid Accounts

In this activity, you will use the usernames that you acquired in Day 1 to log in to the VPN via password guessing.

Once in, you will run a shell script that will log you in to the internal network.

Suggested Time:

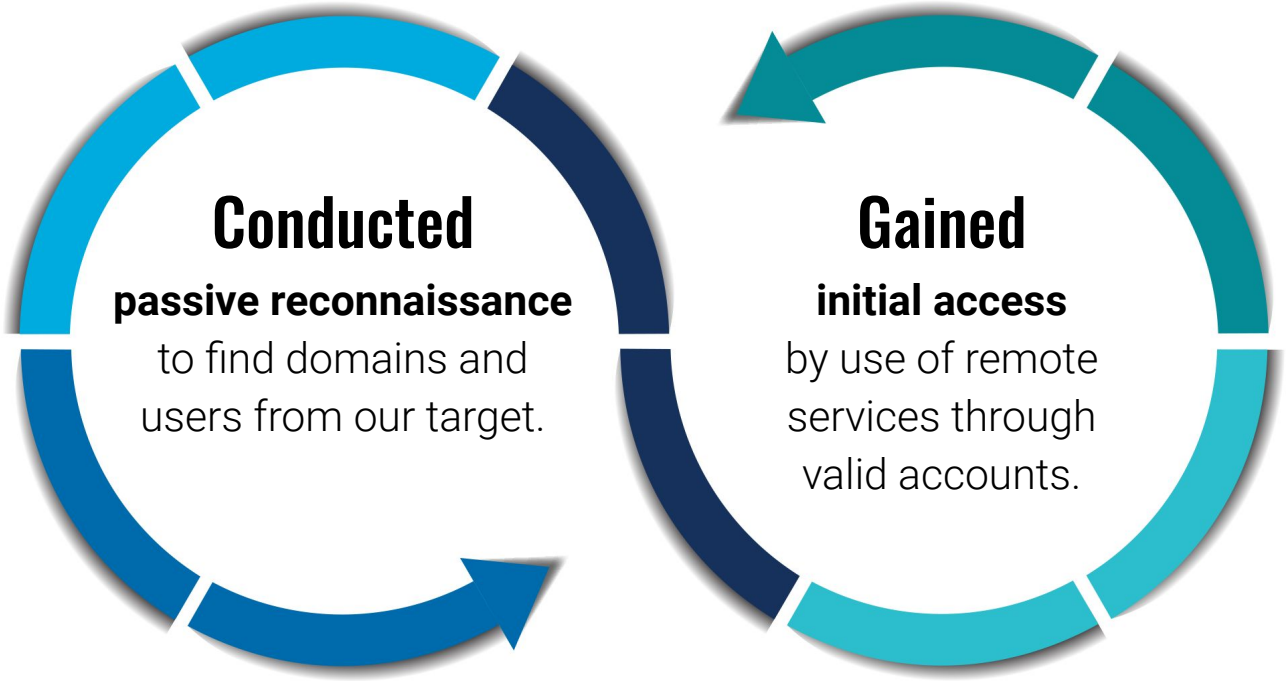
Time’s Up! Let’s Review.

Questions?

Scanning and Internal Reconnaissance

Scanning and Internal Reconnaissance

So far we have:



