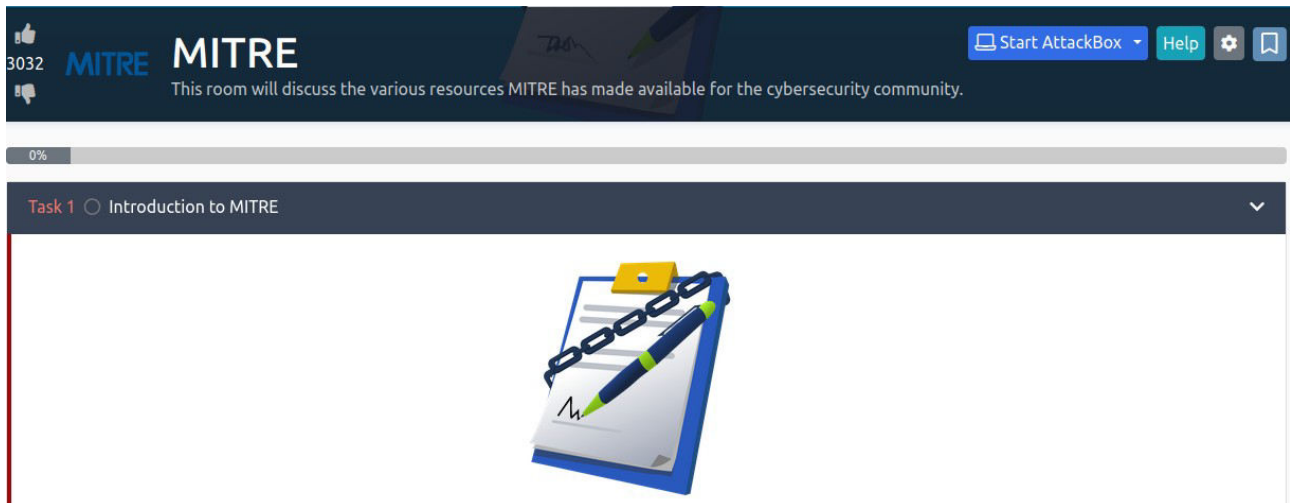




Eric Mwenda

MITRE

<https://tryhackme.com/p/Ericm>



Introduction to MITRE.

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

MITRE is usually associated with CVE (Common Vulnerabilities and Exposure). MITRE researches in many areas, outside of cybersecurity, for the 'safety, stability, and well-being of our nation.' These areas include artificial intelligence, health informatics, space security, to name a few.

Basic Terminology.

APTs

APT stands for Advanced Persistent Threat. This threats can be carried out by a team/group or even a country that engages in long-term attacks against Organizations and countries.

APT groups are quite common but can only be detected with the right implementations in place.

TTP

TTP stands for Tactic, Techniques and Procedures.

- Tactic is the adversary's goal and objective.
- Techniques is how the adversary achieves the goal or objective.
- Procedures is how the technique is executed.

ATT&CK®

From this section I learnt that MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations..

I also got to learn that MITRE began to address the need to record and document common TTPs (Tactics, Techniques and Procedures) that APT (Advanced Persistent Threat) groups used against enterprise Windows networks in 2013. This started with an internal project known as FMX (Fort Meade Experiment). Within this project, selected security professionals were tasked to emulated adversarial TTPs against a network, and data was collected from the attacks on this network. The

gathered data helped construct the beginning pieces of what we know today as the ATT&CK® framework.

Phishing – Phishing is a technique that frauds practice of sending emails or other messages targeting reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

All forms of phishing are electronically delivered using social engineering.

Targeted phishing is know as spear phishing.

Questions.

1. Besides Blue teamers, who else will use the ATT&CK Matrix? (Red Teamers, Purpe Teamers, SOC Managers?)

ANS: Red Teamers. A red team is a group that pretends to be an enemy, attempts a physical or digital intrusion against an organization then reports back so that the organization can improve their defenses.

Answer the questions below

Besides Blue teamers, who else will use the ATT&CK Matrix? (Red Teamers, Purpe Teamers, SOC Managers?)

Red Teamers

Correct Answer

2. What is the ID for this technique? **ANS: T1566.**

Home > Techniques > Enterprise > Phishing

Phishing

Sub-techniques (4)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003, T1566.004

① **Tactic:** Initial Access

① **Platforms:** Google Workspace, Linux, Office 365, SaaS, Windows, macOS

What is the ID for this technique?

T1566

Correct Answer

Hint

3. Based on this technique, what mitigation covers identifying social engineering techniques?

ANS: User Training. Social engineering training gives people the tools they need to recognize threats, which grooms more discerning, responsible employees who are better equipped to protect both themselves and their organization.

Based on this technique, what mitigation covers identifying social engineering techniques?

User Training

Correct Answer

4. What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas) **ANS: Application Log,File,Network Traffic**

What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas)

Application Log,File,Network Traffic

Correct Answer

5. What groups have used spear-phishing in their campaigns? (format: group1,group2) **ANS: Axiom,GOLD SOUTHFIELD**

ID	Name	Description
G0001	Axiom	Axiom has used spear phishing to initially compromise victims. ^{[6][9]}
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines. ^[10]
S0009	Hikit	Hikit has been spread through spear phishing. ^[9]
S1073	Royal	Royal has been spread through the use of phishing campaigns including "call back phishing" where victims are lured into calling a number provided through email. ^{[11][12][13]}

6. Based on the information for the first group, what are their associated groups? **ANS: Group 72**

October 14, 2014



Security

Threat Spotlight: Group 72

Talos Group

Based on the information for the first group, what are their associated groups?

Group 72

Correct Answer

7. What software is associated with this group that lists phishing as a technique? **ANS: Hikit**

- Hikit (aka Matrix RAT aka Gaolmay)

8. What is the description for Hikit software?

ANS: Hikit is malware that has been used by Axiom for late-stage persistence and exfiltration after the initial compromise.

