THM SOC LEVEL 1

CYBER DEFENCE FRAMEWORK

Mikhail Amzar

5/7/2024

Try Hack Me's SOC Level 1 Training Course self-notes 1/7.

CONTENTS

Pyramid Of Pain

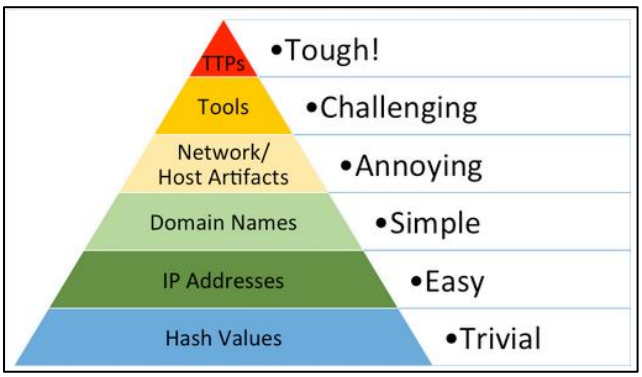
1.Introduction

https://www.picussecurity.com/resource/glossary/what-is-pyramid-of-pain
https://tryhackme.com/r/room/pyramidofpainax

Definition

What is Pyramid of Pain?
The Pyramid of Pain is a conceptual framework that illustrates the varying levels of difficulty and cost an adversary would encounter to evade detection and continue their attack, in the context of cybersecurity defenses.

It's a framework, enabling security experts, predominantly blue teamers, to channel their resources on elements inducing the most pain to adversaries to alter.



2.Hash Values (Trivial)

Definition
What is Hash value?
Hash value is a numeric value of a fixed length that uniquely identifies data. A hash value is the result of a hashing algorithm.

Exm:

- **MD5** (128-bit hash value; No longer secure)
- **SHA-1** (160-bit hash value, 40-digit hexadecimal number; No longer secure)
- **SHA-2** | variant **SHA-256** (256-bits hash value, 64-digit hexadecimal number)

Security professionals usually use the hash values to gain insight into a specific malware sample, a malicious or a suspicious file, and to uniquely identify and reference the malicious artifact.

Even in security reports, sometimes a malware's or file's hash value will be provided in the report.

Sites for reports:

- The DFIR Report
- FireEye Threat Research Blogs

Why is hash value trivial in the pyramid of pain?
Because sure, granted you have the malicious sample's signature in your arsenal to test against, or you're using an online tool that checks for it, you can detect it.

But even a single bit change in a malicious file will change the end hash value. So, an attacker can certainly leverage this.
That makes threat hunting using file hashes as the IoC, difficult.

3.IP Address (Easy)

What's an IP address?
Logical address to identify devices on a network.

IP Address as Indicators of Compromise?
From a defense standpoint, knowledge of the IP addresses an adversary uses can be valuable. A common defense tactic is to block, drop, or deny inbound requests from IP addresses on your parameter or external firewall.

But! This tactic is often not bulletproof as it's trivial for an experienced adversary to recover simply by using a new public IP address.

Bonus
One of the ways an adversary can make it challenging to successfully carry out IP blocking is by using **Fast Flux**.

According to Akamai, **Fast Flux** is a DNS technique used by botnets to hide phishing, web proxying, malware delivery, and malware communication activities behind compromised hosts acting as proxies.

The purpose of using the Fast Flux network is to make the communication between malware and its command-and-control server (C&C) challenging to be discovered by security professionals.

You can analyze malware and its communication in a virtual environment using tools like: Any Run

4.Domain Names (Simple)

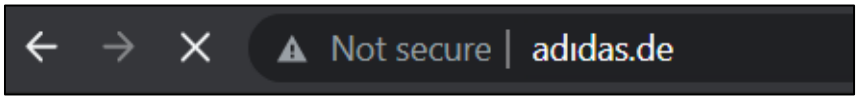
Domain Names as IoC?

Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records.

Unfortunately for defenders, many DNS providers have loose standards and provide APIs to make it even easier for the attacker to change the domain.

Attackers can trick victims by manipulating the display of domain/URLs using a few methods.

- **Punycode** (converting characters into another)

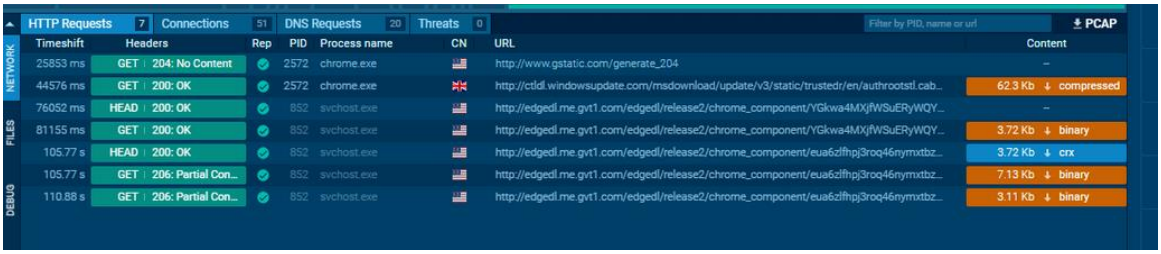


- Hiding malicious URLs using URL shortener services.
    - bit.ly
    - goo.gl
    - ow.ly
    - s.id
    - smarturl.it
    - tiny.pl
    - tinyurl.com
    - x.co

