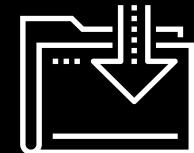




Initial Access and Internal Recon

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.



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

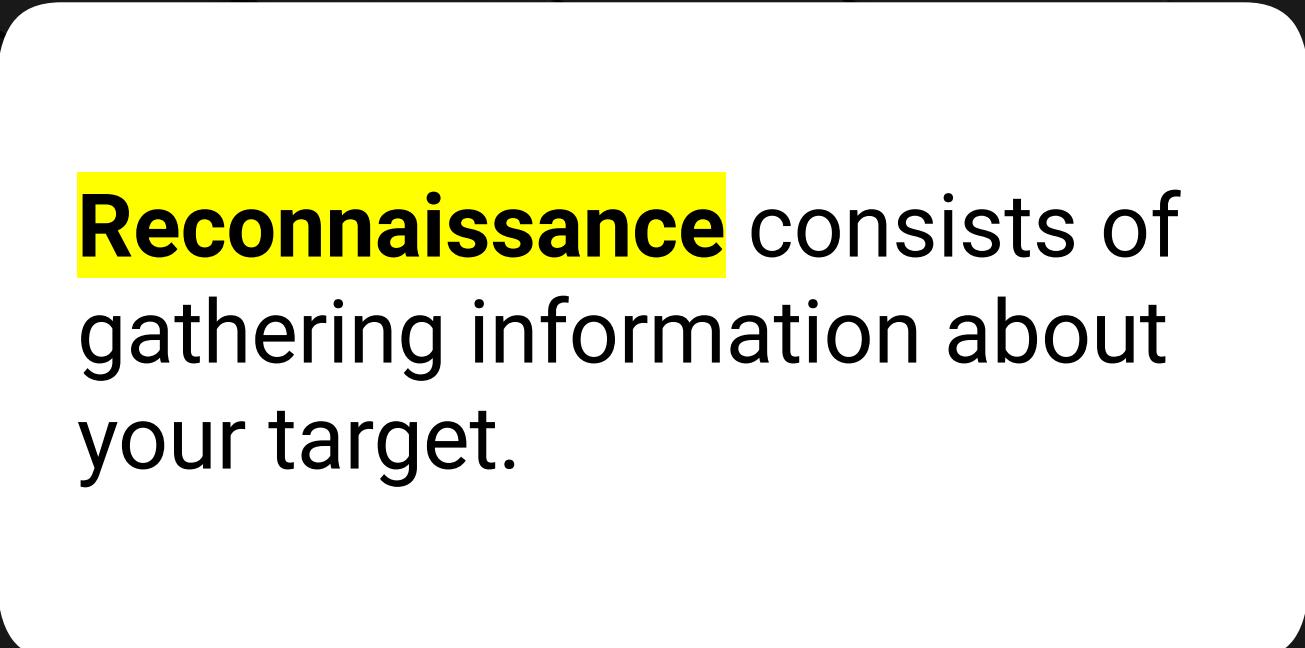
Post exploitation

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

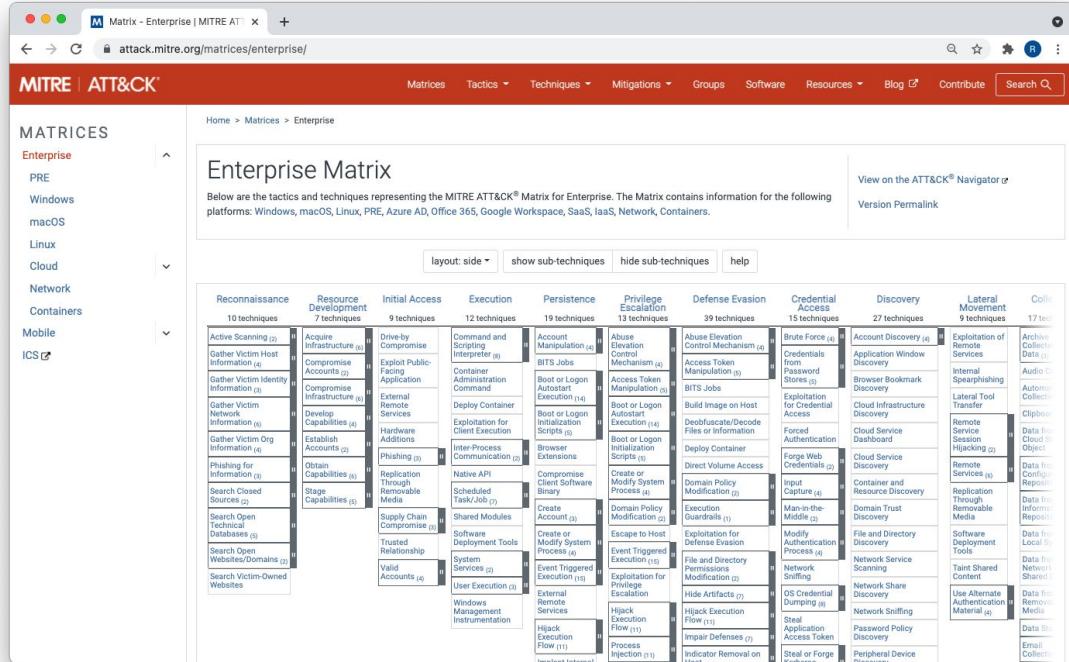
Active Recon

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.