What is the description for this software?

that has been used by Axiom for late-stage persistence and exfiltration after the initial compromise.

Correct Answer

9. This group overlaps (slightly) with which other group?

ANS: Winnti Group

This group overlaps (slightly) with which other group?

Winnti Group

Correct Answer

10. How many techniques are attributed to this group?

ANS: 15

How many techniques are attributed to this group?

15

Correct Answer

Hint

CAR Knowledge Base.

CAR – This represents Cyber Analytics Repository

CAR defines a data model that is leveraged in its pseudocode representations but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics.

Questions

1. What tactic has an ID of TA0003? **ANS: persistence**

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

[Home](#) > [Tactics](#) > [Enterprise](#) > [Persistence](#)

Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

ID: TA0003

Created: 17 October 2018

Last Modified: 19 July 2019

[Version](#) [Permalink](#)

2. What is the name of the library that is a collection of Zeek (BRO) scripts? **ANS: BZAR**

About 25,900 results (0.29 seconds)

BZAR

Currently, the only library is BZAR, a collection of Zeek (Bro) scripts looking primarily at SMB and RPC traffic.

3. What is the name of the technique for running executables with the same hash and different names? **ANS: Masquerading**

4. Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique? **ANS: Unit Tests**

The screenshot shows a Firefox web browser window with the URL <https://tryhackme.com/room/mitre>. The page content includes a section titled "Answer the questions below" with four quiz questions. The first question is "What tactic has an ID of TA0003?" with the answer "persistence". The second question is "What is the name of the library that is a collection of Zeek (BRO) scripts?" with the answer "BZAR". The third question is "What is the name of the technique for running executables with the same hash and different names?" with the answer "Masquerading". The fourth question is "Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique?" with the answer "Unit Tests". Each question has a "Correct Answer" button and a "Hint" button. At the bottom of the page, there are two task cards: "Task 5 ○ MITRE Engage" and "Task 6 ○ MITRE D3FEND".

(The techniques highlighted in purple are the analytics currently in CAR)

Let's look at another analytic to see a different implementation, [CAR-2014-11-004: Remote PowerShell Sessions](#).

Under Implementations, a pseudocode is provided and an EQL version of the pseudocode. EQL (pronounced as 'equal'), and it's an acronym for Event Query Language. EQL can be utilized to query, parse, and organize Sysmon event data. You can read more about [this here](#).

Eql, EQL native

EQL version of the above pseudocode.

```
process where subtype.create and
(process_name == "usmprovhost.exe" and parent_process_name == "svchost.exe")
```

To summarize, CAR is a great place for finding analytics that takes us further than the Mitigation and Detection summaries in the ATT&CK® framework. This tool is not a replacement for ATT&CK® but an added resource.

Answer the questions below

What tactic has an ID of TA0003?

persistence Correct Answer Hint

What is the name of the library that is a collection of Zeek (BRO) scripts?

BZAR Correct Answer Hint

What is the name of the technique for running executables with the same hash and different names?

Masquerading Correct Answer Hint

Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique?

Unit Tests Correct Answer Hint

Task 5 ○ MITRE Engage

Task 6 ○ MITRE D3FEND

MITRE Engage

The screenshot shows the MITRE Engage Matrix website. The URL is <https://engage.mitre.org/matrix/tphase=operate>. The page features a navigation bar with 'Home', 'Tools', 'Why Engage?', and 'Engage with Us'. Below the navigation bar, there are three main sections: 'PREPARE', 'OPERATE' (highlighted in blue), and 'UNDERSTAND'. Under the 'OPERATE' section, there are three filter boxes: 'Filter by ATT&CK® Groups' (with a 'Group' dropdown), 'Filter by ATT&CK® Tactics' (with a 'Tactic' dropdown), and 'Filter by ATT&CK® Techniques' (with a 'Technique' dropdown). Below the filters, there are three tables: 'Expose', 'Affect', and 'Elicit'. The 'Expose' table has two columns: 'Collect' and 'Detect'. The 'Affect' table has three columns: 'Prevent', 'Direct', and 'Disrupt'. The 'Elicit' table has two columns: 'Reassure' and 'Motivate'. Each table contains a list of activities. Below the tables, there is a small thumbnail image of the Engage Matrix website and a small icon in the bottom right corner.

Expose	
Collect	Detect
API Monitoring	Introduced Vulnerabilities
Network Monitoring	Lures
Software Manipulation	Malware Detonation
System Activity Monitoring	Network Analysis

Affect		
Prevent	Direct	Disrupt
Baseline	Attack Vector Migration	Isolation
Hardware Manipulation	Email Manipulation	Lures
Isolation	Introduced Vulnerabilities	Network Manipulation
Network Manipulation	Lures	Software Manipulation
Security Controls	Malware Detonation	
	Network Manipulation	
	Peripheral Management	
	Security Controls	
	Software Manipulation	

Elicit	
Reassure	Motivate
Application Diversity	Application Diversity
Artifact Diversity	Artifact Diversity
Burn-In	Information Manipulation
Email Manipulation	Introduced Vulnerabilities
Information Manipulation	Malware Detonation
Network Diversity	Network Diversity
Peripheral Management	Personas
Pocket Litter	

In this section I gained basic knowledge about the Engage Matrix website, which has different categories. This categories are explained as follows:-

1. Prepare – This focuses on a set of operational actions that will lead to your desired outcome (input)
2. Expose – This is when adversaries when they trigger your deployed deception activities
3. Affect – Here is where adversaries by performing malicious actions they impact negatively on operations
4. Elicit – This is gathering information by observing the adversary and learn more about their modus operandi (TTPs)
5. Understand – In this category we have the outcomes of the operational actions (output)

Question

1. Under Prepare, what is ID SAC0002? **ANS: Persona Creation**

The screenshot shows the MITRE Engage web application. The 'Prepare' section is active, displaying a list of activities: Cyber Threat Intelligence, Engagement Environment, Gating Criteria, Operational Objective, **Persona Creation** (highlighted with a red dashed box), Storyboarding, and Threat Model. Below this, a modal window titled 'PERSONA CREATION' (ID: SAC0002) is open, showing the definition: 'Plan and create a fictitious human user through a combination of planted data and revealed behavior patterns.'