Bonus

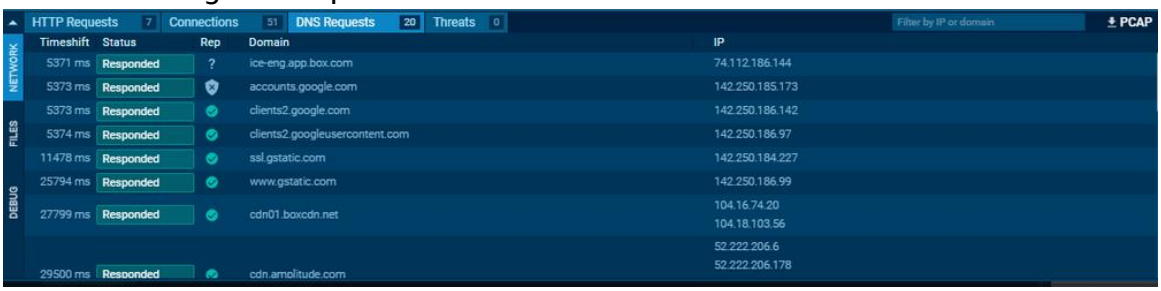
Viewing connections in Any Run

Below: Seeing what resources are being retrieved from a webserver.



Below: Seeing connections made by any process to another host. (Could be C2 traffic)

Below: Checking DNS requests.



5.Host Artifact (Annoying)

Definition

What are host artifacts?

Host artifacts are the **traces** or **observables** that attackers leave on the system, such as registry values, suspicious process execution, attack patterns or IOCs (Indicators of Compromise), files dropped by malicious applications, or anything exclusive to the current threat.

Host artifacts as IoC?

On this level, the attacker will feel a little more annoyed and frustrated if you can detect the attack.

The attacker would need to circle back at this detection level and change his attack tools and methodologies. This is very time-consuming for the attacker, and probably, he will need to spend more resources on his adversary tools.

Exm screenshots:

Report: https://assets.tryhackme.com/additional/pyramidofpain/task5-report.pdf
Below: Files dropped/modified by malicious actor

2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd **MD5:** CC11BFD14D6ECC83477B69FF06C6C587	**SHA256:** A4E8F5821887AC26449C33D9B027CE31BE0E7203DD035C5DC7D34A9AEF01A6DA	tlb
2728	WINWORD.EXE	C:\Users\admin\AppData\Local\Temp\~$O-100120 CDW-102220.doc **MD5:** 2E7A3442236F2D50C669BC79188BBD69	**SHA256:** BF007001BACF8F6ABF371B0B2797B7D13B741879E1E5B76FB616A934318418A9	pgc
3828	POwersheLL.exe	C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB	**SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable
1640	G_jugk.exe	C:\Users\admin\AppData\Local\photowiz\regidle.exe **MD5:** 92F58C4E2F524EC53EBE10D914D96CCB	**SHA256:** 4A9E32BC5348265C43945ADAAF140B98B64329BD05878BC13671FA916F423710	executable

6.Network Artifacts (Annoying)

Network artifacts like:

- user-agent string
  - The User-Agent is defined by RFC2616 as the request-header field that contains the information about the user agent originating the request.
- C2 information
- URI patterns
- HTTP POST requests

Use network protocol analyzer like **TShark** or explore IDS logging (like from **Snort** source).

HTTP POST request Exm:

192.168.100.140	194.187.133.160	936	HTTP	POST /Nqdlz/w2BG/ HTTP/1.1
192.168.100.140	98.174.164.72	936	HTTP	POST /ghMuzyNCNWN/kMmYdVIthxeVy/o2feo8eu7Jyv/O2M8WIf9SpyCp/yLVEV96eosyd5URJ477/8wdGXdz9k9hhJjWp/ HTTP/1.1
192.168.100.140	103.86.49.11	936	HTTP	POST /VCvOqXMjgEehauu/AyEp/O9Qn2/R6Rj7Gw9eOv6yJ/fC5a36YfopGe/Q2AwYvSohZiyaEtbbo/ HTTP/1.1
192.168.100.140	78.24.219.147	904	HTTP	POST /jCOc/oQQPMafJlpMi6n3/Pbao/K7oB22aAUKQ6lA6r/GoOMY/ HTTP/1.1
192.168.100.140	50.245.107.73	888	HTTP	POST /ukXcIsljsvd7W/h2VQlYqB/csuQkgUqlkakMvQRJ9/NCjJodG/ HTTP/1.1
192.168.100.140	110.145.77.103	888	HTTP	POST /QZvVQ6o1I/DYk9QgXU/HtoxMCRHbYCJhgamW/5NsCejn3/ HTTP/1.1