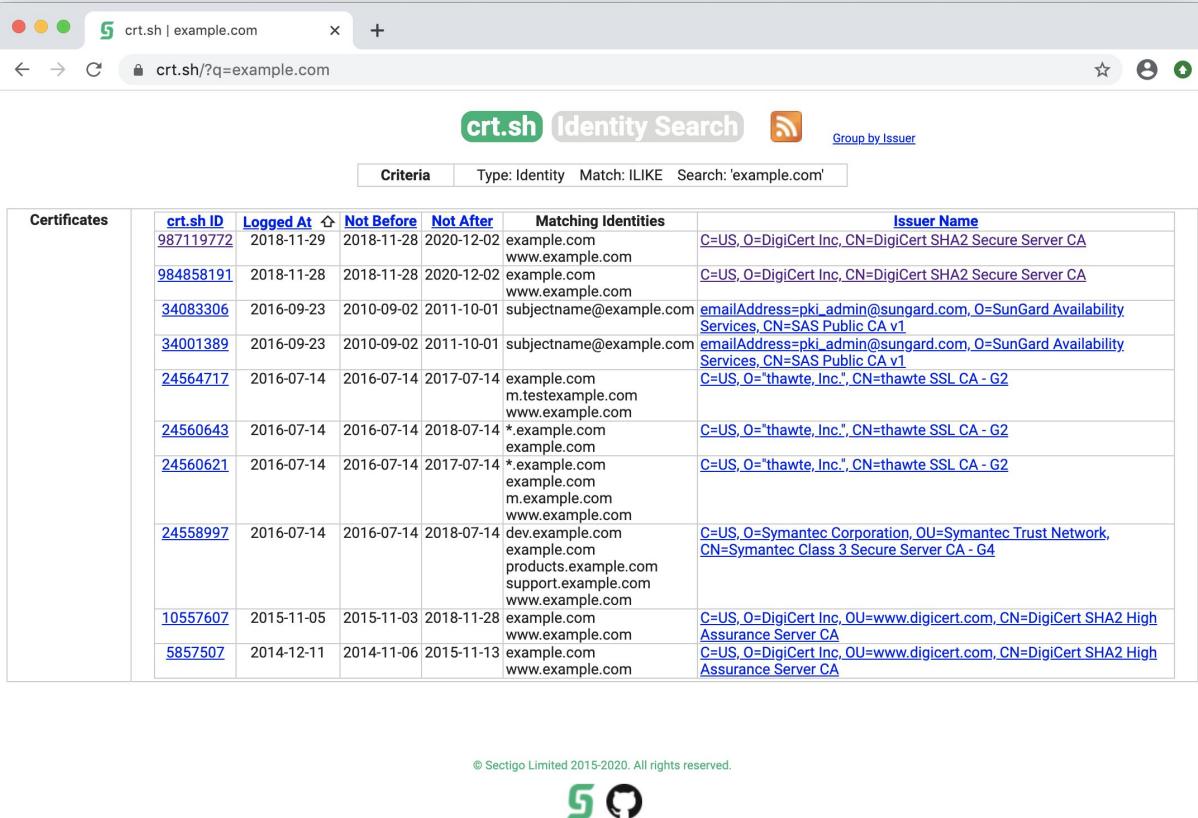
We will use this matrix as a reference for the TTPs that we will conduct throughout the next two weeks of class.

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.



The screenshot shows a web browser window with the address bar containing 'crt.sh | example.com'. The main content is titled 'crt.sh Identity Search' with a subtitle 'Group by Issuer'. Below this is a search bar with the query 'example.com'. A table titled 'Certificates' lists various SSL/TLS certificates issued to 'example.com' and its subdomains. The columns include 'crt.sh ID', 'Logged At', 'Not Before', 'Not After', 'Matching Identities', and 'Issuer Name'. The 'Matching Identities' column shows multiple entries for each certificate, such as 'example.com', 'www.example.com', and various subdomains like 'm.testexample.com'. The 'Issuer Name' column lists the certificate authorities, including DigiCert, SunGard Availability Services, and thawte. The table has 10 rows, each corresponding to a different certificate entry.