Answer the questions below

Under Prepare, what is ID SAC0002?

Persona Creation

Correct Answer

2. What is the name of the resource to aid you with the engagement activity from the previous question? **ANS: PERSONA PROFILE WORKSHEET**

What is the name of the resource to aid you with the engagement activity from the previous question?

PERSONA PROFILE WORKSHEET

Correct Answer

Hint

3. Which engagement activity baits a specific response from the adversary? **ANS: Lures**

Which engagement activity baits a specific response from the adversary?

lures

Correct Answer

4. What is the definition of Threat Model? **ANS: A risk assessment that models organizational strengths and weaknesses**

The screenshot shows a web browser window with the URL <https://tryhackme.com/room/mitre>. The page displays a quiz interface with several questions. The question "What is the definition of Threat Model?" is highlighted with a red box. The correct answer is "A risk assessment that models organizational strengths and weaknesses".

That should be enough of an overview. We'll leave it to you to explore the resources provided to you on this website.

Before moving on, let's practice using this resource by answering the questions below.

Answer the questions below

Under Prepare, what is ID SAC0002?

Persona Creation Correct Answer

What is the name of the resource to aid you with the engagement activity from the previous question?

PERSONA PROFILE WORKSHEET Correct Answer Hint

Which engagement activity baits a specific response from the adversary?

lures Correct Answer

What is the definition of Threat Model?

A risk assessment that models organizational strengths and weaknesses Correct Answer

Task 6 ☐ MITRE D3FEND

Task 7 ☐ ATT&CK® Emulation Plans

Task 8 ☐ ATT&CK® and Threat Intelligence

Task 9 ☐ Conclusion

Created by [tryhackme](#) and [Dex01](#)

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 94402 users are in here and this room is 1174 days old.

MITRE D3FEND

D3FEND stands for Detection, Denial, and Disruption Framework Empowering Network Defense.

The screenshot shows the MITRE D3FEND Matrix website. The header includes the MITRE logo and navigation links: matrix, artifacts, taxonomies, about, resources, contribute, faq, blog. The main title is "DEFEND™ A knowledge graph of cybersecurity countermeasures 0.14.0". Below the title is a search bar labeled "Search D3FEND's 620 Artifacts". The main content is a large matrix of countermeasures organized into columns: Model, Harden, Detect, Isolate, Deceive, Evict, and Restore. Each column contains a list of specific countermeasures.

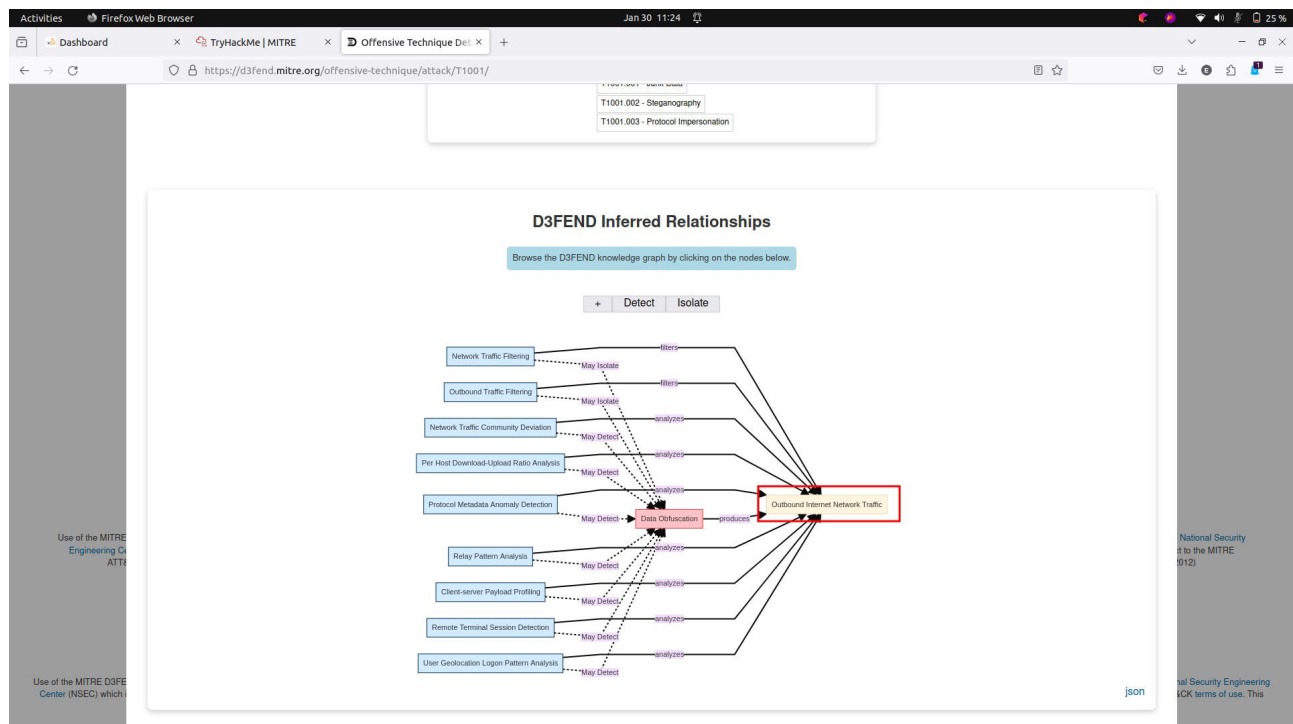
Model	Harden	Detect	Isolate	Deceive	Evict	Restore
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis
Application Configuration Hardening	Biometric Authentication	Message Authentication	Platform Authentication	File Analysis	Identifier Analysis	Message Analysis
Dead Code Elimination	Certificate Pinning	Message Encryption	Platform Encryption	File Analysis	Identifier Analysis	Message Analysis
Exception Handler Pointer Validation	Credential Rotation	Transfer Agent Authentication	Platform Integrity Checking	File Analysis	Identifier Analysis	Message Analysis
Pointer Authentication	Credential Transmission Scoping	Domain Trust Policy	Platform File Permissions	File Analysis	Identifier Analysis	Message Analysis
Process Segment Execution Prevention	Multi-factor Authentication	Domain Trust Policy	Platform File Permissions	File Analysis	Identifier Analysis	Message Analysis
Segment Address Offset Randomization	One-time Password	Domain Trust Policy	Platform File Permissions	File Analysis	Identifier Analysis	Message Analysis
Stack Frame Canary Validation	Strong Password Policy	Domain Trust Policy	Platform File Permissions	File Analysis	Identifier Analysis	Message Analysis
	User Account Permissions	Domain Trust Policy	Platform File Permissions	File Analysis	Identifier Analysis	Message Analysis