TShark analysis Exm:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ tshark -Y http.request -T fields -e http.user_agent -r analysis.pcap

lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
lozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
```

7.Tools (Challenging)

At this stage, we have levelled up our detection capabilities against the artifacts. The attacker would most likely give up trying to break into your network or go back and try to create a new tool that serves the same purpose.

It will be a game over for the attackers as they would need to invest some money into building a new tool (if they can do so), find the tool that has the same potential, or even get some training to learn how to be proficient in a certain tool.

What would an attacker do?

Attackers would use the utilities to create:

- Malicious macro documents (maldocs) for spearphishing attempts.
- A backdoor that can be used to establish C2 (Command and Control Infrastructure).
- Any custom .EXE, and .DLL files, payloads, or password crackers.

Antivirus signatures, detection rules, and YARA rules can be great weapons for you to use against attackers at this stage.

MalwareBazaar and Malshare for samples, malicious feeds, YARA results – useful for threat hunting and incident response.

SOC Prime Threat Detection Marketplace for detection rules shared by other security professionals.

8.TTP (Tactics, Techniques, Procedures) – (Tough)

Useful resource with regard to studying TTPs is the MITRE ATT&CK Matrix.

If you manage to detect a specific attack and know the techniques, it should be easy to remediate swiftly.

For, example if you could detect a Pass-the-Hash attack using Windows Event Log Monitoring and remediate it, you would be able to find the compromised host very quickly and stop the lateral movement inside your network. At this point, the attacker would have two options:

1. Go back, do more research and training, reconfigure their custom tools.
2. Give up and find another target.

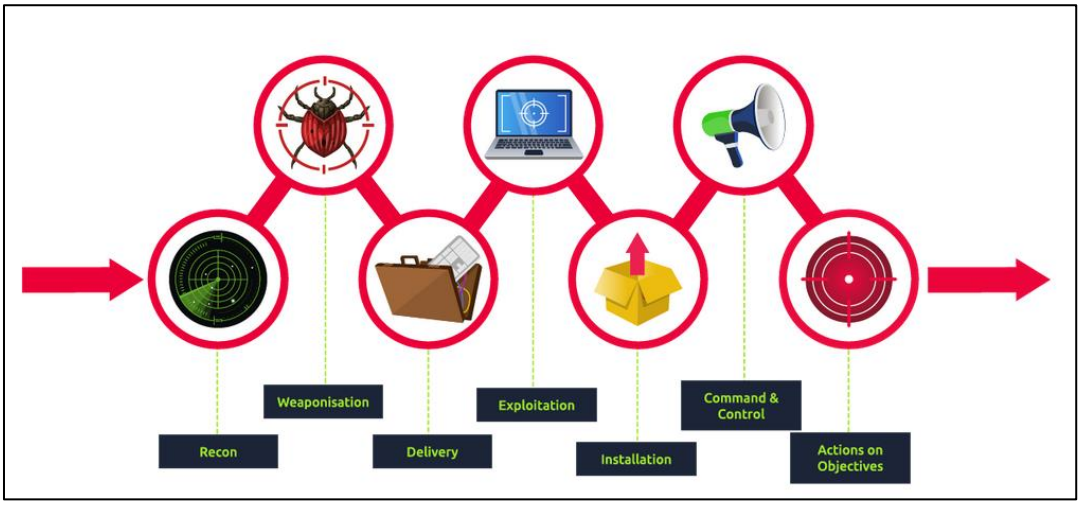
Option 2 sounds less time and resource consuming.

Cyber Kill Chain

Introduction to CKC

What's it for?

The Cyber Kill Chain framework is designed for **identification** and **prevention** of the network intrusions. Learn what the adversaries need to do to achieve their goals.



Use the knowledge of Cyber Kill Chain to:

- Assess your network and system security.
- Identify missing security controls.
- Close security gaps in your infra.

As defender, we must identify and **break the kill chain.**

1.Reconnaissance

From the attacker's perspective:

Reconnaissance is discovering and collecting information on the system and the victim. The reconnaissance phase is the planning phase for the adversaries.