Certificates	crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
	987119772	2018-11-29	2018-11-28	2020-12-02	example.com www.example.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	984858191	2018-11-28	2018-11-28	2020-12-02	example.com www.example.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	34083306	2016-09-23	2010-09-02	2011-10-01	subjectname@example.com	emailAddress=pki_admin@sungard.com, O=SunGard Availability Services, CN=SAS Public CA v1
	34001389	2016-09-23	2010-09-02	2011-10-01	subjectname@example.com	emailAddress=pki_admin@sungard.com, O=SunGard Availability Services, CN=SAS Public CA v1
	24564717	2016-07-14	2016-07-14	2017-07-14	example.com m.testexample.com www.example.com	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
	24560643	2016-07-14	2016-07-14	2018-07-14	*.example.com example.com	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
	24560621	2016-07-14	2016-07-14	2017-07-14	*.example.com example.com m.example.com www.example.com	C=US, O="thawte, Inc.", CN=thawte SSL CA - G2
	24558997	2016-07-14	2016-07-14	2018-07-14	dev.example.com example.com products.example.com support.example.com www.example.com	C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4
	10557607	2015-11-05	2015-11-03	2018-11-28	example.com www.example.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
	5857507	2014-12-11	2014-11-06	2015-11-13	example.com www.example.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA

© Sectigo Limited 2015-2020. All rights reserved.



Day 1 Recap

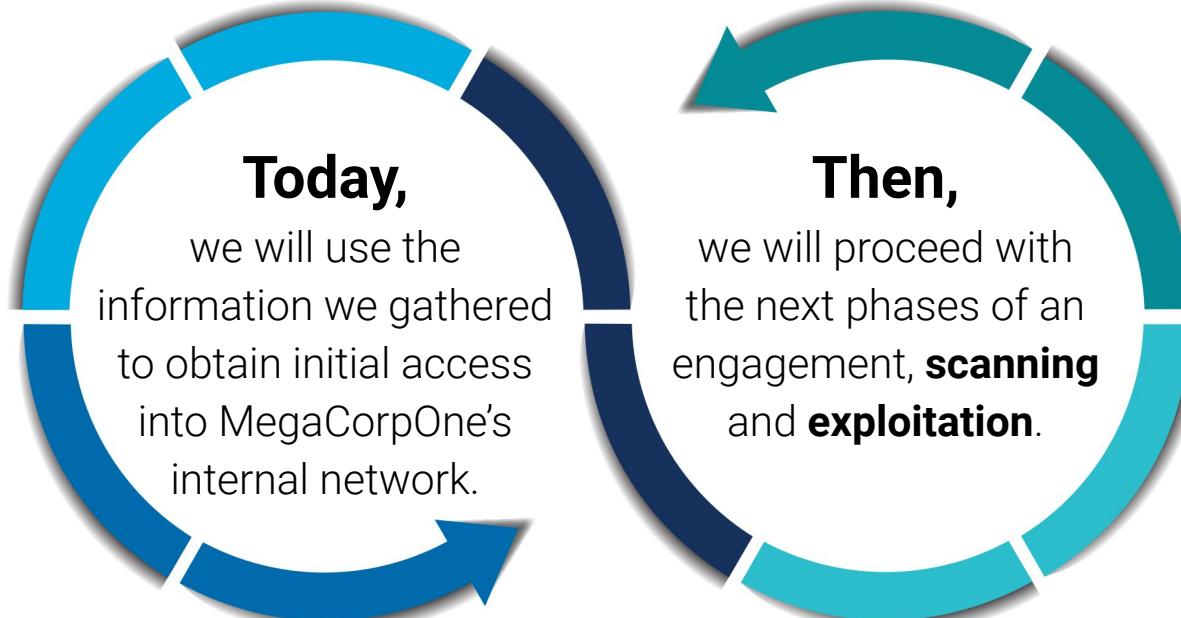
Shodan.io is a reconnaissance website that conducts port scanning across the entire internet and catalogs the results for quick searching.

The screenshot shows the Shodan.io interface. At the top, there's a search bar with the IP address "93.184.216.34" and a map of Massachusetts. Below the map, the host information for "93.184.216.34" is displayed, including the city (Norwell), country (United States), organization (Verizon Business), ISP (Verizon Business), last update (2020-04-24T17:31:40.422234), and ASN (AS15133). On the right, there are sections for "Ports" (showing 80 and 443) and "Services" (listing 80, tcp, and http). The "Services" section also displays the response headers for port 80:

```
HTTP/1.1 200 OK
Age: 354667
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Fri, 24 Apr 2020 17:31:40 GMT
Etag: "3147526947+ident"
Expires: Fri, 01 May 2020 17:31:40 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
Server: ECS (bsa/EB11)
Vary: Accept-Encoding
X-Cache: HIT
Content-Length: 1256
```

