Cyber attackers

CalPolyPomona

Cyber attackers: classification attributes

- **Internal vs. External:** We most often think about the threat actors who exist outside our organizations: competitors, criminals, and the curious. However, some of the most dangerous threats come from within our own environments.
  - Complex attacks often come from externals with some internal complicity
- **Level of Sophistication/Capability:** Threat actors vary greatly in their level of cybersecurity sophistication and capability. As we explore different types of threat actors in this lesson, we'll discuss how they range from the unsophisticated *script kiddie* simply running code borrowed from others to the *advanced persistent threat* (APT) actor exploiting vulnerabilities discovered in their own research labs and unknown to the security community.
- **Resources/Funding:** Just as threat actors vary in their sophistication, they also vary in the resources available to them. Highly organized attackers sponsored by criminal syndicates or national governments often have virtually limitless resources, whereas less organized attackers may simply be hobbyists working in their spare time.
- **Intent/Motivation:** Attackers also vary in their motivation and intent. The *script kiddie* may be simply out for the thrill of the attack, whereas competitors may be engaged in highly targeted corporate espionage. *Nation-states* seek to achieve political objectives; criminal syndicates often focus on direct financial gain.

The Hats Hackers Wear

The cybersecurity community uses a shorthand lingo to refer to the motivations of attackers, describing them as having different-colored hats. The origins of this approach date back to old Western films, where the “good guys” wore white hats, and the “bad guys” wore black hats to help distinguish them in the film. Cybersecurity professionals have adopted this approach to describe different types of cybersecurity adversaries:

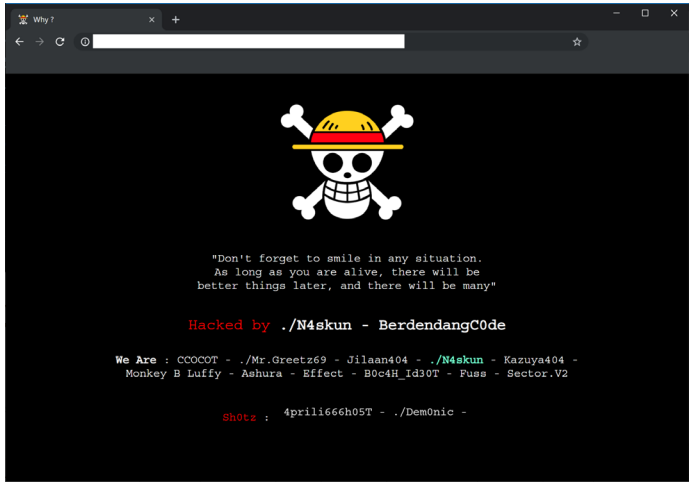
- **White-hat hackers,** also known as authorized attackers, are those who act with authorization and seek to discover security vulnerabilities with the intent of correcting them. White-hat attackers may either be employees of the organization or contractors hired to engage in ***penetration testing*** (they are often called ***penetration testers*****)**.
- **Black-hat hackers**, also known as unauthorized attackers, are those with malicious intent. They seek to defeat security controls and compromise the confidentiality, integrity, or availability of information and systems for their own, unauthorized, purposes.
- **Gray-hat hackers**, also known as semi-authorized attackers, are those who fall somewhere between white- and black-hat hackers. They act without proper authorization, but they do so with the intent of informing their targets of any security vulnerabilities. It's important to understand that simply having good intent does not make gray-hat hacking legal or ethical. The techniques used by gray-hat attackers can still be punished as criminal offenses.

Classes of Intruders: *Cyber Criminals*

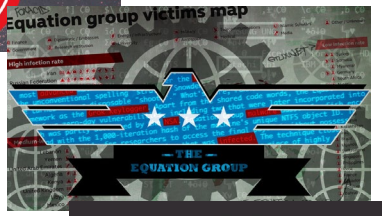
- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
  - Identity theft: stealing and using information and documents by someone else with a false identity. E.g., opening accounts, posting on social media, performing transactions, accessing physically secured areas
  - Theft of financial credentials: stealing of data for financial purposes
  - Corporate espionage: stealing information for accessing business or secreted information. E.g., inventions and patents, political secrets
  - Data theft: generic stealing of data for different purposes: e.g., copyright violation, re-sale, etc.
  - Data ransoming: "kidnapping" data to be released after payment
- Typically, they are young who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

Classes of Intruders: *Activists/Hacktivist*

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
  - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
  - Website defacement: partial or total alternation of victim website
  - Denial of Service attacks: interruption of service from victim of attack
  - Reputation: Theft and distribution of data that results in negative publicity or compromise of their targets
- Examples: Anonymous, Edward Snowden, etc.



Classes of Intruders: *State-Sponsored Organizations*



- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Widespread nature and scope of these activities by a wide range of countries:
  - E.g,. from one country against another

Not all but some of the groups indicated here https://attack.mitre.org/groups/ are *state-sponsored*

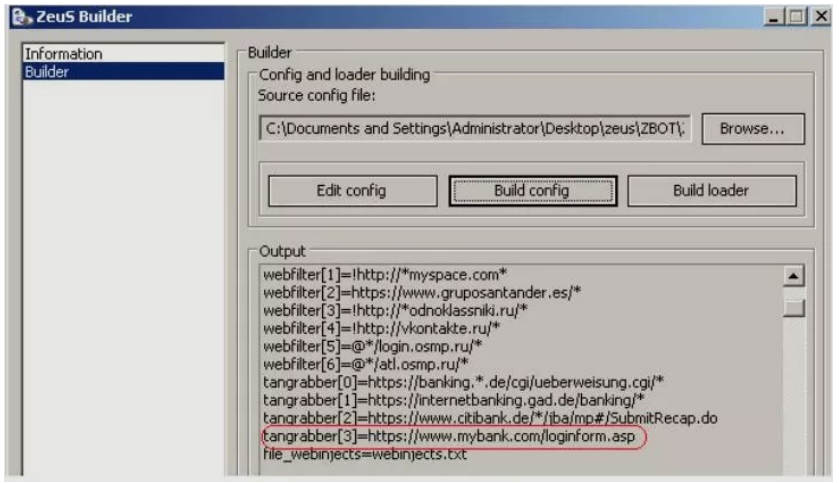
Classes of Intruders: *Others*

Hackers with motivations other than those previously listed

- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of "hobby hackers" using them to explore system and network security