Internal Reconnaissance

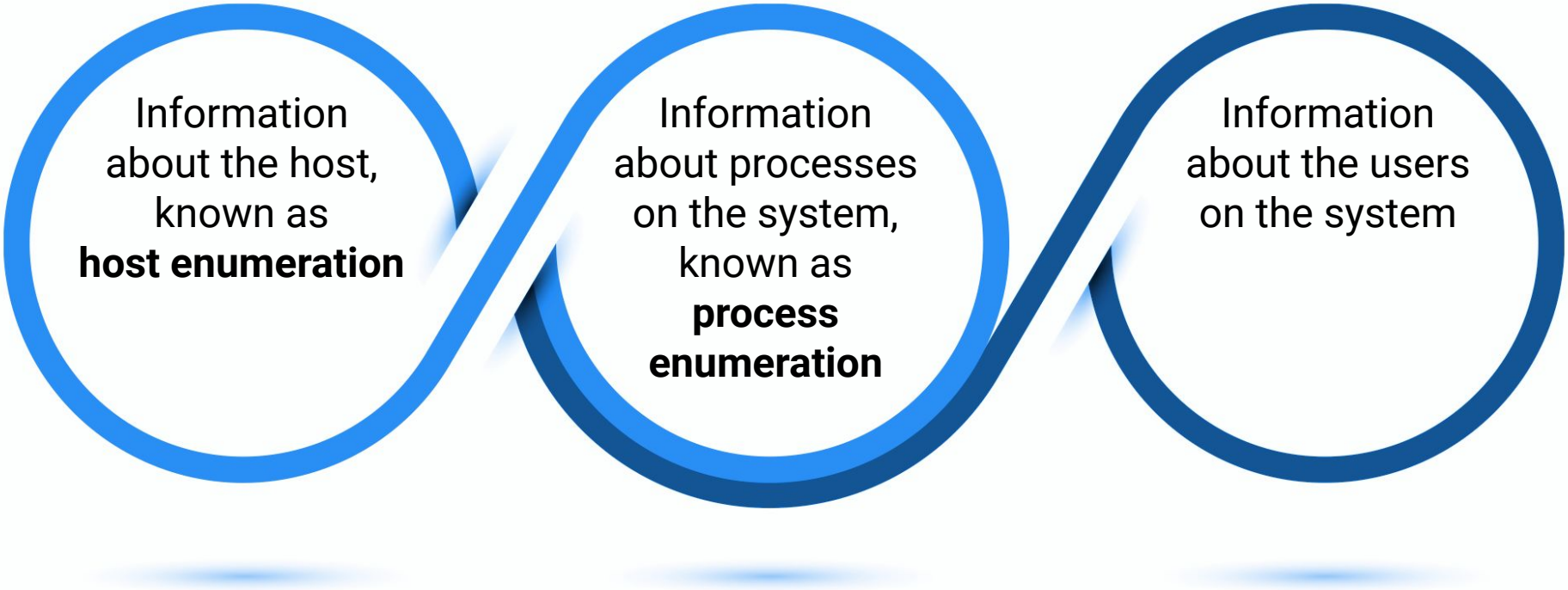
Now, we'll perform reconnaissance inside the internal network, known as **active reconnaissance**, in order to reveal which devices are on the network and what potential new targets await.

We call this **active reconnaissance** because we are directly interacting with our target.

We can also call it **internal reconnaissance** because it's conducted internally within the target.

Internal Reconnaissance

Inside the network, we can gather the following:



We can more aggressively gather information through a process called scanning.

Scanning is the second phase of pen testing. Scanning uses tools to gather information such as network information and potential vulnerabilities.

While we will scan our target from inside their network, scanning can also be conducted externally and before initial access.

Reporting

Post Exploitation

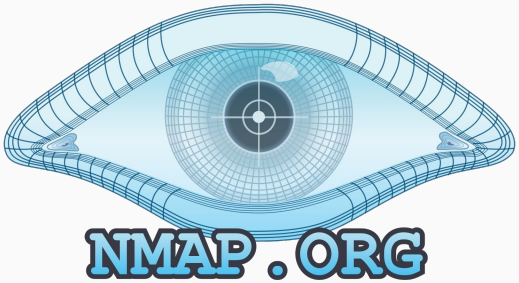
Exploitation

Scanning

Planning and Reconnaissance

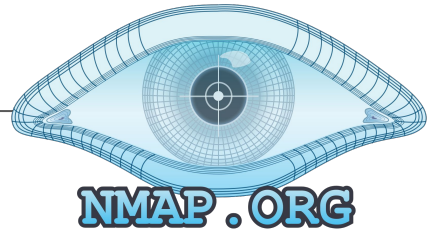
Phase 2: Scanning

The following tools are often used to conduct scanning:



We will explore the scanning phase by revisiting the tool **Nmap**.

About Nmap



Nmap is a popular scanning tool that we covered in the Networking units.

Nmap excels at identifying which ports are open, the services behind those ports, and their versions.