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

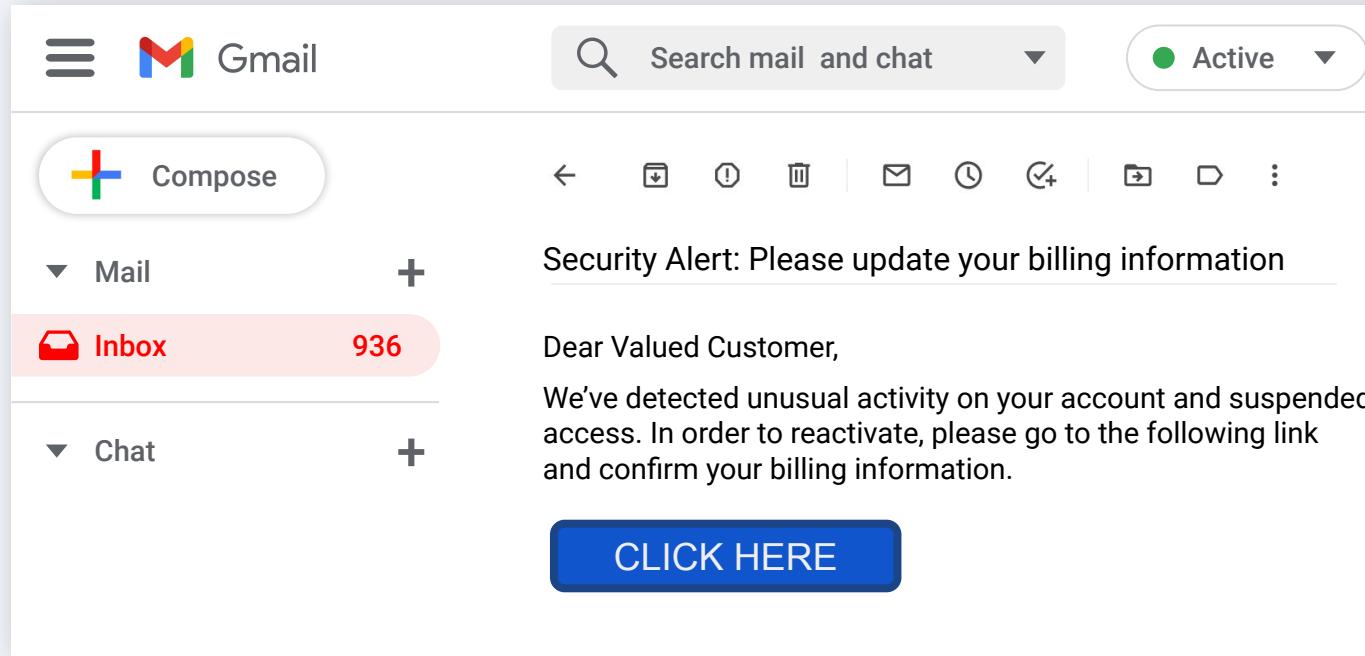
Gaining Initial Access

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.

Gaining Initial Access

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

The screenshot shows the MITRE ATT&CK website. The top navigation bar includes links for Matrices, Tactics, Techniques, Mitigations, Groups, Software, Resources, Blog, and Contribute. A search bar is also present. On the left, a sidebar titled 'TACTICS' lists various tactics under 'Enterprise': Reconnaissance, Resource Development, **Initial Access**, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The main content area shows the 'Initial Access' tactic page. The breadcrumb navigation indicates the path: Home > Tactics > Enterprise > Initial Access. The title 'Initial Access' is displayed, followed by a description: 'The adversary is trying to get into your network.' Below this, a detailed description explains that Initial Access consists of techniques using various entry vectors to gain a foothold within a network, mentioning spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access can allow for continued access or be limited-use. To the right, a box contains the tactic's ID (TA0001), creation date (17 October 2018), and last modified date (19 July 2019). A 'Version Permalink' link is also provided. At the bottom, a table titled 'Techniques' shows two entries: T1189 (Drive-by Compromise) and T1190 (Exploit Public-). The table has columns for ID, Name, and Description.

ID	Name	Description
T1189	Drive-by Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.
T1190	Exploit Public-	Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program

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.