OSINT (Open Source Intelligence) – Publicly available data

OSINT tools such as theHarvester , Hunter.io , OSINT Framework

2.WEAPONIZATION

Definition

The phase where an attacker may create their malicious payload, set up their C2 techniques, etc.

Perhaps the attacker creates their own malware and payload here (like some APTs), perhaps they choose to buy malware off the dark web etc.

Interesting links:

- Intro to Macros and VBA For Script Kiddies" by TrustedSec
- DarkWeb

3.DELIVERY

The phase where the attacker decides the method for transmitting their payload.

Exm:
Phishing email, Malicious USB distribution (USB drop attack), Watering hole attack, Drive by attack.

4.EXPLOITATION

Concerning attackers' method of exploitation

How does the attacker carry out their exploit in this phase?

- Perhaps the victim triggered it by opening malicious attachment or links.
- Zero-day exploit
- Exploiting vulnerabilities in software, hardware, or even human.

5.INSTALLATION

In this phase, Attacker might install something on the system they compromised, that would allow them to have **persistence** in the system.

Exm: Windows Persistence Room

Could be:

- Install web shell on a webserver. (Malicious script for attacker to maintain access,
  Exm: https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/)
- Install a backdoor on victim machine,
  Exm: meterpreter interactive shell.
- Create or modifying windows services,
  Exm: masquerading malicious process as a legitimate windows service.
- https://attack.mitre.org/techniques/T1547/001/

Timestomping technique can also help attacker avoid detection.

6.Command & Control (C2)

After gaining persistence, the attacker opens up their C2 channel to remotely control and manipulate the victim.

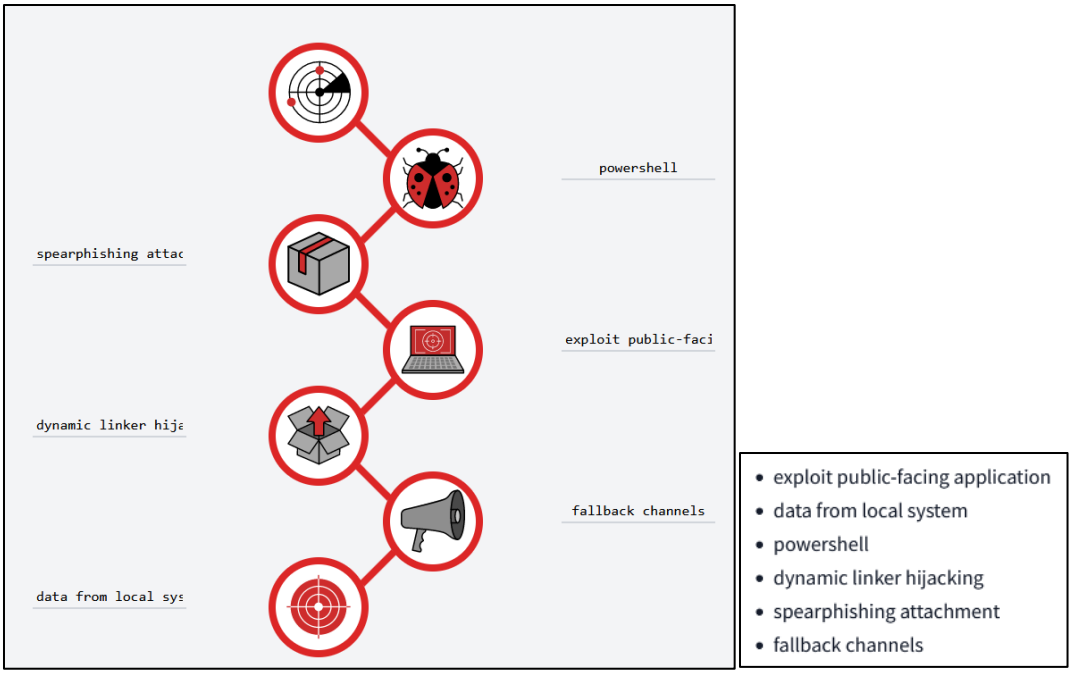
Common C2 channels today like HTTP p80, HTTPS p443 (Blends in with legitimate web traffic to evade firewall).
DNS, Infected making DNS request to the DNS server that belongs to the attacker (DNS Tunneling).

7.Exfiltration (Actions on Objectives)

Now the attacker act on his ultimate objective.

Can be anything,

- Collect the credentials from users.
- Perform privilege escalation (gaining elevated access like domain administrator access from a workstation by exploiting the misconfiguration).
- Internal reconnaissance (for example, an attacker gets to interact with internal software to find its vulnerabilities).
- Lateral movement through the company's environment.
- Collect and exfiltrate sensitive data.
- Deleting the backups and shadow copies. Shadow Copy is a Microsoft technology that can create backup copies, snapshots of computer files, or volumes.
- Overwrite or corrupt data.