Intruder Skill Levels – Apprentice/Beginner

- Hackers with minimal technical skill who primarily use existing **attack toolkits** (aka, **crimeware**)
  - E.g. Zeus toolkit, Angler
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Also known as "**script-kiddies**" due to their use of existing scripts (tools)



https://www.pdf-archive.com/2011/03/26/zeus-crimeware-toolkit/

Given their use of existing known tools, these attackers are the easiest to defend against

Intruder Skill Levels – Journeyman/Skilled

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

Given their generation of new tools or variants of existing tools, these attackers are harder to defend from compared to the script kiddies

Intruder Skill Levels – Master/Expert

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations

Defending against these attacks is of the highest difficulty

Cyber attack stages

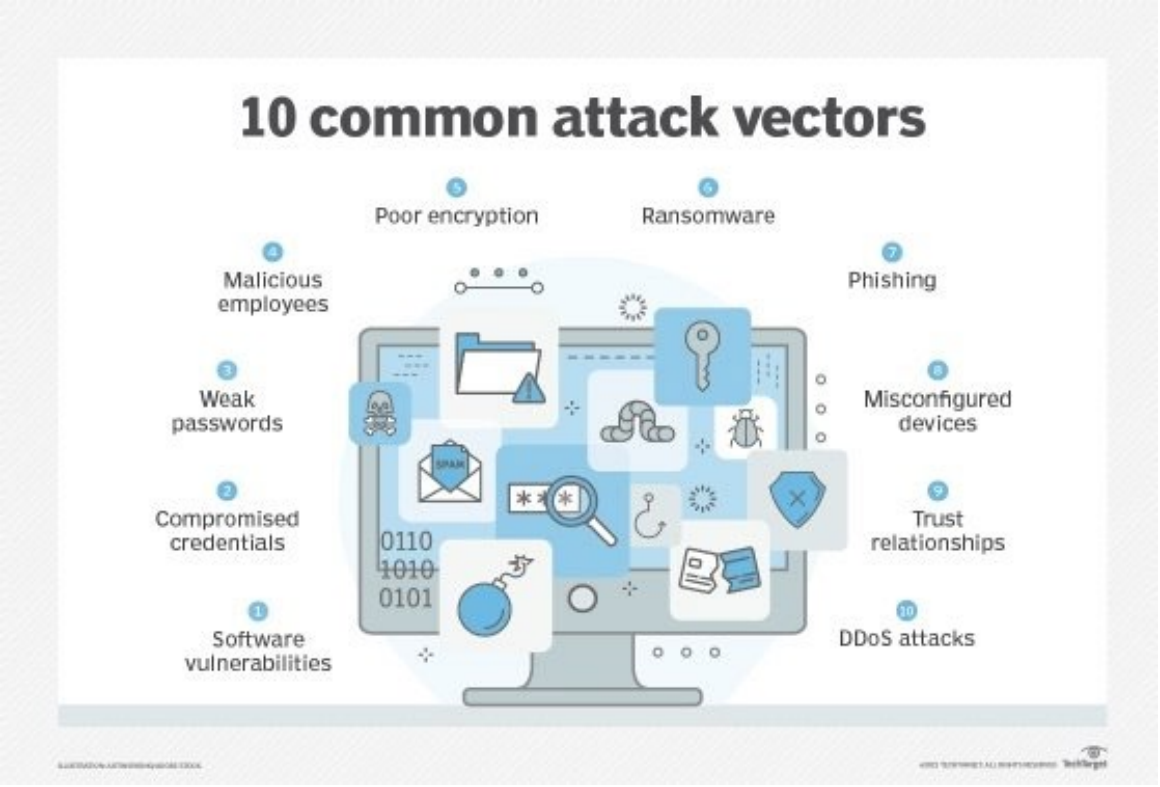
CalPolyPomona

Attack vectors

- An **attack vector** is a generic way to indicate the method or combination of methods that cybercriminals use to breach or infiltrate a victim's network.

- Adversaries typically develop an arsenal of attack vectors that they routinely use to carry out their attacks. Over time and with repeated use, these attack vectors can become virtual "calling cards" for cybercriminals or organized eCrime gangs, making it possible for threat intelligence analysts, cybersecurity service providers, law enforcement, and government agencies to assign an identity to different adversaries.

- Recognizing and tracking an adversary's attack vectors can help organizations better defend against existing or upcoming targeted attacks.



Malware

NIST 800-83 defines malware as:

"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim."

Note: A malware is a software with malicious intent (so, it's a potential attack vector).
It usually exploits the vulnerabilities of other software and/or systems.
It's one of the main categories of threats that is required to execute an attack (however, is not the only one).

Table 6.1 Malware Terminology

Name	Description
Advanced Persistent Threat (APT)	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by-download	An attack using code on a compromised website that exploits a browser Vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.

Table 6.1 Malware Terminology (2 of 3)

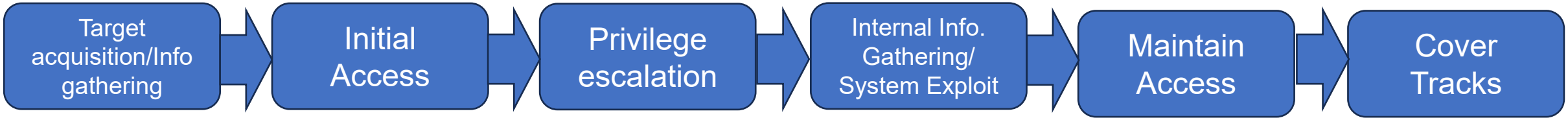
Name	Description
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a Predefined condition is met; the code then triggers some payload.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a Document or document template, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script and macro) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.

General Intruder Behavior in staged attack

Intruders typically use steps from a common attack methodology.

- Even if specific techniques and tools evolve as much as new vulnerabilities are found and patched

a) Target acquisition and information gathering
b) Initial access
c) Privilege escalation
d) Information gathering or system exploit
e) Maintaining access
f) Covering tracks



(a) Target Acquisition and Information Gathering

Where the attacker identifies and characterizes the target systems using publicly available information, both technical and non-technical, and the use network exploration tools to map target resources.

Examples

- Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific Web server and OS used.
- Gather information on target network using DNS lookup tools such as dig, host, and others; and query WH OIS database.
- Map network for accessible services using tools such as NMAP.
- Send query email to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
- Identify potentially vulnerable services, for example, vulnerable Web CMS.

(b) Initial Access

The initial access to a target system, typically by exploiting a remote network vulnerability, by guessing weak authentication credentials used in a remote service, or via the installation of malware on the system using some form of social engineering or drive-by-download.