Questions.

1. What is the first MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown? **ANS: Data Obfuscation**

The screenshot shows the D3FEND Matrix website interface. The 'ATT&CK Lookup' dropdown menu is open, displaying a list of MITRE ATT&CK techniques. The first technique listed is 'T1001 - Data Obfuscation', which is highlighted in blue. Other techniques visible include T1001.001 - Junk Data, T1001.002 - Steganography, T1001.003 - Protocol Impersonation, T1002 - Data Compressed, T1003 - OS Credential Dumping, T1003.001 - LSASS Memory, T1003.002 - Security Account Manager, T1003.003 - NTDS, T1003.004 - LSA Secrets, T1003.005 - Cached Domain Credentials, T1003.006 - DCSync, T1003.007 - Proc Filesystem, T1003.008 - etc/passwd and etc/shadow, T1004 - Winlogon Helper DLL, T1005 - Data from Local System, and T1006 - Direct Volume Access.

2. In D3FEND Inferred Relationships, what does the ATT&CK technique from the previous question produces? **ANS: Outbound Internet Network Traffic**



Activities Firefox Web Browser Jan 30 11:24

Dashboard TryHackMe | MITRE Offensive Technique Details

https://tryhackme.com/room/mitre

A CSV file with decoy user credentials is placed on a system. The system or network is then monitored to detect any accesses to the decoy files.

Digital Artifact Relationships:
This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

Decoy File → File

As you can see, you're provided with information on what is the technique (definition), how the technique works (how it works), things to think about when implementing the technique (considerations), and how to utilize the technique (example).

Note, as with other MITRE resources, you can filter based on the ATT&CK matrix.

Since this resource is in beta and will change significantly in future releases, we won't spend that much time on D3FEND.

The objective of this task is to make you aware of this MITRE resource and hopefully you'll keep an eye on it as it matures in the future.

We will still encourage you to navigate the website a bit by answering the questions below.

Answer the questions below

What is the first MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown?

Data Obfuscation Correct Answer

In D3FEND Inferred Relationships, what does the ATT&CK technique from the previous question produce?

Outbound Internet Network Traffic Correct Answer Hint

Task 7 ATT&CK® Emulation Plans

Task 8 ATT&CK® and Threat Intelligence

Task 9 Conclusion

Created by tryhackme and Dex01

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 94402 users are in here and this room is 1174 days old.

ATT&CK Emulation Plans

In this section another tool is introduced called: **CTID**
CTID – Stands for Center of Threat-Informed defense.

1. In Phase 1 for the APT3 Emulation Plan, what is listed first? **ANS: C2 Setup**

Activities Firefox Web Browser Jan 30 11:32

Dashboard TryHackMe | MITRE Adversary Emulation Plans

https://attack.mitre.org/resources/adversary-emulation-plans/

MITRE | ATT&CK®

Matrices Tactics Techniques Defenses CTI Resources Benefactors Blog Search

RESOURCES

- Get Started
- Learn More about ATT&CK
- ATT&CK Data & Tools
- FAQ
- Engage with ATT&CK
- Version History
- Legal & Branding

Built on these open threat reports, they have the same limitations. To help with this, we provided a sample way to string the ATT&CK tactics together based on general red teaming experience. To create these plans, the team drilled down on specific APT groups listed in ATT&CK and see what kind of plans could be generated for an operator to emulate those APTs. After reading what capabilities were provided by an APT's tools, we compiled a list of other ways to exhibit the same behavior. We wanted operators to behave generally like a specific adversary (sticking to that adversary's known TTPs and behaviors), but having some latitude in actual implementation. To help with this, we also provided a cheat sheet for commands that can be executed for similar behavior in some of the most commonly used red teaming tools. An example, high-level diagram below highlights one possible way to structure an APT3 emulation plan.

APT 3 Emulation Plan

Approved for Public Release: Distribution Unlimited. Case Number 17-3368. ©2018 The MITRE Corporation. All Rights Reserved.

We will not be going through this for every group on ATT&CK, rather select a subset we feel offer a unique perspective for defenses to be measured. We hope that the community finds use in these prototypes, and builds on them to make ATT&CK actionable. These are living documents that can be updated with newer information, format, or changed for other uses. Please reach out to attack@mitre.org for anything relating to these prototypes.