Last time the Cyber Kill Chain was updated was 2011. The absence of update may cause security gaps in the framework, as such, you should also rely on other tools as well because the landscape today has evolved.

We recommend not only relying on the traditional Cyber Kill Chain model but also referring to MITRE ATT&CK as well as Unified Kill Chain to apply a more comprehensive approach to your defence methodologies.

Unified Kill Chain

Introduction

https://tryhackme.com/r/room/unifiedkillchain

What is a kill chain?

Like in Cyber Kill Chain, kill chain refers to the steps and methodology an attacker use to approach and intrude their victim.

From a defenders' perspective:

Objective is to understand the Kill Chain. Know what the attacker will do, in order to know how to stop them (security measures).

What is Threat Modelling?

Identifying risk, vulnerabilities, and assets to take steps in improving the security of a system.

Do threat modelling to reduce risk with a system and to mitigate threats.

Other frameworks concerned with TM - STRIDE, DREAD, CVSS.

18 Phases in the Unified Kill Chain

Phase In >	Phase Through >	Phase Out
Iniatial foothold	Network Propagation	Action on Objectives

Benefits of the UKC

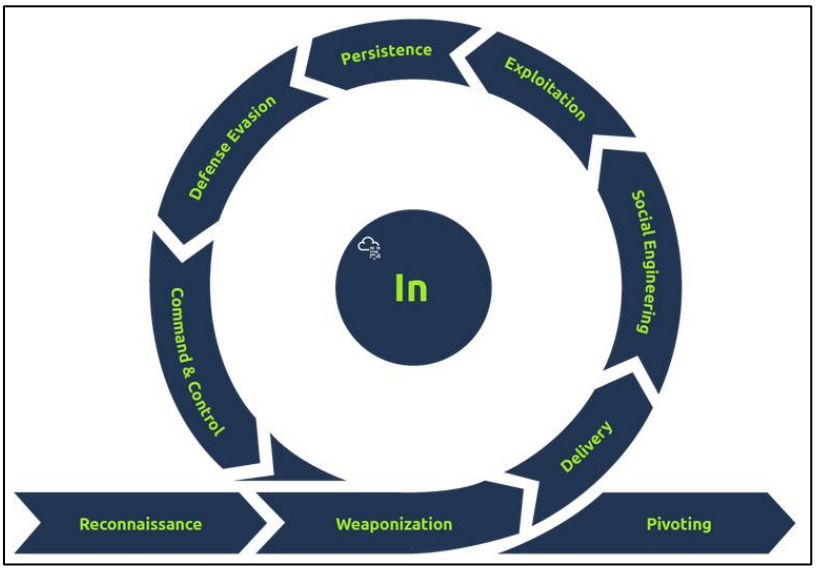
Benefits	How do other frameworks compare?
Modern (released in 2017, updated in 2022).	Some frameworks, such as MITRE's were released in 2013, when the cybersecurity landscape was very different.
The UKC is extremely detailed (18 phases).	Other frameworks often have a small handful of phases.
The UKC covers an entire attack - from reconnaissance, exploitation, post-exploitation and includes identifying an attacker's motivation.	Other frameworks cover a limited number of phases.
The UKC highlights a much more realistic attack scenario. Various stages will often re-occur. For example, after exploiting a machine, an attacker will begin reconnaissance to pivot another system.	Other frameworks do not account for the fact that an attacker will go back and forth between the various phases during an attack.

1.Phase In (Initial Foothold)

Main focus of this phase

For an attacker to gain access to a system or networked environment.

This series of phases also accommodates for an attacker creating a form of persistence (such as files or a process that allows the attacker to connect to the machine at any time)

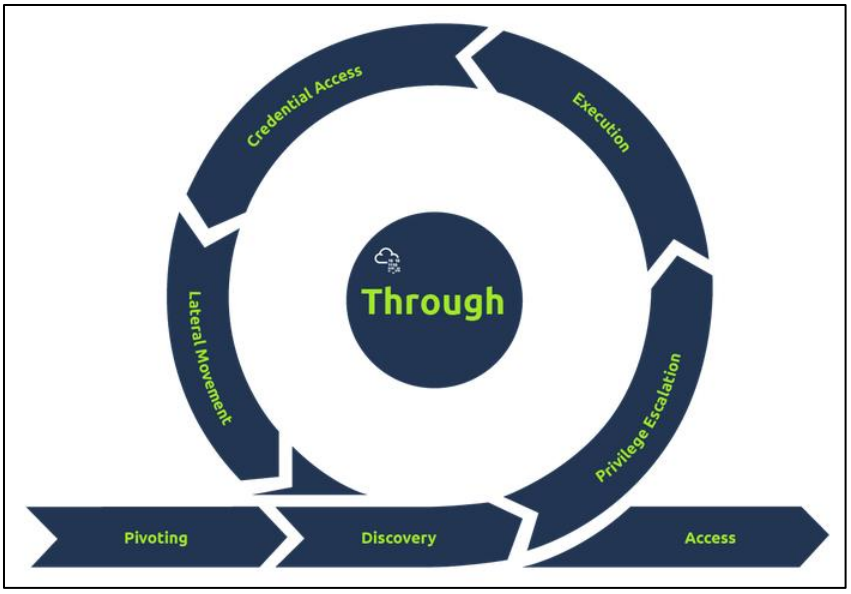


2.Phase Through (Network Propagation)

Main focus of this phase

This phase follows a successful foothold being established on the target network.

- An attacker would seek to gain additional access and privileges to systems and data to fulfil their goals.
- The attacker would set up a base on one of the systems to act as their pivot point and use it to gather information about the internal network.