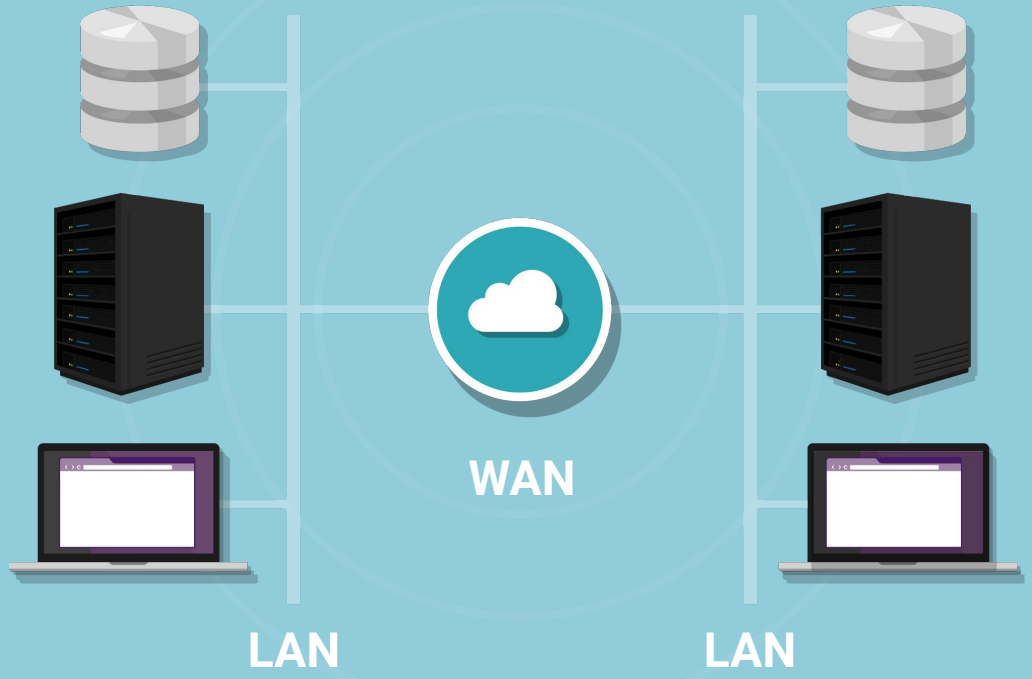
Nmap also has additional functionality, which we will explore in a later activity.

Using Nmap, we will search the machines on the network for any potentially vulnerable services that are outdated or could potentially be abused, e.g., brute forcing SSH logins.

Scanning and Internal Reconnaissance

It’s important to identify the purpose of the machines on the network. For example:

- A properly set-up network has several virtual LANs (VLANs) with different purposes, e.g., servers on one, workstations on another.
- Identifying high-value targets (secret-storing servers, domain controllers, etc.) is important, as they’re often an end-game target.
- Servers often have less security software on them than user workstations, because businesses focus on preventing attackers from gaining initial access.



Nmap and Zenmap Demonstration

In the following demonstration, we will:

01

Use Nmap to perform a port scan on an internal network.

02

Introduce a GUI alternative to Nmap called Zenmap.

03

Use Zenmap to perform a port scan and highlight the additional features offered.

Instructor Demonstration

Nmap and Zenmap

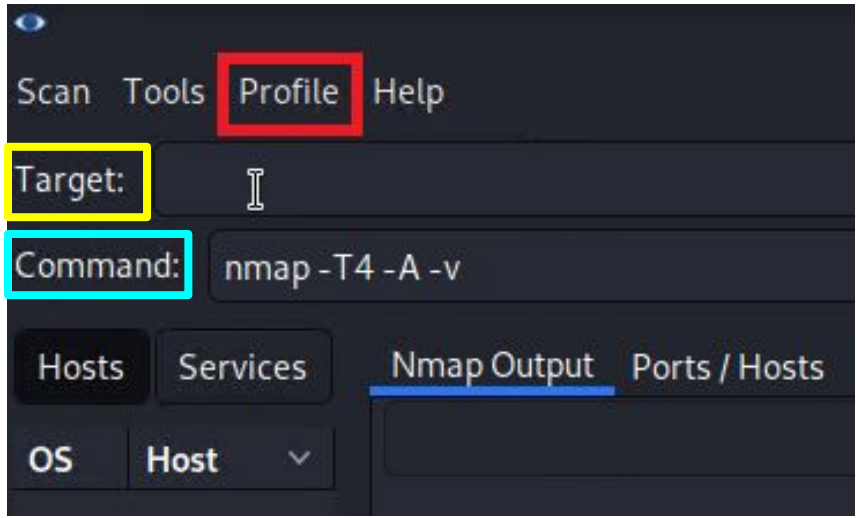
Nmap and Zenmap demonstration

The Zenmap interface includes:

Target: Where we input a hostname or IP address. CIDR notation is also accepted.

Profile: A drop-down menu which contains several pre-built scans. These can be changed and edited. You can also create custom profiles.

Command: Shows the Nmap command being run. This will update automatically if we change or edit a profile.



Summary

Scanning is the second phase of a pen testing engagement. Scanning uses tools to gather information such as network information and potential vulnerabilities.

- While we scanned our target from inside the network, scanning is often conducted externally and before initial access.

Nessus, **Hping**, and **Nmap** are tools that we often use to conduct scanning.

Zenmap is the GUI version of Nmap. It provides an easy-to-use tool to automate scanning tasks.

NSEs (Nmap scripting engines) are scripts that are commonly used to test whether a service is vulnerable to an exploit.

Questions?

Activity: Zenmap

In this activity, you will use Zenmap and NSE scripts to build out a profile in order to perform a scan on a certain machine on the network.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Vulnerability Scanning

NSE Scripts vs. Vulnerability Scanning

While NSE has its advantages, it also has disadvantages when compared to other vulnerability scanners.

NSE is not fully comprehensive, meaning many vulnerabilities are not covered.

NSE cannot perform a large number of scans simultaneously.

NSE is most efficient when performing single host scans.

NSE is most useful when doing basic information gathering or enumeration tasks.

Vulnerability Scanning

Vulnerability scanners such as **Nessus** can be used to identify vulnerabilities and create inventories of all interconnected systems.

Vulnerability Scanning

Most vulnerability scanners will attempt to log into systems using default passwords or other credentials in order to establish a more detailed picture of the network infrastructure.

After establishing an inventory list, vulnerability scanners check each item against one or more databases of known vulnerabilities. This identifies which items are associated with specific threats.

Pen Testing vs. Vulnerability Scanning

Vulnerability testing often gets confused with penetration testing. While similar, they have distinct differences:

Vulnerability scanning

Identifies systems that have known vulnerabilities.

- Scans use a database of known vulnerabilities.
- Vulnerabilities are rated based on the severity level.
- Vulnerabilities are given a Common Vulnerability Scoring System (CVSS) score.

Penetration testing

Attempts to identify weaknesses that can be exploited, such as:

- Specific system configurations
- Organizational processes and practices

Pen Testing vs. Vulnerability Scanning

For these reasons, vulnerability scanning is often found more during security audits rather than penetration tests. Unfortunately, companies often do not understand the differences between the two and sometimes think a vulnerability scan passes as a penetration test when they're actually very different.

Vulnerability Scanning and Nessus

A vulnerability scanner, such as Nessus, is an application that identifies vulnerabilities and creates inventory of all interconnected systems. These include the following:

- Servers
- Containers
- Desktops
- Firewalls
- Laptops
- Switches
- Virtual machines
- Printers