Emulation Plan Documents

APT3

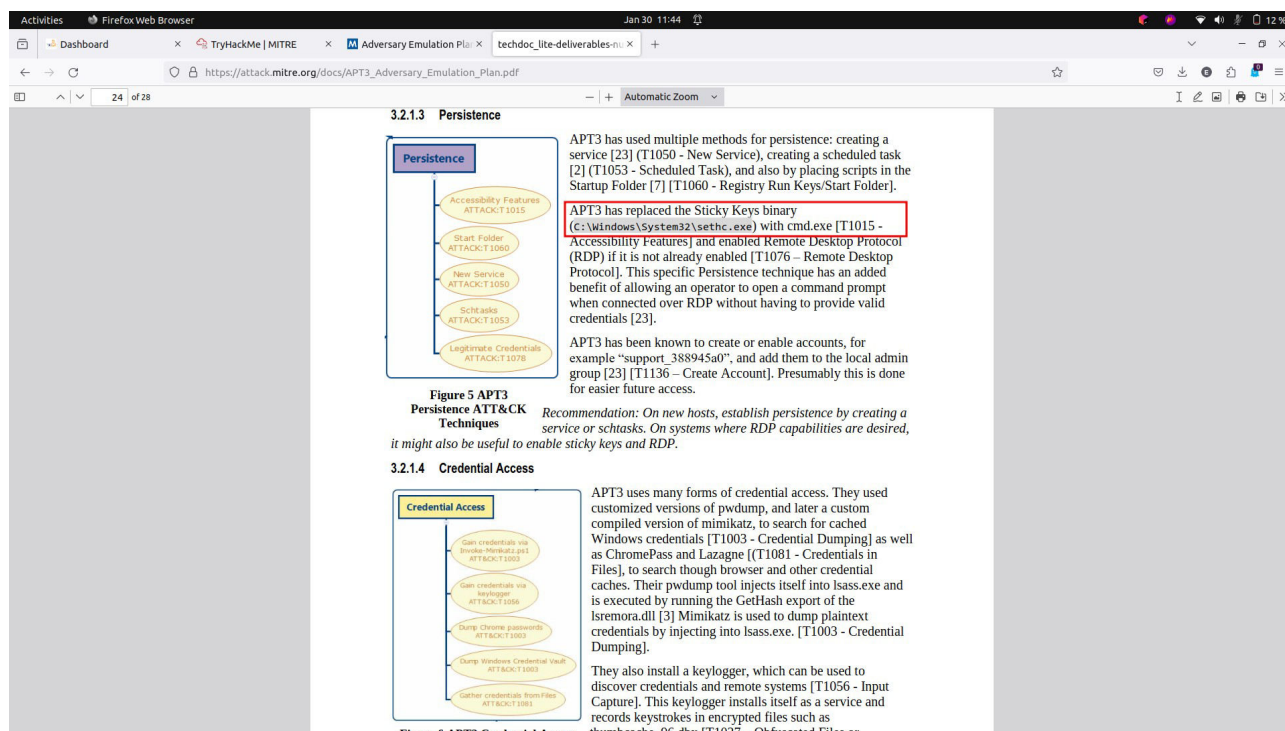
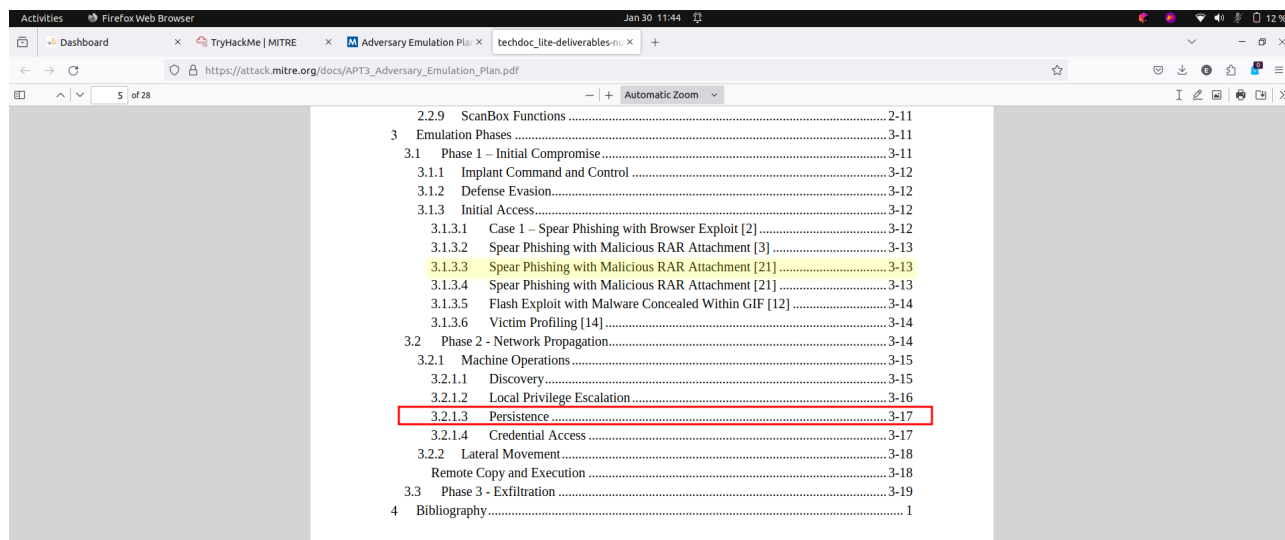
The MITRE APT3 Adversary Emulation Plans outline the behavior of persistent threat groups mapped to ATT&CK. They are used by adversary emulation teams to test an organizations network security and security products against specific threats.