Examples

- Brute force (guess) a user's Web content management system (CMS) password.
- Exploit vulnerability in Web CMS plugin to gain system access.
- Send spear-phishing e-mail with link to Web browser exploit to key people.

(c) Privilege Escalation

Actions taken on the system, typically via a local access vulnerability, to increase the privileges available to the attacker to enable their desired goals on the target system.

Examples

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

(d) Information Gathering or System Exploit

Actions by the attacker to access or modify information or resources on the system, or to navigate to another target system *(lateral movements)*.

Examples:

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

Actions such as the installation of backdoors or other malicious software, or through the addition of covert authentication credentials or other configuration changes to the system, to enable continued access by the attacker after the initial attack.

Examples:

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

(f) Covering Tracks

Where the attacker disables or edits audit logs, to remove evidence of attack activity, and uses rootkits and other measures to hide covertly installed files or code.

Examples

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

Advanced Persistent Threats (APT) and models

CalPolyPomona

Advanced Persistent Threats (APTs)

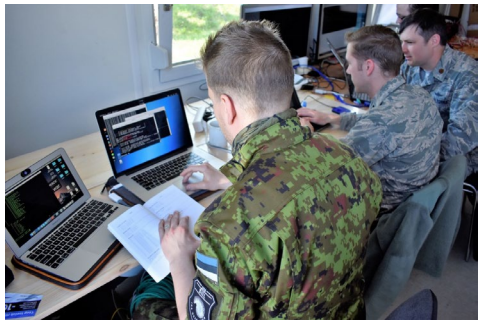
- Well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets (usually business or political)
- Typically attributed to state-sponsored organizations and criminal enterprises
- Differ from other types of attack by their careful target selection and stealthy intrusion efforts over extended periods
- High-profile attacks include *Aurora, RSA, APT1, and Stuxnet*
  - I.e., attacks funded and developed by special teams supported by governments

APT Characteristics (1 of 2)

- **Advanced**
  - Used by the attackers of a **wide variety of intrusion technologies and** malware including the development of **custom malware** if required
    - For example, Zero day exploits, social engineering, phishing
  - The individual components may not necessarily be technically advanced but a carefully selected to **suit the chosen target**

- **Persistent**
  - Determined application of the attacks over an **extended period** against the chosen target in order to maximize the chance of success
  - A variety of **attacks may be progressively applied** until the target is compromised

APT Characteristics (2 of 2)



- **Threats**
  - Threats to the selected targets as a result of the **organized, capable, and well-funded attackers** intent **to compromise** the specifically **chosen targets**
  - The **active involvement of people** in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks
    - I.e., many experts of specific target systems and devices are involved in the creation of malwares and attack strategies.
    - For example, experts of specific software installed inside a commercial industrial control system, electric system, power plant, machine, etc.

E.g., APT against banks: https://www.banktech.com/anatomy-of-an-advanced-persistent-threat-attack/a/d-id/1316528.html

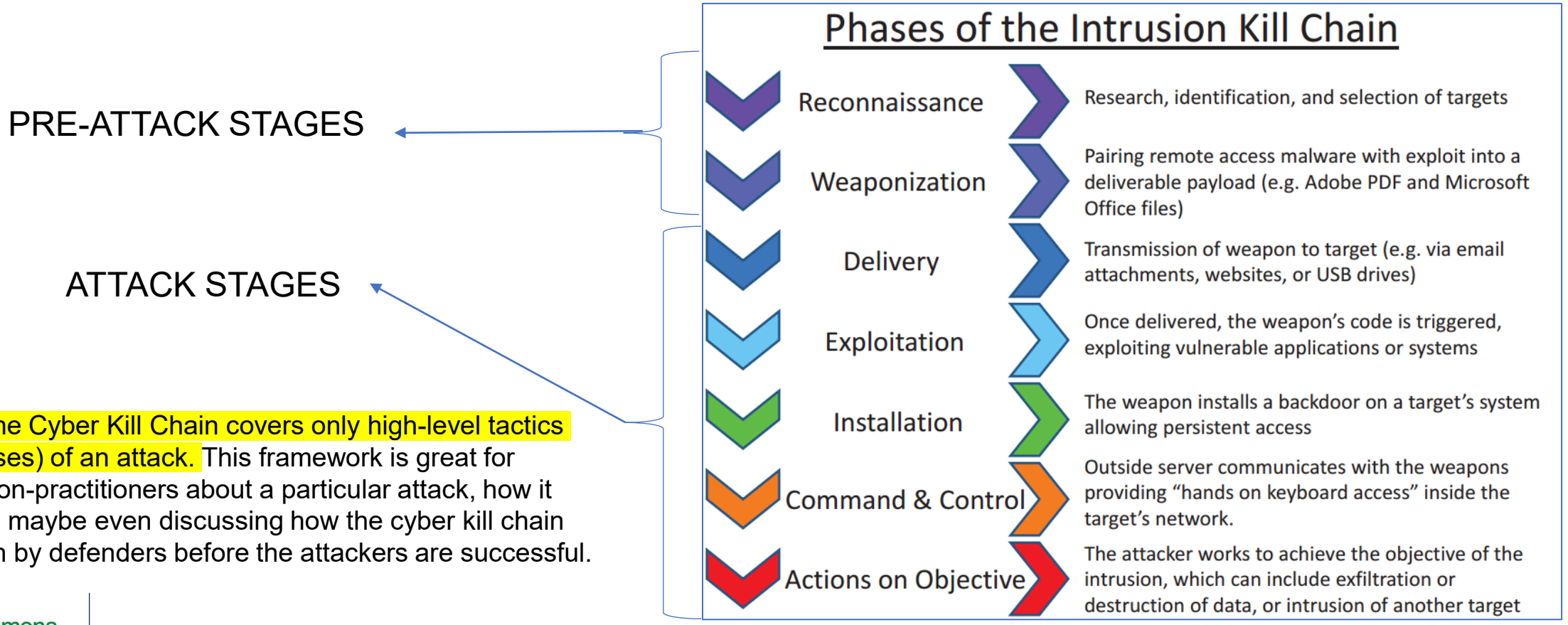
APT and Zero-day exploits

- **APT make large use of Zero-day exploits**
- APT attackers often conduct their own security vulnerability research in an attempt to discover vulnerabilities that are not known to other attackers or cybersecurity teams.
- After they uncover a vulnerability, they do not disclose it but rather store it in a vulnerability repository for later use.
- Zero-day attacks are particularly dangerous because they are unknown to product vendors, and therefore, no patches are available to correct them. APT actors who exploit zero-day vulnerabilities are often able to easily compromise their targets.
  - Stuxnet is one of the most well-known examples of an APT attack. The Stuxnet attack, traced to the U.S. and Israeli governments, exploited zero-day vulnerabilities to compromise the control networks at an Iranian uranium enrichment facility.