Instructor Demonstration

Nessus


Break

SearchSploit

SearchSploit

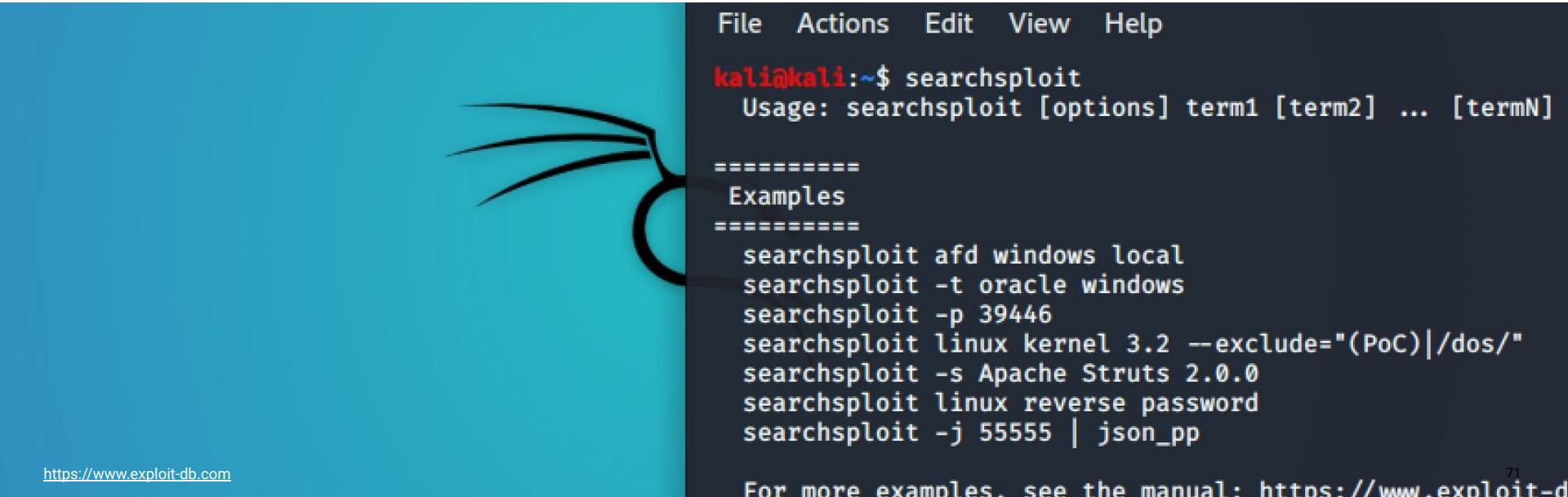
Through our Nmap scans, we've found several services on several machines on the network.

These services and their versions can quickly be searched for any vulnerabilities and exploits written for them.

SearchSploit

Now, we will use a tool called **SearchSploit** to locally store a library of exploit information, as well as the scripts needed to execute the exploits, on our Kali machine.

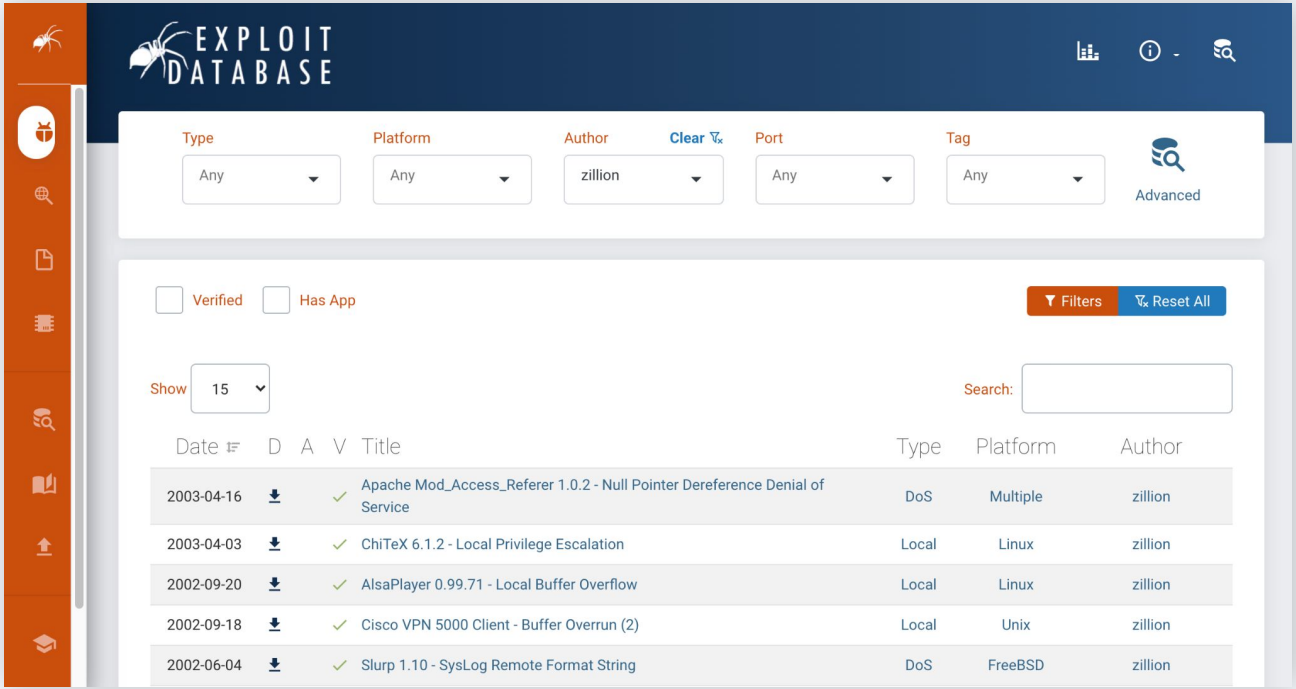
Exploit Database (Exploit-DB) is a popular online database that contains publicly disclosed exploits, cataloged according to their **Common Vulnerability and Exposure (CVE)** identifiers.