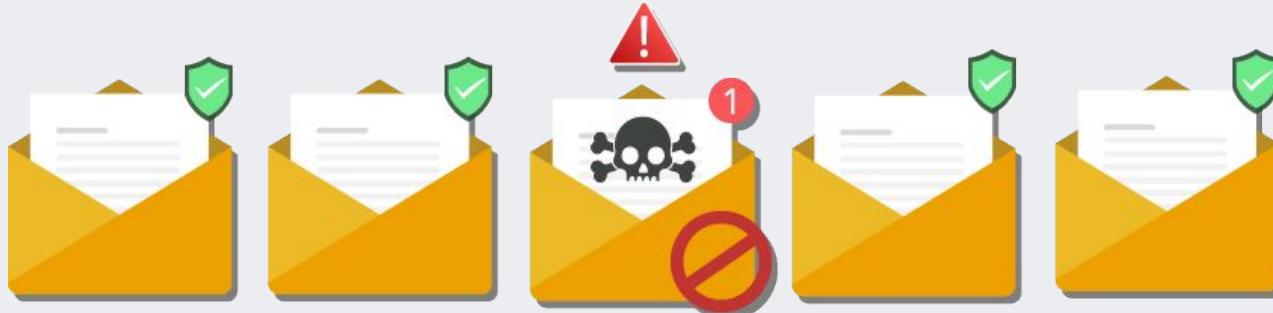


Other times,
the email contains a malicious link
that will install malware or a
backdoor on the victim's computer.

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 logically 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](#).

The screenshot shows a web page titled "Can you spot when you're being phished?". The page is in English (United States). The main text explains that phishing is an attempt to trick users into giving up personal information by pretending to be someone they know. A blue button at the bottom left says "TAKE THE QUIZ". To the right, there is a stylized illustration of a yellow hand holding a blue circle, with a black string or cord hanging from the bottom of the circle.

English (United States) ▾

Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ

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.

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.



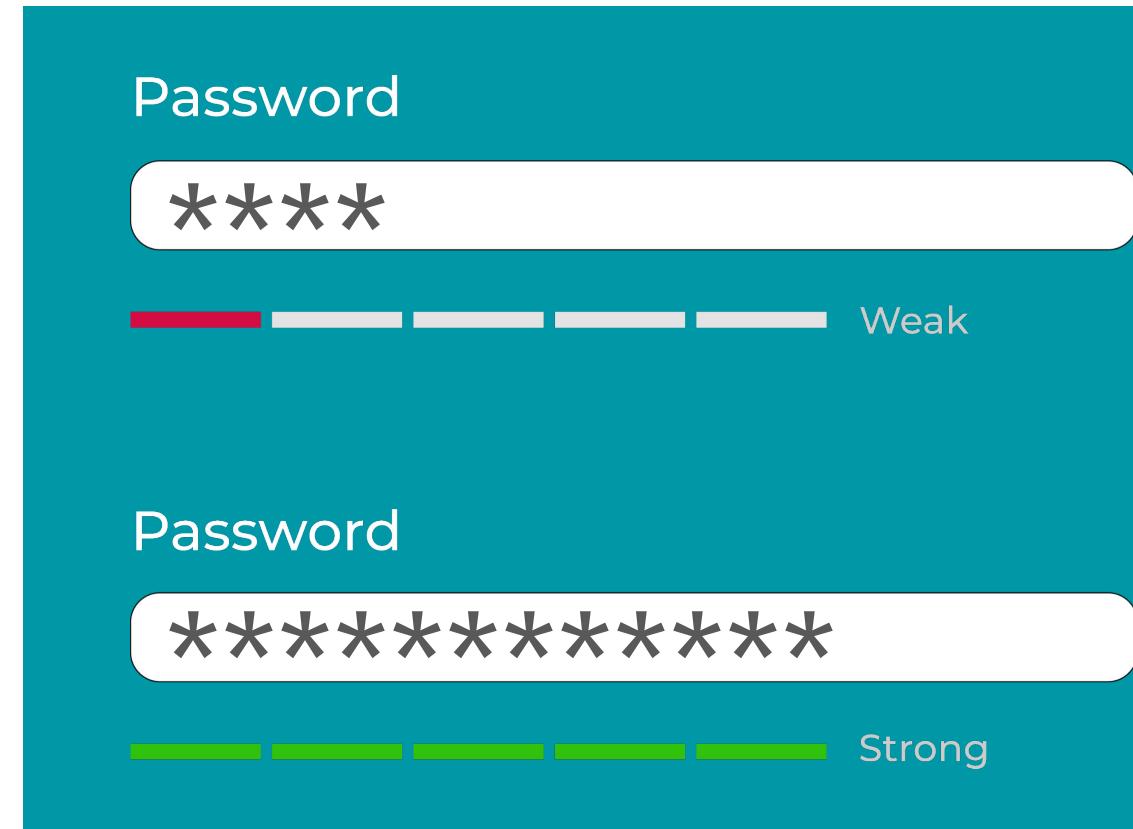
How do we determine what credentials to use to try and gain access to the target?

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\$h13y, 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 through 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.