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

Staged cyber attacks models: Cyber Kill Chain by Lockheed Martin

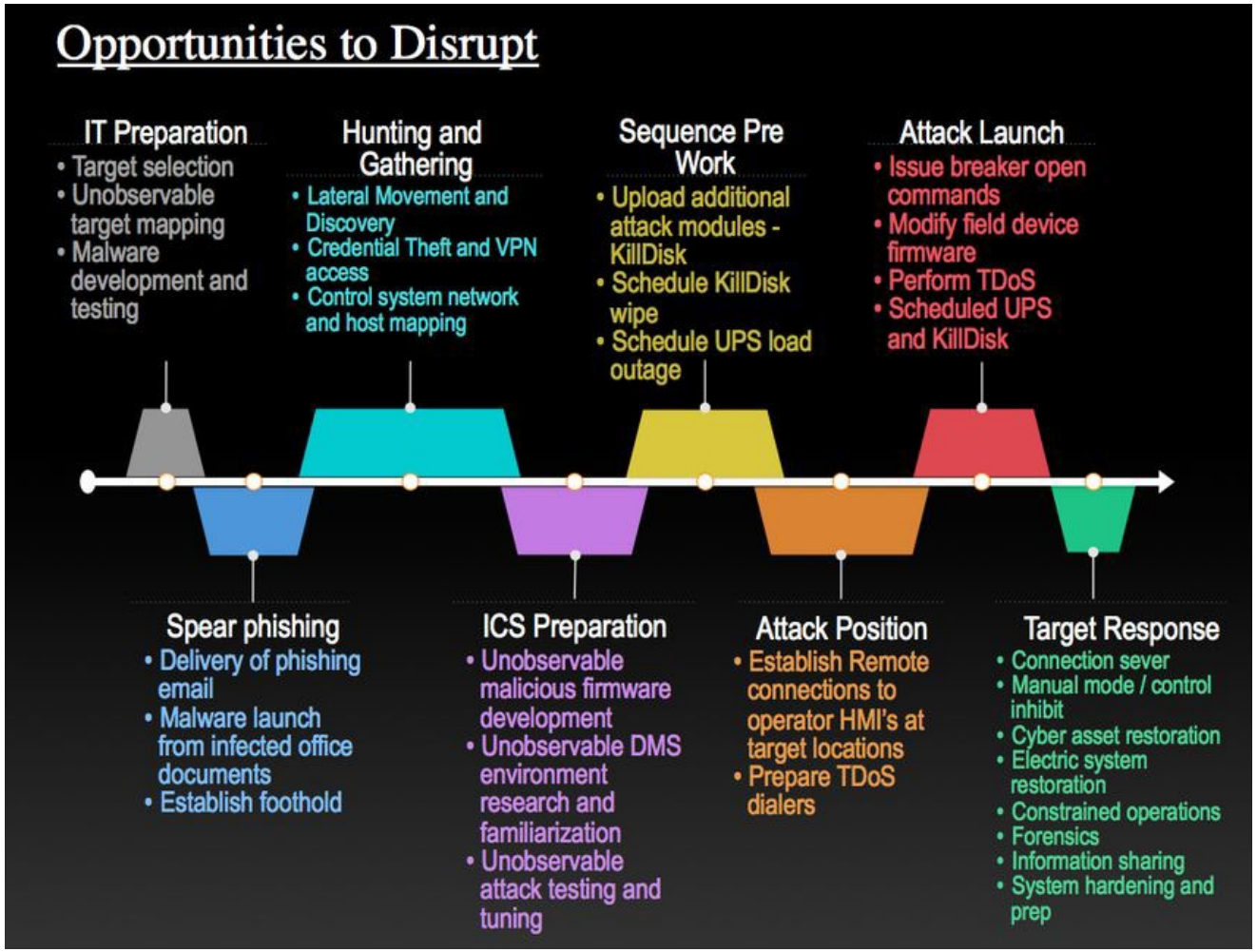
- In 2011, Lockheed Martin published Cyber Kill Chain as one of the first attempts to explain how APT attacks work. The Cyber Kill Chain covers 7 high level goals, or tactics, attackers perform during an attack. As one can see from the original publication, these 7 steps are very easy to understand and communicate



Problems is the Cyber Kill Chain covers only high-level tactics (goals or phases) of an attack. This framework is great for speaking to non-practitioners about a particular attack, how it occurred, and maybe even discussing how the cyber kill chain can be broken by defenders before the attackers are successful.

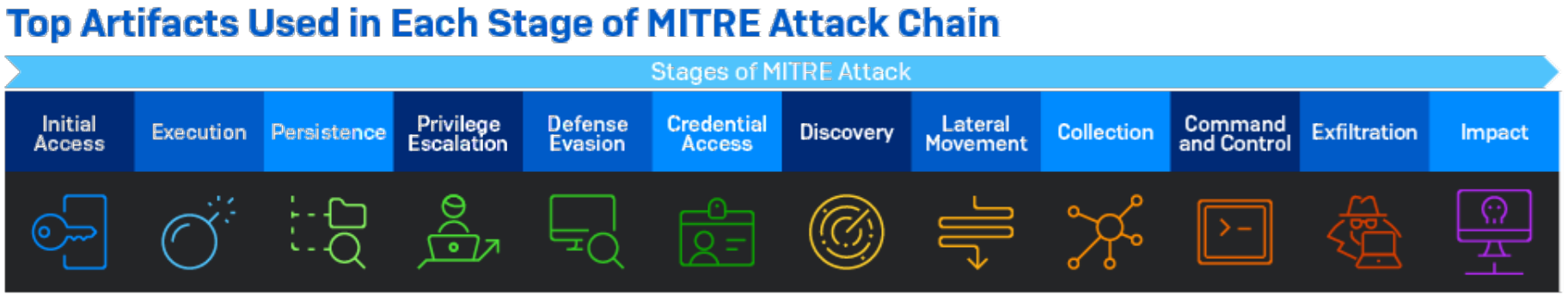
Example: Attack to the Ukraine power grid in 2015 (SANS report)

On December 23, 2015, the power grid in two western oblasts of Ukraine was hacked, which resulted in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours. The attack took place during the ongoing Russo-Ukrainian War (2014-present) and is attributed to a Russian advanced persistent threat group known as "Sandworm". It is the first publicly acknowledged successful cyberattack on a power grid.