https://www.exploit-db.com

SearchSploit

Exploit-DB's catalog of exploits is constantly updated as software developers patch their systems.

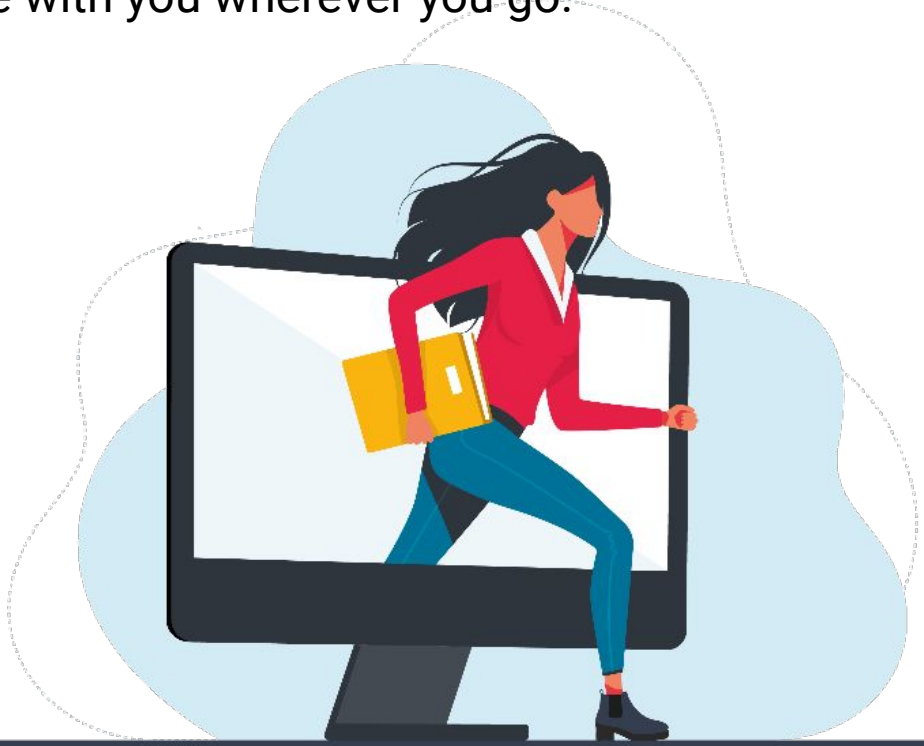


SearchSploit Overview

SearchSploit is a command-line utility for Exploit-DB that allows you to take an offline copy of the Exploit Database with you wherever you go.

Security professionals can perform detailed offline searches of hundreds of exploit scripts through their local copy of the repository.

This capability is useful if you are working on a security assessment with an air-gapped, segregated network that lacks internet connectivity.