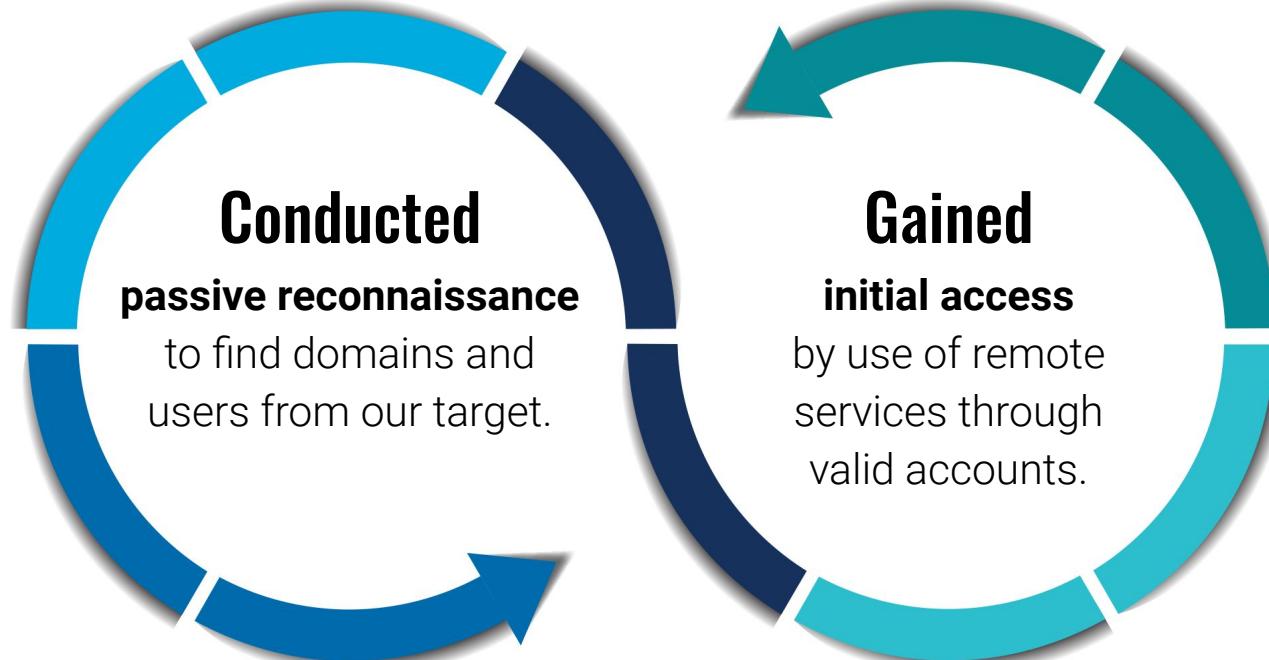
Questions?



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.