Cyber Kill Chain model - MITRE ATT&CK

- In 2015, MITRE released ATT&CK: Adversary Tactics, Techniques, and Common Knowledge. This is the current industry standard and most used framework for understanding and communicating how attacks work. It goes a step further than the Cyber Kill Chain by expanding the attackers' high-level goals to 14 different tactics.



https://doc.sophos.com/central/mdr/help/en-us/welcomeguides/mdr/index.html

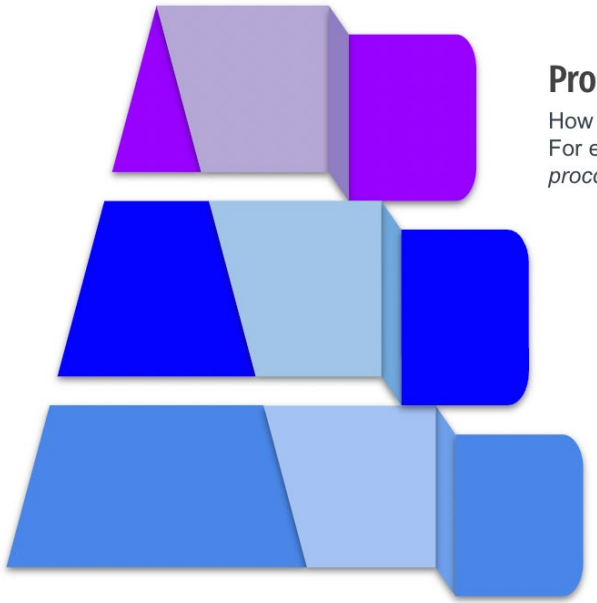
MITRE ATT&CK framework (enterprise - map view)

https://attack.mitre.org/

Tactics, Techniques, and Procedures (TTP)

Tactics, Techniques, and Procedures (TTP) is the method used by IT and military professionals to determine the behavior of a threat actor (hacker). These three elements help you understand your adversaries better.

- **Procedures –** Procedures are the specific implementation the adversary uses for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim. Procedures are categorized in ATT&CK as the observed in the wild use of techniques in the "Procedure Examples" section of technique pages.
- **Techniques –** Techniques represent ‘‘how’’ an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.
  - **Sub-techniques** are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique. For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets.
- **Tactics –** Tactics represent the ‘‘why’’ of an ATT&CK technique or sub-technique. It is the adversary’s tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.



Procedures

How the technique was carried out.
For example, the attacker used
procdump -ma lsass.exe lsass_dump

Techniques

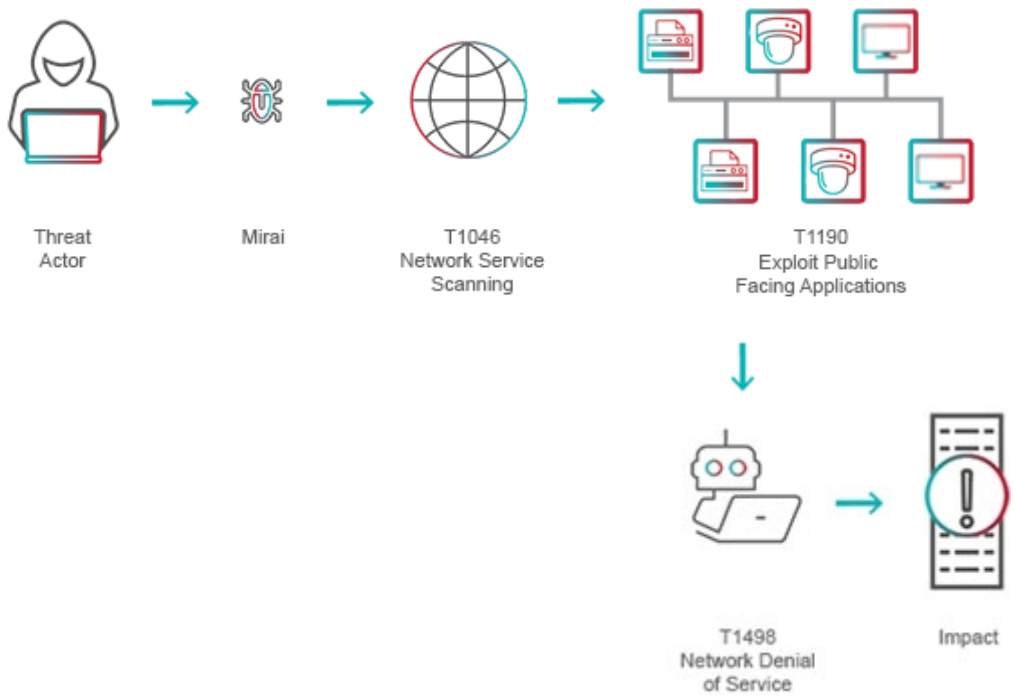
Techniques represent the tactical goal of the procedure. For example, T1003.001 - OS Credential Dumping: LSASS Memory.

Tactics

Tactics represent the strategic goal of the adversary. For example, TA006 - Credential Access

Example of TTP from a kill chain

- **Mirai** is a piece of malware that turns IoT devices (e.g., Internet cameras) running the Linux operating system into controlled 'bots' that can be used as part of a botnet in large-scale network DDoS attacks.



Check the TTP IDs on Mitre

Impact	Technique	ID	Description
Initial Access	Exploit Public-Facing Applications	T1190	Mirai variants take advantage of design vulnerabilities in internet facing IoT devices by exploiting SSH/Telnet
Lateral Movement	Exploitation of Remote Services	T1210	Mirai variants spread through remote code execution (RCE) vulnerabilities
Discovery	Network Service Scanning	T1046	Mirai conducts internet wide scans to discover new vulnerable IoT devices
Credential Access	Brute Force	T1110	Mirai leverages a list of hardcoded credentials to brute force IoT devices through Telnet and SSH
Execution	Exploitation for Client Execution	T1203	Demonbot was observed attempting to exploit known vulnerabilities in Hadoop
Command and Control	Domain Generation Algorithms	T1520	A Mirai variant was observed using DGA for protecting its command and control infrastructure
Defense Evasion	Connection Proxy	T1090	Botnets such as OMG, VPNFilter create anonymizing proxy networks through socks enabled bots leveraging open source software such as 3proxy. UPnP vulnerabilities in consumer routers have been abused to create port forwarding schemes that conceal malicious communications and attacks through port-hopping across multiple routers
Impact	Network Denial of Service	T1498	Mirai can conduct network denial-of-service attacks
Impact	Endpoint Denial of Service	T1499	Mirai can conduct endpoint denial-of-service attacks such as simple HTTP(S) floods