APT3 Adversary Emulation Plan

2. Under Persistence, what binary was replaced with cmd.exe? ANS: sethc.exe

APT3 Adversary Emulation Plan

By clicking on APT3 Adversary Emulation Plan link, a pdf file opens in a new tab which I then navigated under persistence where this statement catches my eye:- “APT3 has replaced the Sticky Keys binary (C:\Windows\System32\sethc.exe) with cmd.exe”



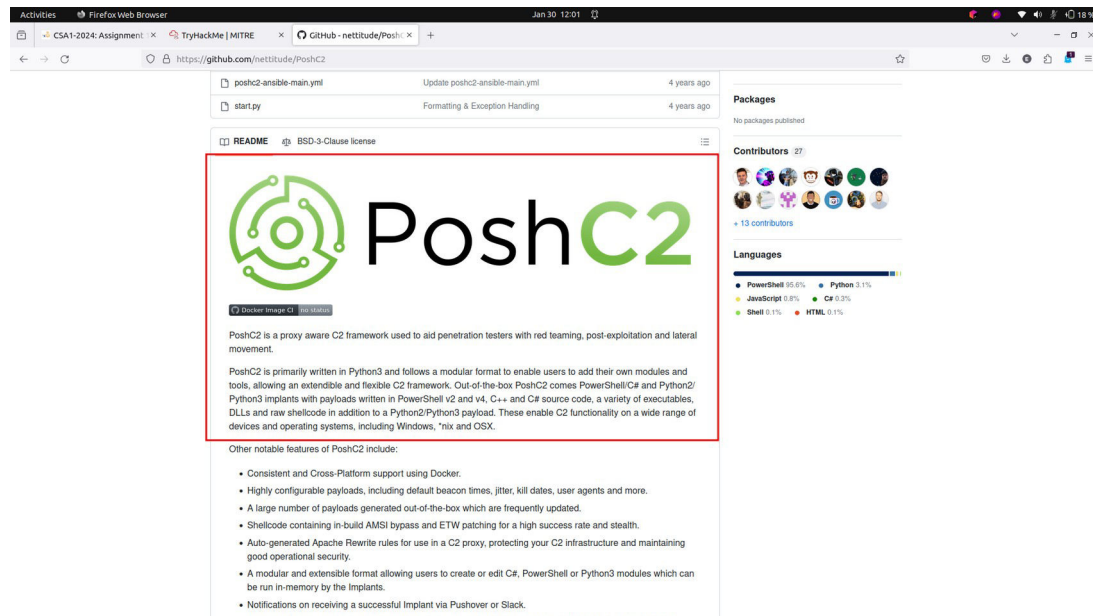
3. Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2) ANS: Pupy, Metasploit Framework

Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)

Pupy, Metasploit Framework

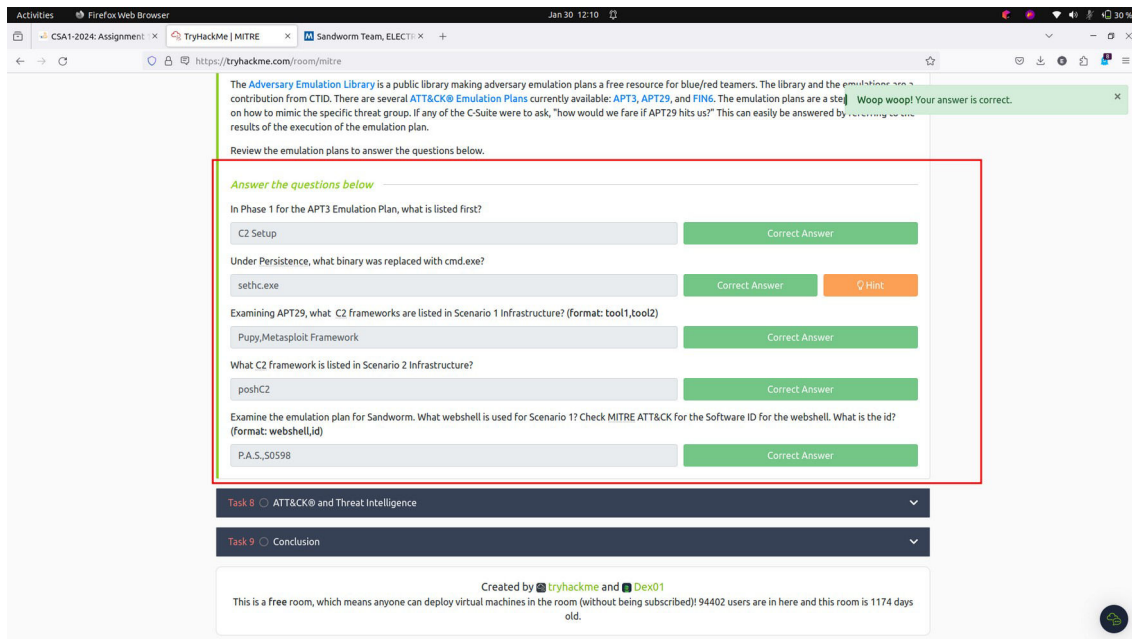
Correct Answer

4. What C2 framework is listed in Scenario 2 Infrastructure? ANS: **PoshC2**



5. Examine the emulation plan for Sandworm. What webshell is used for Scenario 1? Check MITRE ATT&CK for the Software ID for the webshell. What is the id? (format: webshell,id) ANS: **P.A.S.,S0598**

MITRE ATT&CK			
Groups			
Sandworm Team			
Scarlet Mimic			
Scattered Spider			
SideCopy			
Sidewinder			
Silence			
Silent Librarian			
Silver Tumbler			
Sowbug			
Stealth Falcon			
Strider			
Suckfly			
TA2541			
TA459			
TA505			
TA551			
TeamTNT			
TEMPVeles			
The White Company			
Threat Group-1314			
Threat Group-3390			
Thrip			
Toronto Team			
References			
1. Scott W. Brady. (2020, October 15). United States vs. Yuri Sergeyevich Andrienko et al. Retrieved November 25, 2020.			
2. UK NCSC. (2020, October 19). UK exposes series of Russian cyber attacks against Olympic and Paralympic Games. Retrieved November 30, 2020.			
22. Dragos Inc.. (2017, June 13). CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. Retrieved December 18, 2020.			
23. US-CERT. (2016, February 25). ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure. Retrieved June 10, 2020.			