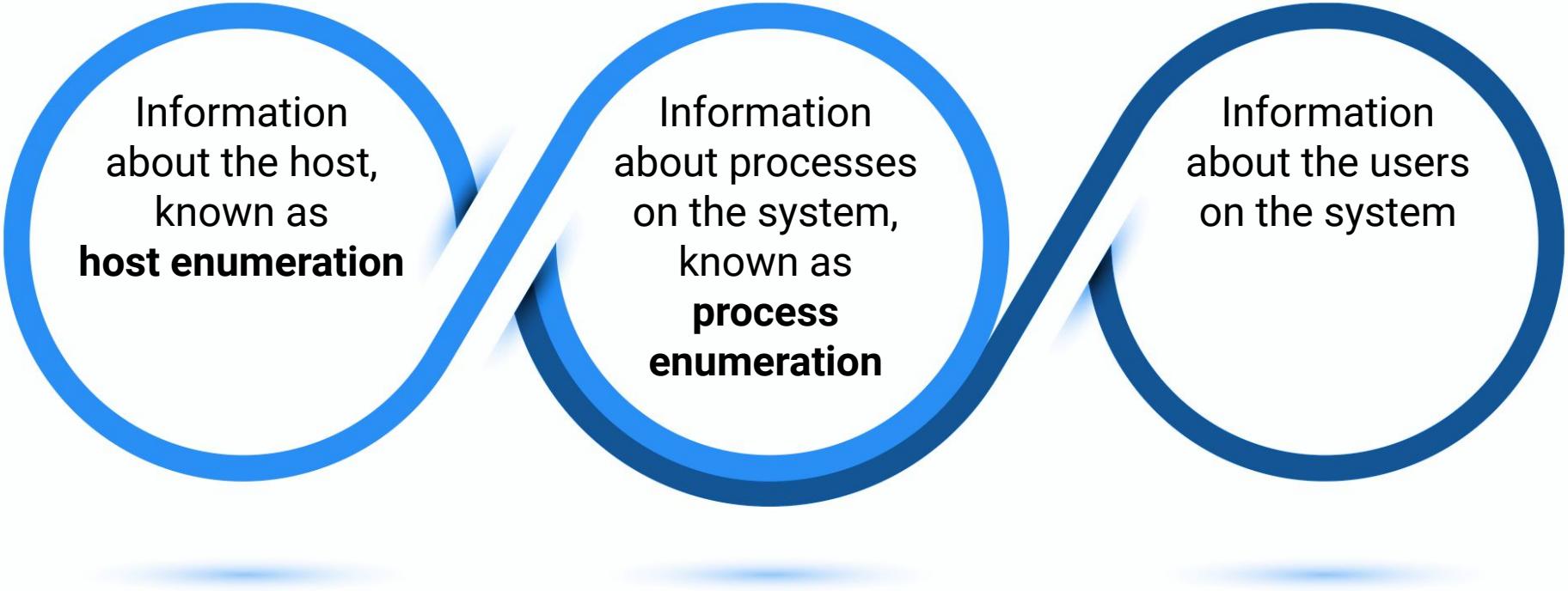


We call this **active reconnaissance** because we are directly interacting with our target.

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:



Information about the host, known as **host enumeration**

Information about processes on the system, known as **process enumeration**

Information about the users on the system



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.



Planning and
Reconnaissance

Scanning

Exploitation

Post Exploitation

Reporting

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

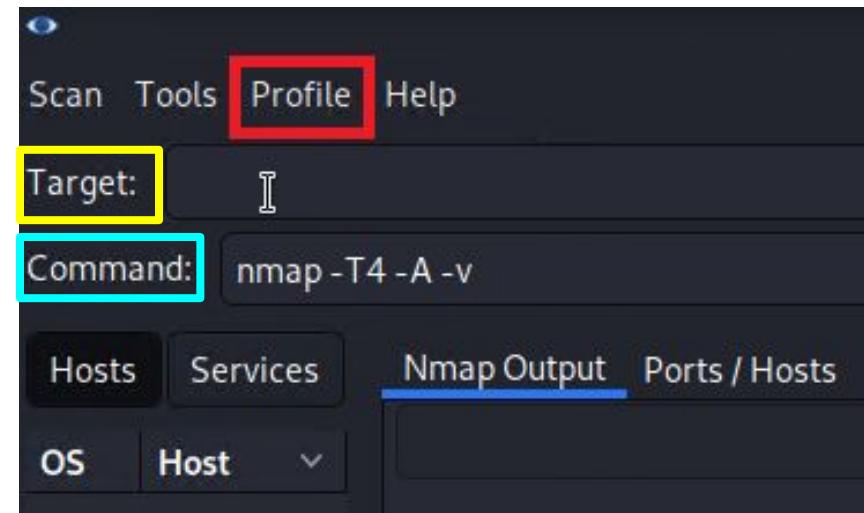
Nmap and Zenmap demonstration

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.

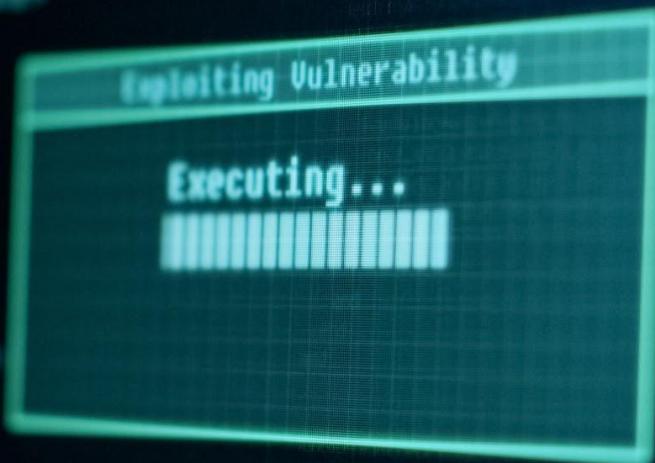
Vulnerability Scanning

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

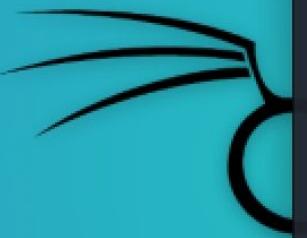
SearchSploit

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.



```
File Actions Edit View Help
kali㉿kali:~$ searchsploit
Usage: searchsploit [options] term1 [term2] ... [termN]
=====
Examples
=====
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
searchsploit linux kernel 3.2 --exclude="(PoC)|/dos/"
searchsploit -s Apache Struts 2.0.0
searchsploit linux reverse password
searchsploit -j 55555 | json_pp
```

SearchSploit

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

The screenshot shows the Exploit Database search interface. The top navigation bar includes a logo of a spider, the text "EXPLOIT DATABASE", and icons for search, refresh, and help. On the left, there is a vertical sidebar with orange icons for various functions like search, upload, and export. The main search area has filters for Type (Any), Platform (Any), Author (zillion), Port (Any), and Tag (Any). It also includes checkboxes for Verified and Has App, and buttons for Filters and Reset All. The results table lists five vulnerabilities with columns for Date, Title, Type, Platform, and Author. The first exploit is a DoS attack on Apache Mod_Access_Referrer.