Unified Kill Chain model

In 2017, Paul Pols published the Unified Cyber Kill Chain to overcome and expand on the Cyber Kill Chain of Lockheed Martin and MITRE. (This is an Academic attempt to model attacks rather than purely technical)

The Unified Kill Chain			
1	***Reconnaissance***	*Researching, identifying and selecting targets using active or passive reconnaissance.*	*In* stage or *Initial Foothold*
2	***Weaponization***	*Preparatory activities aimed at setting up the infrastructure required for the attack.*	
3	***Delivery***	*Techniques resulting in the transmission of a weaponized object to the targeted environment.*	
4	***Social Engineering***	*Techniques aimed at the manipulation of people to perform unsafe actions.*	
5	***Exploitation***	*Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.*	
6	***Persistence***	*Any access, action or change to a system that gives an attacker persistent presence on the system.*	
7	***Defense Evasion***	*Techniques an attacker may specifically use for evading detection or avoiding other defenses.*	
8	***Command & Control***	*Techniques that allow attackers to communicate with controlled systems within a target network.*	
9	***Pivoting***	*Tunneling traffic through a controlled system to other systems that are not directly accessible.*	*Through* stage or *Network Propagation*
10	***Discovery***	*Techniques that allow an attacker to gain knowledge about a system and its network environment.*	
11	***Privilege Escalation***	*The result of techniques that provide an attacker with higher permissions on a system or network.*	
12	***Execution***	*Techniques that result in execution of attacker-controlled code on a local or remote system.*	
13	***Credential Access***	*Techniques resulting in the access of, or control over, system, service or domain credentials.*	
14	***Lateral Movement***	*Techniques that enable an adversary to horizontally access and control other remote systems.*	
15	***Collection***	*Techniques used to identify and gather data from a target network prior to exfiltration.*	*Out* stage or *Action on Objectives*
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.*	

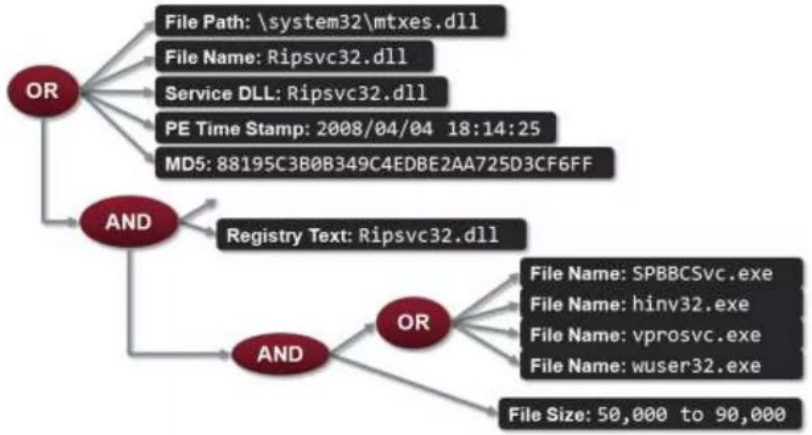
Digital forensics and threat intelligence

CalPolyPomona

Indicator of Compromise (IOC)

- An **Indicator of Compromise (IOC)** is a piece of digital forensics that suggests that an endpoint or network may have been breached.
- Just as with physical evidence, these digital clues help information security professionals identify malicious activity or security threats, such as data breaches, insider threats or malware attacks.

- Way of describing threat data like
  - Malware
  - Attacker Methodology
  - Evidence of compromise or activity
- What Is An Indicator?
  - MD5: Change Frequently
  - File Names/Directories: Many Reused
  - Registry Key Values: Many Reused
  - Services With Wrong Service dll's: Outliers
  - IPs and Domain Names: Change Frequently