ATT&CK and Threat Intelligence

In this section I learnt about Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) which is explained as the information, or TTPs (Tactics, Techniques and Procedures), attributed to the adversary.

I have understood that it is important for a large organisation to have a separate teams that gathers threat intelligence for other teams within the organization, in order for the organisation to have a large amount of TI Information.

Questions

1. What is a group that targets your sector who has been in operation since at least 2013? **ANS: APT33**

MITRE | ATT&CK

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

GROUPS

- APT33**
- APT37
- APT38
- APT39
- APT41
- Aquatic Panda
- Axiom
- BackdoorDiplomacy
- BITTER
- BlackOasis
- BlackTech
- Blue Mockingbird
- Bouncing Golf
- BRONZE BUTLER
- Carbanak
- Chimera
- Cleaver
- Cobalt Group
- Confucius
- CopyKittens
- CURIUM
- Dark Caracal

APT33

APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors. ^{[1] [2]}

ID: G0064
 Associated Groups: HOLMIUM, Elfin
 Contributors: Dragos Threat Intelligence
 Version: 1.4
 Created: 18 April 2018
 Last Modified: 08 March 2023

[Version](#) [Permalink](#)

Associated Group Descriptions

Name	Description
HOLMIUM	^[3]
Elfin	^[4]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	APT33 has used HTTP for command and control. ^[6]
Enterprise	T1560	.001 Archive Collected Data: Archive via Utility	APT33 has used WinRAR to compress data prior to exfiltration. ^[4]
Enterprise	T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT33 has deployed a tool known as DarkComet to the Startup folder of a victim, and used Registry run keys to gain persistence. ^{[4][9]}

ATT&CK® Navigator Layers

2. As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it? **ANS: Cloud Accounts**

Activities

Firefox Web Browser

Jan 30 12:33

56%

CSA1-2024: Assignment

TryHackMe | MITRE

APT33, HOLMIUM, Elfir

+

←

→

↺

↻

🔍

🌟

📄

📌

👤

☰

https://attack.mitre.org/groups/G0064/

MITRE | ATT&CK®

Matrices

Tactics

Techniques

Defenses

CTI

Resources

Benefactors

Blog

Search

GROUPS

APT33

APT37

APT38

APT39

APT41

Aquatic Panda

Axiom

BackdoorDiplomacy

BITTER

BlackOasis

BlackTech

Blue Mockingbird

Bouncing Golf

BRONZE BUTLER

Carbanak

Chimera

Cleaver

Cobalt Group

Confucius

CopyKittens

CURIUM

Dark Caracal

Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT33 has sent spearphishing e-mails with archive attachments. ^[4]
		.002	Phishing: Spearphishing Link	APT33 has sent spearphishing emails containing links to .hta files. ^{[1][4]}
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day. ^[4]
Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	APT33 has used a variety of publicly available tools like LaZagne to gather credentials. ^{[4][5]}
		.006	Unsecured Credentials: Group Policy Preferences	APT33 has used a variety of publicly available tools like Gpppassword to gather credentials. ^{[4][5]}
Enterprise	T1204	.001	User Execution: Malicious Link	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails. ^{[1][4]}
		.002	User Execution: Malicious File	APT33 has used malicious e-mail attachments to lure victims into executing malware. ^[4]
Enterprise	T1078		Valid Accounts	APT33 has used valid accounts for initial access and privilege escalation. ^{[2][3]}
		.004	Cloud Accounts	APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints. ^[3]
ICS	T0852		Screen Capture	APT33 utilize backdoors capable of capturing screenshots once installed on a system. ^{[4][7]}
ICS	T0853		Scripting	APT33 utilized PowerShell scripts to establish command and control and install files for execution. ^{[8][9]}
ICS	T0865		Spearphishing Attachment	APT33 sent spear phishing emails containing links to HTML application files, which were embedded with malicious code. ^[6] APT33 has conducted targeted spear phishing campaigns against U.S. government agencies and private sector companies. ^{[1][6]}

Software

ID	Name	References	Techniques
S0129	Autolt backdoor	[4]	Abuse Elevation Control Mechanism: Bypass User Account Control, Command and Scripting Interpreter: PowerShell, Data Encoding: Standard Encoding, File and Directory Discovery
S0363	Emoire	[5][4]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: SID-History Injection, Access Token Manipulation

cloud

^

▼

☐ Highlight All

☐ Match Case

☐ Match Diacritics

☐ Whole Words

1 of 3 matches

×

As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?