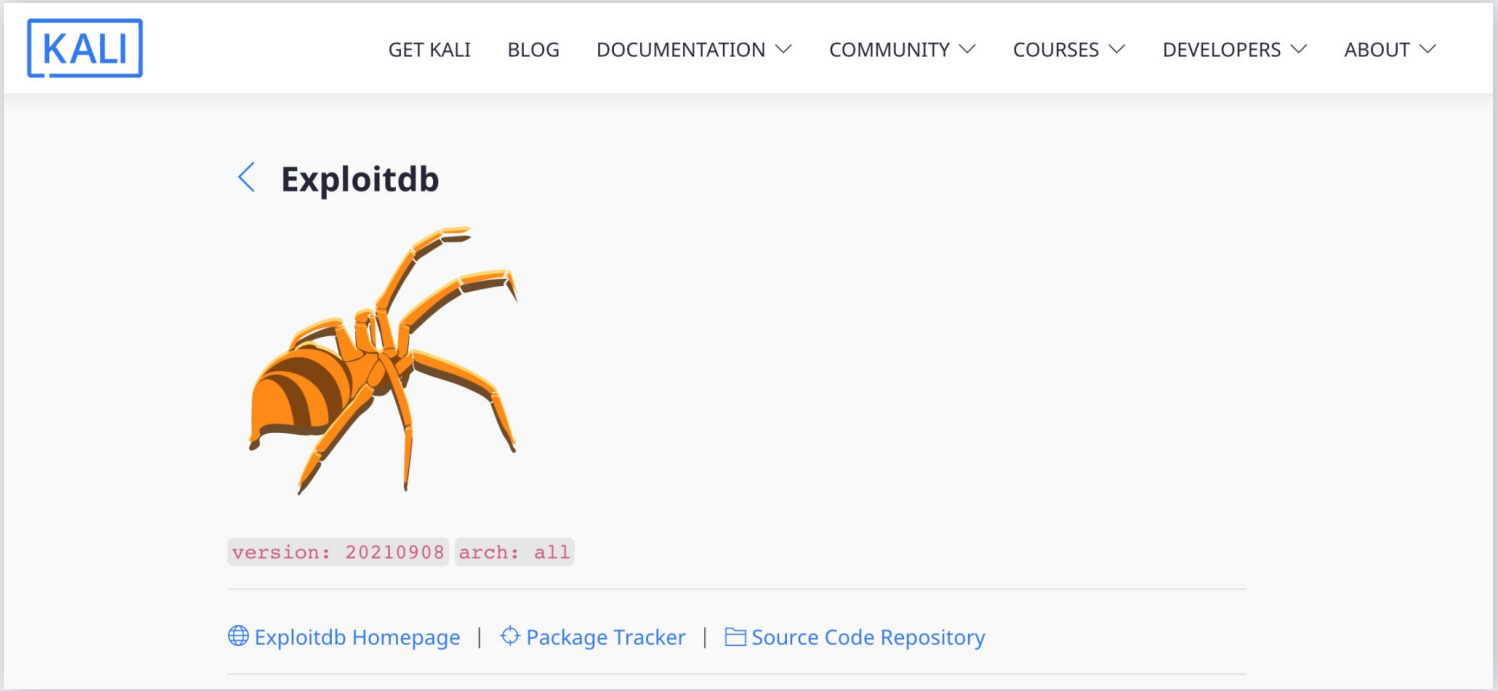


SearchSploit Overview

SearchSploit, as indicated by its name, will search for all exploits and shell code contained within the Exploit-DB repository.

SearchSploit Overview

SearchSploit comes preinstalled on Kali Linux, but should be updated on a weekly basis and prior to each use.



SearchSploit Demonstration

In this demonstration, we will:

01 Run through some basic help commands that are useful when searching for exploit scripts.

02 Discuss the various file formats associated with SearchSploit exploit scripts.

03 Break down the command syntax for the typical SearchSploit command.

Instructor Demonstration

SearchSploit

Summary

SearchSploit is a command-line utility for Exploit-DB that allows you to take an offline copy of the entire Exploit Database with you wherever you go.

Security professionals can perform detailed offline searches of hundreds of exploit scripts from Exploit-DB using the locally checked-out copy of the online repository.

SearchSploit comes preinstalled on Kali Linux and should be updated regularly.

Questions?

Exploitation with Shells

Shells

A common goal of exploitation is to obtain access to the remote machine.

Exploited access to the machine is typically granted in the form of terminal access, which is referred to as a **shell**.