3.Phase Out (Action on Objectives)

Main focus of this phase

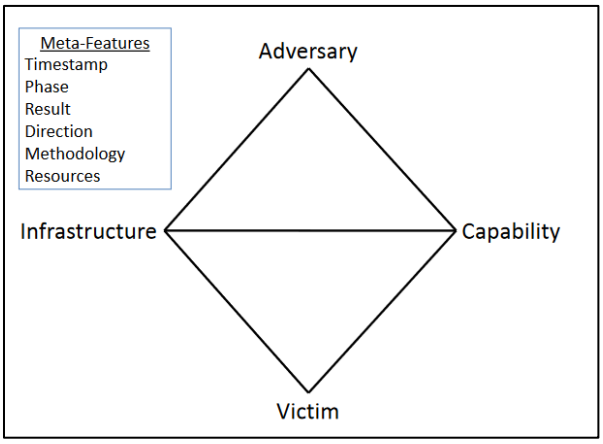
This phase wraps up the journey of an adversary's attack on an environment, where they have critical asset access and can fulfil their attack goals. These goals are usually geared toward compromising the confidentiality, integrity and availability (CIA) triad.

15	**Collection**	Techniques used to identify and gather data from a target network prior to exfiltration.
16	**Exfiltration**	Techniques that result or aid in an attacker removing data from a target network.
17	**Impact**	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	**Objectives**	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

DIAMOND MODEL

INTRO OF DIAMOND MODEL

Diamond Model of Intrusion Analysis.
https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
Basically - The Diamond Model can help you identify the elements of an intrusion.



1.ADVERSARY

Adversary Operator is the "hacker", someone conducting the intrusion.
Adversary Customer is the entity that stand to benefits from the activity in the intrusion. It **can** be the same person with Adversary Operator, or it can be different.

2.VICTIM

Target of the adversary.
Can be a person, group, organization, email address, IP address, domain, etc.

Victim Personae – People (or Org, industries, job roles, etc) being targeted and whose assets are being attacked.

Victim Assets – The attack surface, include the set of systems, network, email, hosts, IP addresses, socmed accounts, etc, to which the adversary direct their capabilities.

3.Capability

The skill, tools, and techniques used by the adversary in the event. The capability highlights the adversary's tactics, techniques, and procedures (TTPs).

Capability Capacity

Capability Capacity is all the vulnerabilities and exposures that the individual capability can use.

Adversary Arsenal

An **Adversary Arsenal** is a set of capabilities that belong to an adversary. The combined capacities of an adversary's capabilities make it the adversary's arsenal.

4.Infrastructure

The physical or logical interconnections that the adversary uses to deliver a capability or maintain control of capabilities.

Type 1 Infrastructure is the infrastructure controlled or owned by the adversary.

Type 2 Infrastructure is the infrastructure controlled by an intermediary. Sometimes the intermediary might or might not be aware of it. This is the infrastructure that a victim will see as the adversary. Type 2 Infrastructure has the purpose of obfuscating the source and attribution of the activity. Type 2 Infrastructure includes malware staging servers, malicious domain names, compromised email accounts, etc.