Cloud Accounts

Correct Answer

3. What tool is associated with the technique from the previous question? **ANS: Ruler**

S0358	Ruler	[5][3]	Account Discovery: Email Account, Office Application Startup: Outlook Rules, Office Application Startup: Outlook Forms, Office Application Startup: Outlook Home Page
-------	-------	--------	---

4. Referring to the technique from question 2, what mitigation method suggests using SMS messages as an alternative for its implementation? **ANS: Multi-factor Authentication**

On clicking the link cloud accounts, it gives more information about the topic too, this is where I find the mitigation method that suggests using SMS messages as an alternative for its implementation

MITRE | ATT&CK

Techniques

Enterprise

Reconnaissance

Resource Development

Initial Access

Content Injection

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing

Replication Through Removable Media

Supply Chain Compromise

Trusted Relationship

Valid Accounts

Default Accounts

Domain Accounts

Local Accounts

Cloud Accounts

Execution

Persistence

Privilege Escalation

Valid Accounts: Cloud Accounts

ID	Mitigation	Description
M1036	Account Use Policies	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[15]
M1015	Active Directory Configuration	Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead.
M1032	Multi-factor Authentication	Use multi-factor authentication for cloud accounts, especially privileged accounts. This can be implemented in a variety of forms (e.g. hardware, virtual, SMS), and can also be audited using administrative reporting features. ^[16]
M1027	Password Policies	Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Cloud service providers may track access key age to help audit and identify keys that may need to be rotated. ^[16]
M1026	Privileged Account Management	Review privileged cloud account permission levels routinely to look for those that could allow an adversary to gain wide access, such as Global Administrator and Privileged Role Administrator in Azure AD. ^{[17][8][19]} These reviews should also check if new privileged cloud accounts have been created that were not authorized. For example, in Azure AD environments configure alerts to notify when accounts have gone many days without using privileged roles, as these roles may be able to be removed. ^[20] Consider using temporary, just-in-time (JIT) privileged access to Azure AD resources rather than permanently assigning privileged roles. ^[19]
M1018	User Account Management	Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts.
M1017	User Training	Applications may send push notifications to verify a login as a form of multi-factor authentication (MFA). Train users to only accept valid push notifications and to report suspicious push notifications.

Detection

ID	Data Source	Data Component	Detects
DS0028	Logon Session	Logon Session Creation	Monitor for suspicious account behavior across cloud services that share account.

cloud

Highlight All Match Case Match Diacritics Whole Words 1 of 3 matches

5. What platforms does the technique from question #2 affect? ANS: **Azure AD, Google Workspace, IaaS, Office 365, SaaS**

MITRE | ATT&CK

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

Techniques

Enterprise

Reconnaissance

Resource Development

Initial Access

Content Injection

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing

Replication Through Removable Media

Supply Chain Compromise

Trusted Relationship

Valid Accounts

Default Accounts

Domain Accounts

Local Accounts

Cloud Accounts

Execution

Persistence

Privilege Escalation

Valid Accounts: Cloud Accounts

Other sub-techniques of Valid Accounts (4)

Valid accounts in cloud environments may allow adversaries to perform actions to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. Cloud Accounts can exist solely in the cloud or be hybrid joined between on-premises systems and the cloud through federation with other identity sources such as Windows Active Directory.^{[1][2][3]}

Service or user accounts may be targeted by adversaries through Brute Force, Phishing, or various other means to gain access to the environment. Federated accounts may be a pathway for the adversary to affect both on-premises systems and cloud environments.

An adversary may create long lasting Additional Cloud Credentials on a compromised cloud account to maintain persistence in the environment. Such credentials may also be used to bypass security controls such as multi-factor authentication.

Cloud accounts may also be able to assume Temporary Elevated Cloud Access or other privileges through various means within the environment. Misconfigurations in role assignments or role assumption policies may allow an adversary to use these mechanisms to leverage permissions outside the intended scope of the account. Such over privileged accounts may be used to harvest sensitive data from online storage accounts and databases through Cloud API or other methods.

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 has used compromised Office 365 service accounts with Global Administrator privileges to collect email from user inboxes. ^[4]

ID: T1078.004

Sub-technique of: T1078

Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

Platforms: Azure AD, Google Workspace, IaaS, Office 365, SaaS

Permissions Required: Administrator, User

Contributors: Jon Sternstein, Stern Security

Version: 1.6

Created: 13 March 2020

Last Modified: 16 October 2023

Version Permalink

cloud

Highlight All Match Case Match Diacritics Whole Words 1 of 3 matches

Activities Firefox Web Browser Jan 30 12:46

CSA1-2024: Assignment TryHackMe | MITRE Valid Accounts: Cloud Accounts

https://tryhackme.com/room/mitre

Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) is the information, or TTPs, attributed to the adversary. By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy. Large corporations might have an in-house team whose primary objective is to gather threat intelligence for other teams within the organization, aside from using threat intel already readily available. Some of this threat intel can be open source or through a subscription with a vendor, such as [CrowdStrike](#). In contrast, many defenders wear multiple hats (roles) within some organizations, and they need to take time from their other tasks to focus on threat intelligence. To cater to the latter, we'll work on a scenario of using ATT&CK for threat intelligence. The goal of threat intelligence is to make the information actionable.

Scenario: You are a security analyst who works in the aviation sector. Your organization is moving their infrastructure to the cloud. Your goal is to use the ATT&CK Matrix to gather threat intelligence on APT groups who might target this particular sector and use techniques targeting your areas of concern. You are checking to see if there are any gaps in coverage. After selecting a group, look over the selected group's information and their tactics, techniques, etc.

Answer the questions below

What is a group that targets your sector who has been in operation since at least 2013?

APT33 Correct Answer

As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?

Cloud Accounts Correct Answer

What tool is associated with the technique from the previous question?

Ruler Correct Answer

Referring to the technique from question 2, what mitigation method suggests using SMS messages as an alternative for its implementation?

Multi-factor Authentication Correct Answer

What platforms does the technique from question #2 affect?

Azure AD, Google Workspace, IaaS, Office 365, SaaS Correct Answer

Task 9 Conclusion

Created by TryHackMe and Dex01

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 94402 users are in here and this room is 1174 days old.

Conclusion.

From this lab I have learnt on different how to extract intelligence from MITRE websites. I now have a better understanding on MITRE ATT&CK knowledge base which describes the actions, tactics, and techniques commonly employed by cyber adversaries. This room has provided me with practical knowledge and important skills in cybersecurity.

Thank you.