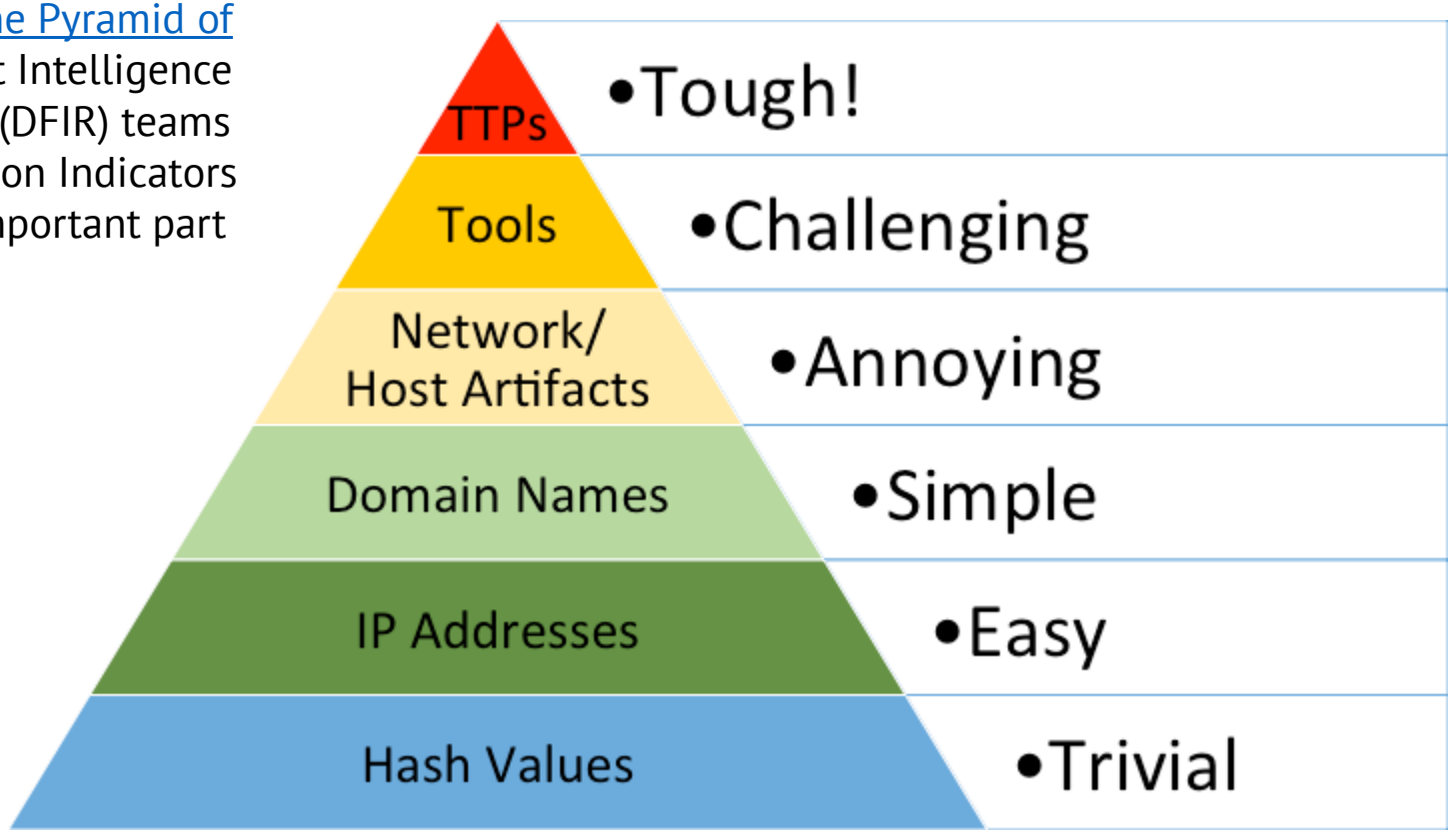


More examples:

- Unusual inbound and outbound network traffic
- Geographic irregularities, such as traffic from countries or locations where the organization does not have a presence
- Unknown applications within the system
- Unusual activity from administrator or privileged accounts, including requests for additional permissions
- An uptick in incorrect log-ins or access requests that may indicate brute force attacks
- Anomalous activity, such as an increase in database read volume
- Large numbers of requests for the same file
- Suspicious registry or system file changes
- Unusual Domain Name Servers (DNS) requests and registry configurations
- Unauthorized settings changes, including mobile device profiles
- Large amounts of compressed files or data bundles in incorrect or unexplained locations

The Pyramid of Pain

In 2013, David Bianco, a SANS instructor, authored The Pyramid of Pain which covers the different forms of Cyber Threat Intelligence provided by Digital Forensics and Incident Response (DFIR) teams after an incident. The bottom of the pyramid focuses on Indicators of Compromise, while the top focuses on the most important part for Tactics, Techniques, and Procedures.

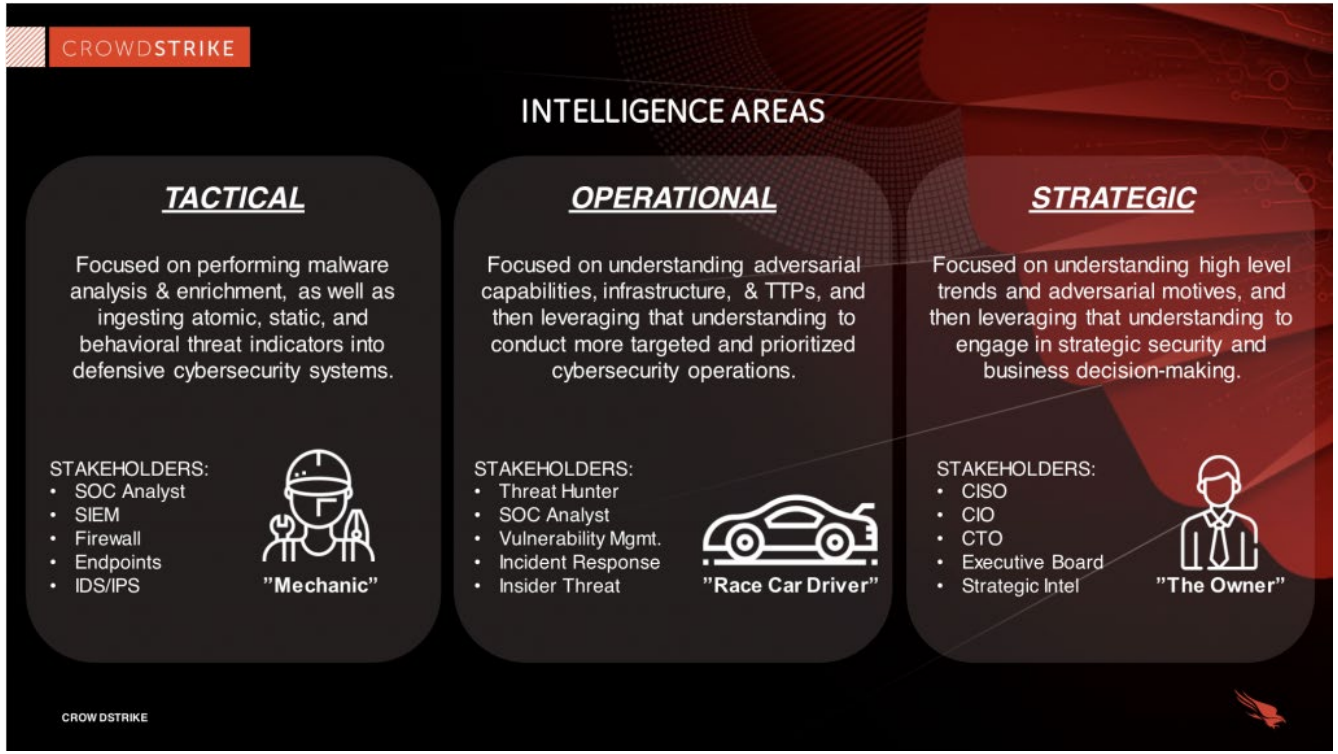


https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Cyber Threat Intelligence

Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets. – Gartner

1. **Tactical:** exchange/obtain **IOC** from feeds or internal intelligence.
   It's a very technical process of data collection about threats, to prepare/update defensive systems.
2. **Operational:** It gives insight into the origin and complexity of the group(s) involved and aids responders in comprehending the type, intent, and timeframe of a specific attack, hence, preventing next steps. (in other words, a Context for attack stages connected to APTs or known or unknown groups).
3. **Strategic:** It shows how global events, foreign policies, and other long-term local and international movements can potentially impact the cyber security of an organization.



Open-source intelligence (OSINT)

- Threat intelligence feeds are a critical part of TI. Widely available online, these feeds record and track IP addresses and URLs that are associated with phishing scams, malware, bots, trojans, adware, spyware, ransomware and more. Open source threat intelligence feeds can be extremely valuable—if you use the right ones. While these collections are plentiful, there are some that are better than others.