Service Providers are organizations that provide services considered critical for the adversary availability of Type 1 and Type 2 Infrastructures, Exm: Internet Service Providers, domain registrars, and webmail providers.

--Incomplete diamond model note

MITRE

ATT&CK Framework

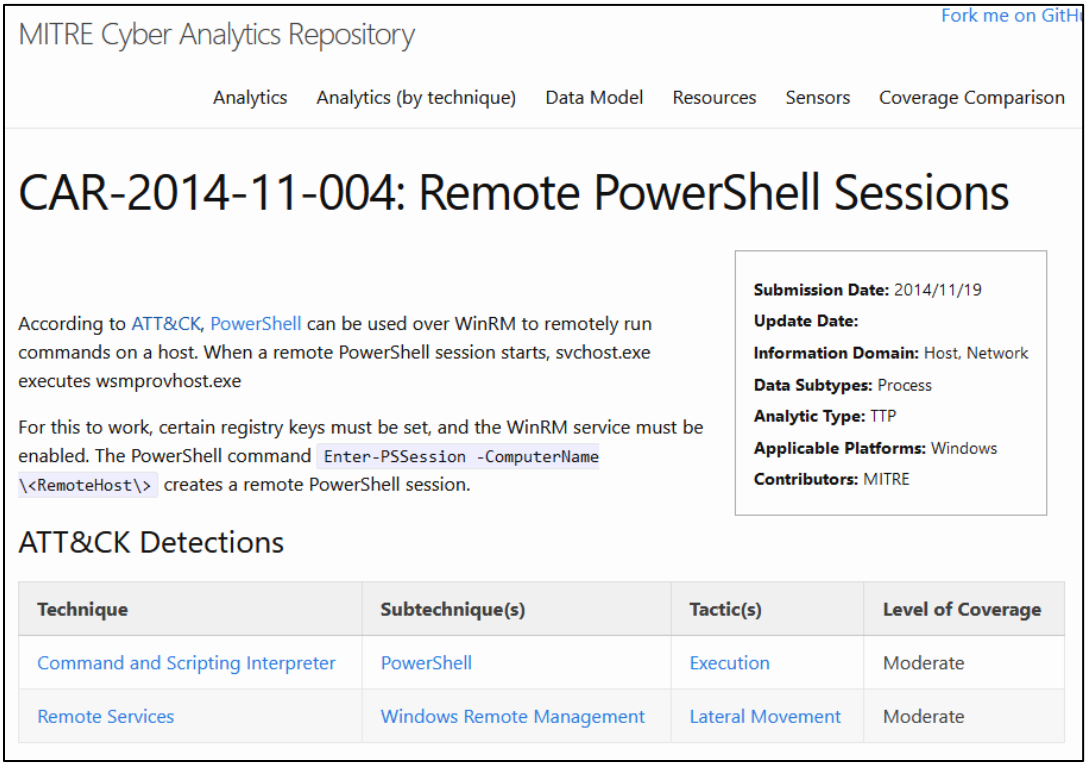
MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.
https://attack.mitre.org/

CAR Knowledge Base (Cyber Analytics Repository)

(CAR) is a knowledge base of analytics developed by *MITRE* based on the *MITRE* ATT&CK®adversary model. 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.

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.

Exm:

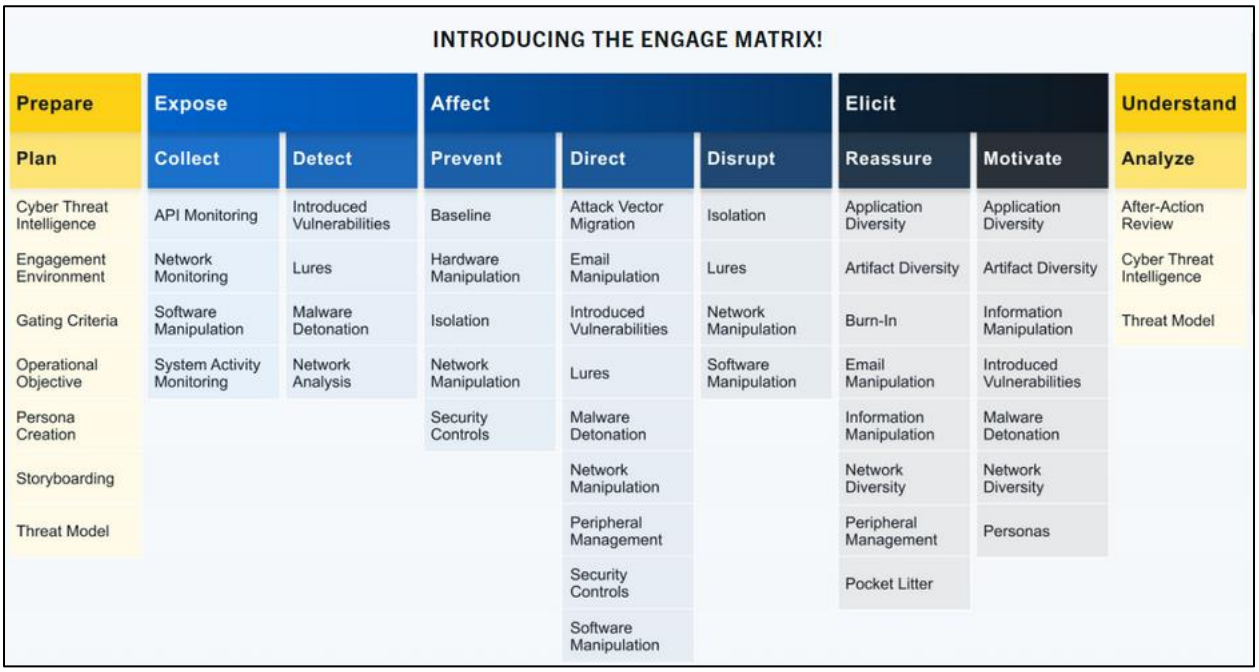


MITRE ENGAGE

***MITRE* Engage** is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals.

Adversary Engagement Approach – Implementing **Cyber Denial** & **Cyber Deception**.
https://engage.mitre.org/matrix/

Cyber Denial	We prevent the adversary's ability to conduct their operations
Cyber Deception	We intentionally plant artifacts to mislead the adversary



INTRODUCING THE ENGAGE MATRIX!

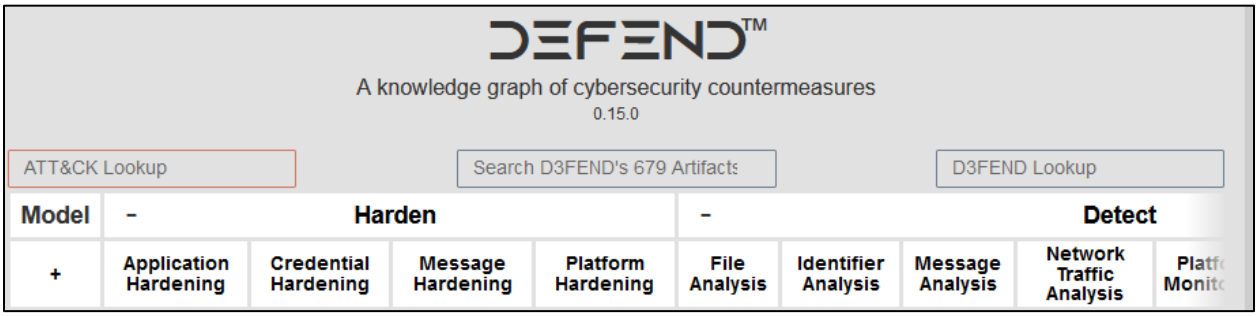
Prepare	Expose		Affect			Elicit		Understand
Plan	**Collect**	**Detect**	**Prevent**	**Direct**	**Disrupt**	**Reassure**	**Motivate**	**Analyze**
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

- **Prepare** the set of operational actions that will lead to your desired outcome (input)
- **Expose** adversaries when they trigger your deployed deception activities
- **Affect** adversaries by performing actions that will have a negative impact on their operations
- **Elicit** information by observing the adversary and learn more about their modus operandi (TTPs)
- **Understand** the outcomes of the operational actions (output)

MITRE D3FEND

(Detection-Denial-Disruption Framework Empowering Network Defense)

MITRE D3FEND is A knowledge graph of cybersecurity countermeasures. Collection of knowledge based on defense strategy/actions and can be cross referenced with ATT&CK. https://d3fend.mitre.org/
Exm:



ATT&CK Emulation Plans

MITRE formed an organization named The Center of Threat-Informed Defense (CTID). This organization consists of various companies and vendors from around the globe. Their objective is to conduct research on cyber threats and their TTPs and share this research to improve cyber defense for all.

The Adversary Emulation Library is a public library making adversary emulation plans a free resource for blue/red teamers.

Github: https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master

Exm showing details of APT3 Persistance operation and techniques:

3.2.1.3 Persistence

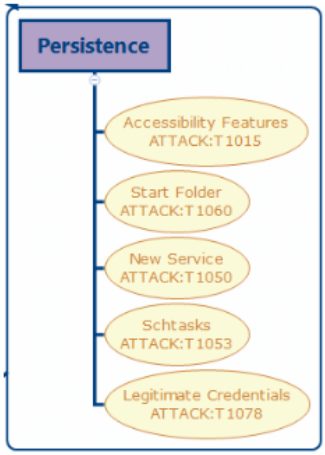


Figure 5 APT3 Persistence ATT&CK Techniques