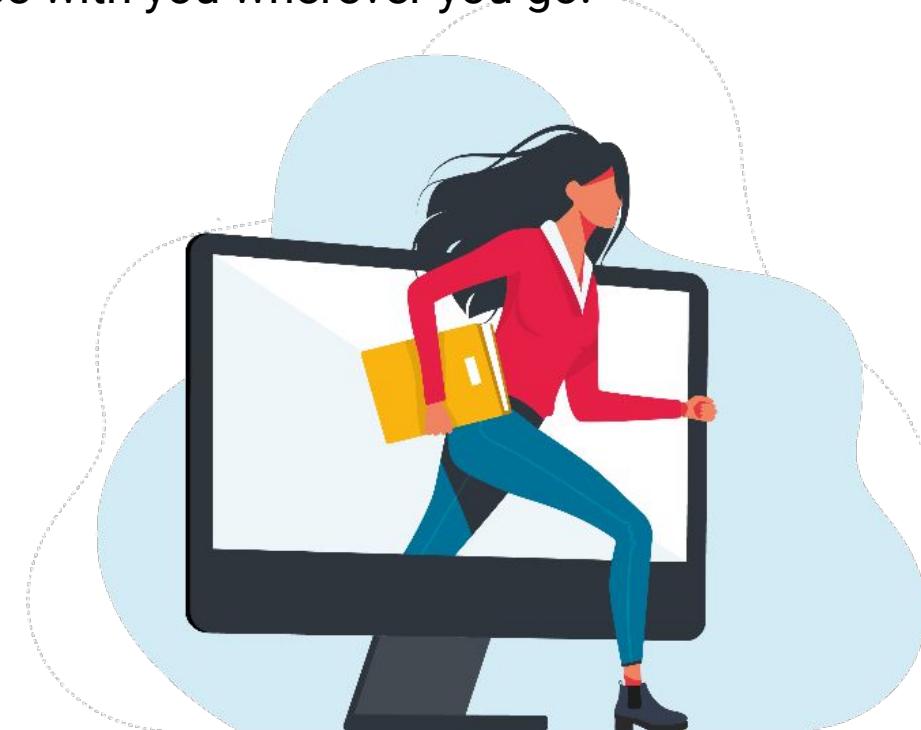
Date	Title	Type	Platform	Author
2003-04-16	Apache Mod_Access_Referrer 1.0.2 - Null Pointer Dereference Denial of Service	DoS	Multiple	zillion
2003-04-03	ChiTeX 6.1.2 - Local Privilege Escalation	Local	Linux	zillion
2002-09-20	AlsaPlayer 0.99.71 - Local Buffer Overflow	Local	Linux	zillion
2002-09-18	Cisco VPN 5000 Client - Buffer Overrun (2)	Local	Unix	zillion
2002-06-04	Slurp 1.10 - SysLog Remote Format String	DoS	FreeBSD	zillion

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.

The screenshot shows the Kali Linux website with a navigation bar at the top. The navigation items include 'GET KALI', 'BLOG', 'DOCUMENTATION ▾', 'COMMUNITY ▾', 'COURSES ▾', 'DEVELOPERS ▾', and 'ABOUT ▾'. The main content area features a large orange and yellow striped spider icon. Above the icon, the text 'Exploitdb' is displayed with a left arrow icon. Below the icon, there is a small text box containing 'version: 20210908 arch: all'. At the bottom of the page, there are links to 'Exploitdb Homepage', 'Package Tracker', and 'Source Code Repository'.

KALI

GET KALI BLOG DOCUMENTATION ▾ COMMUNITY ▾ COURSES ▾ DEVELOPERS ▾ ABOUT ▾

Exploitdb

version: 20210908 arch: all

Exploitdb Homepage | Package Tracker | Source Code Repository

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.

Reverse shell

Attacker



IP: 1.2.3.4

Victim



IP: 4.3.2.1

Attacker exploits
victim's machine

listen
p:4444

reverse TCP
connection to
1.2.3.4:4444

Bind shell

Attacker



IP: 1.2.3.4

Victim



IP: 4.3.2.1

Attacker exploits
victim's machine

bind TCP
connection to
14.3.2.1:4444

listen
p:4444

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*