A shell is a **terminal**. Opening a terminal on your Kali machine is opening a “shell” on your own machine.

A **remote shell** is opened on a remote computer on the network.

Shells

We will cover two types of shells today:

Bind shell

The remote host opens a port for the current host to connect to.

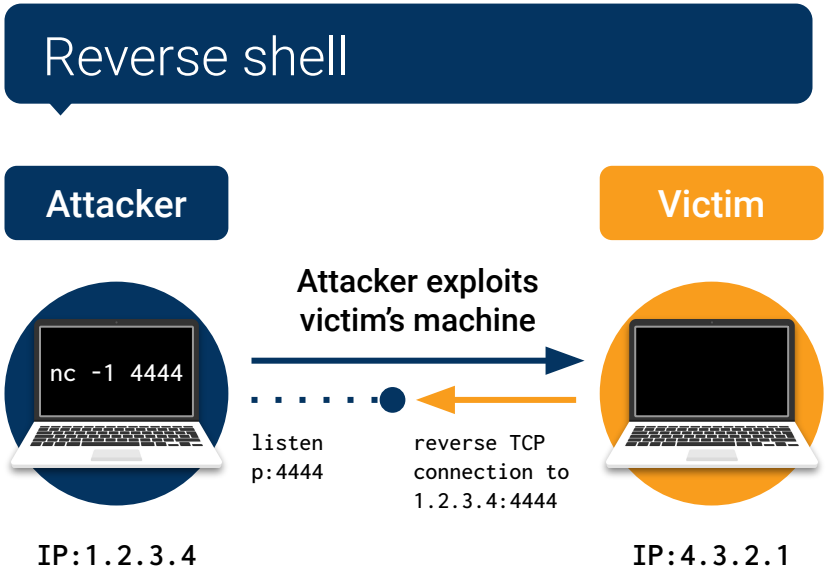
The current, local host then connects to that remote host's port.

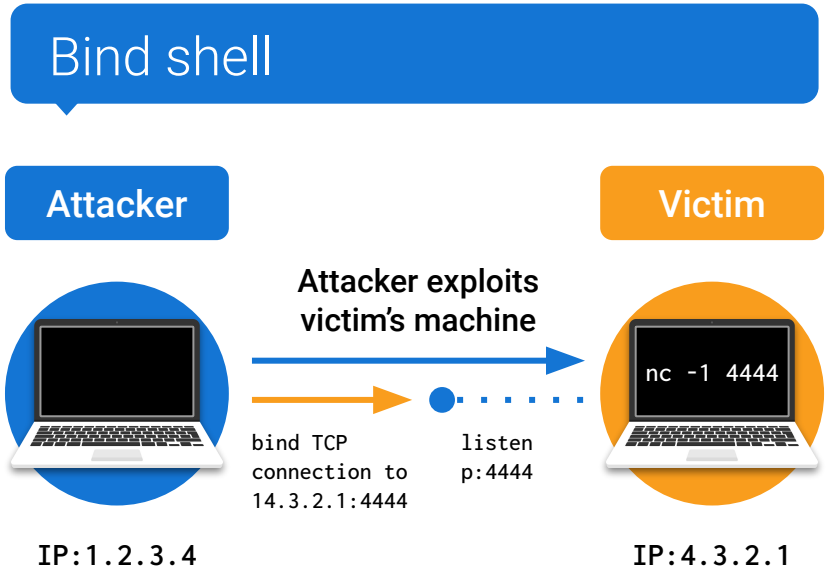
Reverse shell

The remote host connects back to a port on the local host.

Shells

The advantage of a reverse shell over a bind shell is that egress (exit) ports are more commonly open than ingress (enter) ports. This means that a remote host will have fewer firewall issues connecting back to a port on the local host. This also circumvents NATing.





Shells

Next, we'll use a tool called **Netcat** to demonstrate bind and reverse shells.

Netcat is commonly referred to as the "Swiss army knife" of networking tools, because it can assist with many security and admin activities.

Instructor Demonstration

Shells

Activity: Exploitation

In this activity, you will use a SearchSploit exploit to determine whether you can gain shell access on the host.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?


The End