APT3 has used multiple methods for persistence: creating a service [23] (T1050 - New Service), creating a scheduled task [2] (T1053 - Scheduled Task), and also by placing scripts in the Startup Folder [7] [T1060 - Registry Run Keys/Start Folder].

APT3 has replaced the Sticky Keys binary (`C:\Windows\System32\sethc.exe`) with cmd.exe [T1015 - Accessibility Features] and enabled Remote Desktop Protocol (RDP) if it is not already enabled [T1076 – Remote Desktop Protocol]. This specific Persistence technique has an added benefit of allowing an operator to open a command prompt when connected over RDP without having to provide valid credentials [23].

APT3 has been known to create or enable accounts, for example "support_388945a0", and add them to the local admin group [23] [T1136 – Create Account]. Presumably this is done for easier future access.

Recommendation: On new hosts, establish persistence by creating a service or schtasks. On systems where RDP capabilities are desired, it might also be useful to enable sticky keys and RDP.

ATT&CK and Threat Intelligence

Threat Intelligence (TI) or **Cyber Threat Intelligence (CTI)** is the information, or TTPs, attributed to the adversary.

HOLOTAPES

C2

Command and Control (C2) Infrastructure are a set of programs used to communicate with a victim machine. This is comparable to a reverse shell, but is generally more advanced and often communicate via common network protocols, like HTTP, HTTPS and DNS.

FTP

File Transfer Protocol (FTP) is a protocol designed to help the efficient transfer of files between different and even non-compatible systems. It supports two modes for file transfer: binary and ASCII (text).

CVE

Common Vulnerabilities and Exposures (CVE), this term is given to a publicly disclosed vulnerability

CVSS

Common Vulnerability Scoring System

API

API, which stands for Application Programming Interface, is a set of rules and protocols for building software and applications. An API allows different software programs to communicate with each other. It defines methods of communication between various components, including the kinds of requests that can be made, how they're made, the data formats that should be used, and conventions to follow.

IOC

Indicator of Compromise is a forensic artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

SOC

Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring, preventing , detecting , investigating, and responding to threats within a company's network and systems.

MISP

Malware Information Sharing Platform is is an open-source threat information platform used to facilitate the collection and sharing of threat information.

HIDS

Host Intrusion Detection System (HIDS) analyzes system state, system calls, file-system modifications, application logs, and other system activity.