Tools to generate and share intelligence among partner organizations, Countries, groups:

- **MISP**
- **TheHive**
- **Cortex**
- **Yeti**
- **Cuckoo Sandbox**
- **OpenCTI (Open Cyber Threat Intelligence)**
- **T-Pot**

Open-Source Threat Intelligence Feeds:

- **AlienVault Open Threat Exchange (OTX)**
- **Cyber Threat Intelligence Network (CTIN)**
- **Abuse.ch**
- **CIRCL (Computer Incident Response Center Luxembourg) Passive DNS and Passive SSL**
- **Spamhaus**
- **PhishTank**
- **Malware Domain List**
- **SANS Internet Storm Center (ISC)**

Testing strategies

CalPolyPomona

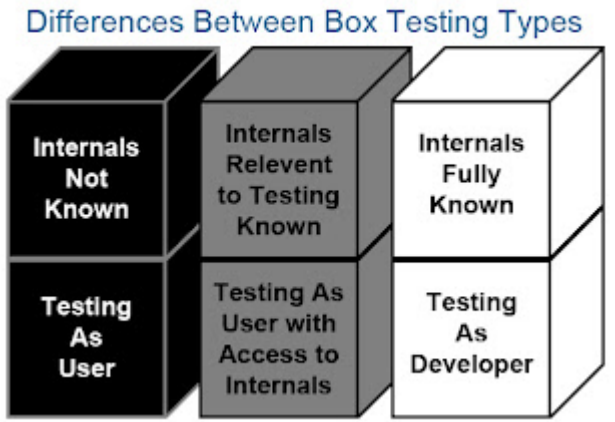
White hats: Penetration testing and testing modes

- ***Penetration testing*** (or ***pen testing***)**:** challenges a network's security. Given the value of a business's network, it is imperative that businesses consult with experts before pen testing. Experts can ensure that testing does not damage the network, and they can also provide better insights into vulnerabilities. Pen testing experts can help businesses before, during, and after the tests to help obtain useful and beneficial results.

•**White box testing** — in this format, pen testers have full access and knowledge of the systems they are testing, including source code, IP addresses, etc. Also sometimes called clear or open box testing, this approach can simulate an internal attack and allows for an extremely rigorous test.

•**Black box testing** — unlike white box scenarios, testers here have no information about the systems they will attempt to breach. Because of this, these tests often take longer to complete, as they may rely heavily on an automated, trial & error approach.

•**Gray box testing** — as the name indicates, this approach is a combination of the other two approaches. Testers have some visibility and can pose as an attacker who has gathered limited information about the target.

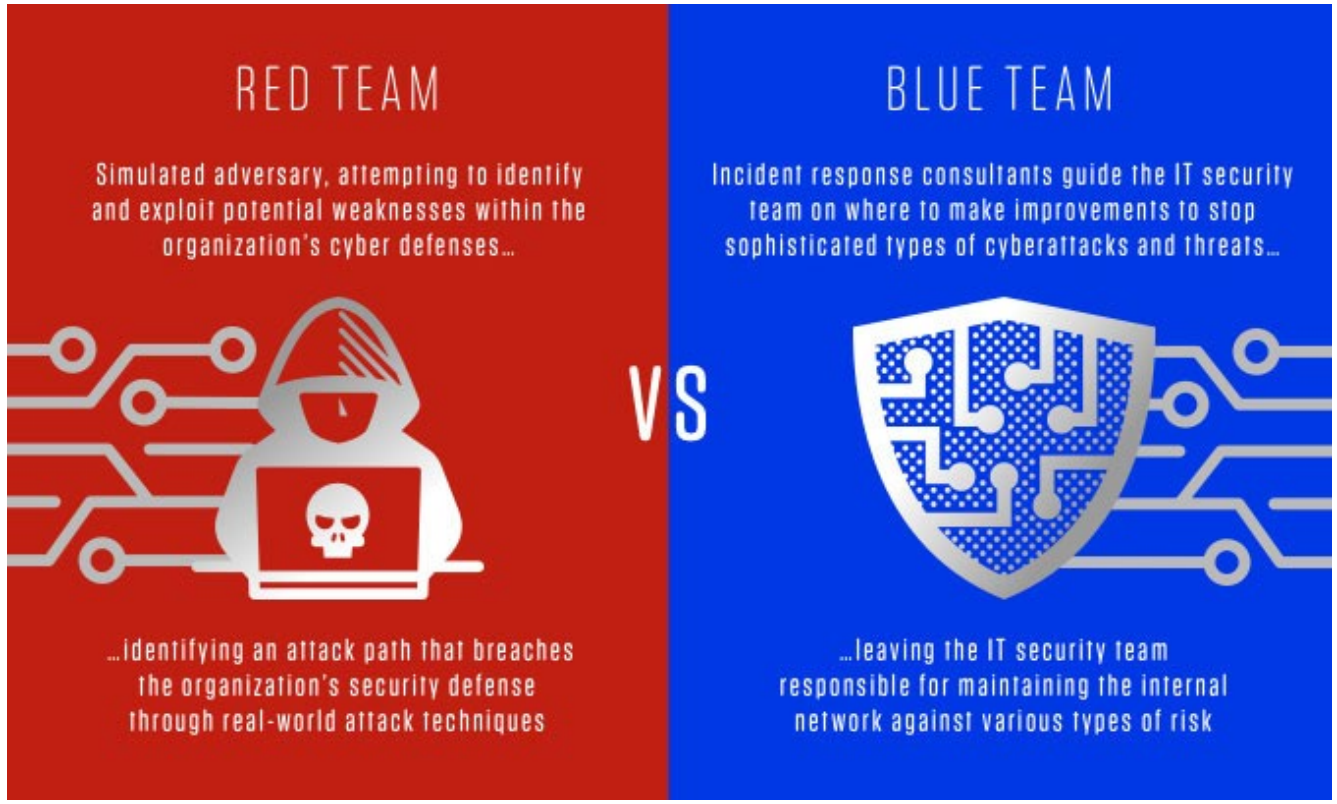


Red/Blue teaming

In a **red team/blue team** exercise, the **red team** is made up of offensive security experts who try to attack an organization's cybersecurity defenses. The **blue team** defends against and responds to the red team attack.

- Red team/blue team simulations play an important role in defending the organization against a wide range of cyberattacks from today's sophisticated adversaries. These exercises help organizations:
  - Identify points of vulnerability as it relates to people, technologies and systems
  - Determine areas of improvement in defensive **incident response** processes across every phase of the kill chain
  - Build the organization's first-hand experience about how to detect and contain a targeted attack
  - Develop response and remediation activities to return the environment to a normal operating state

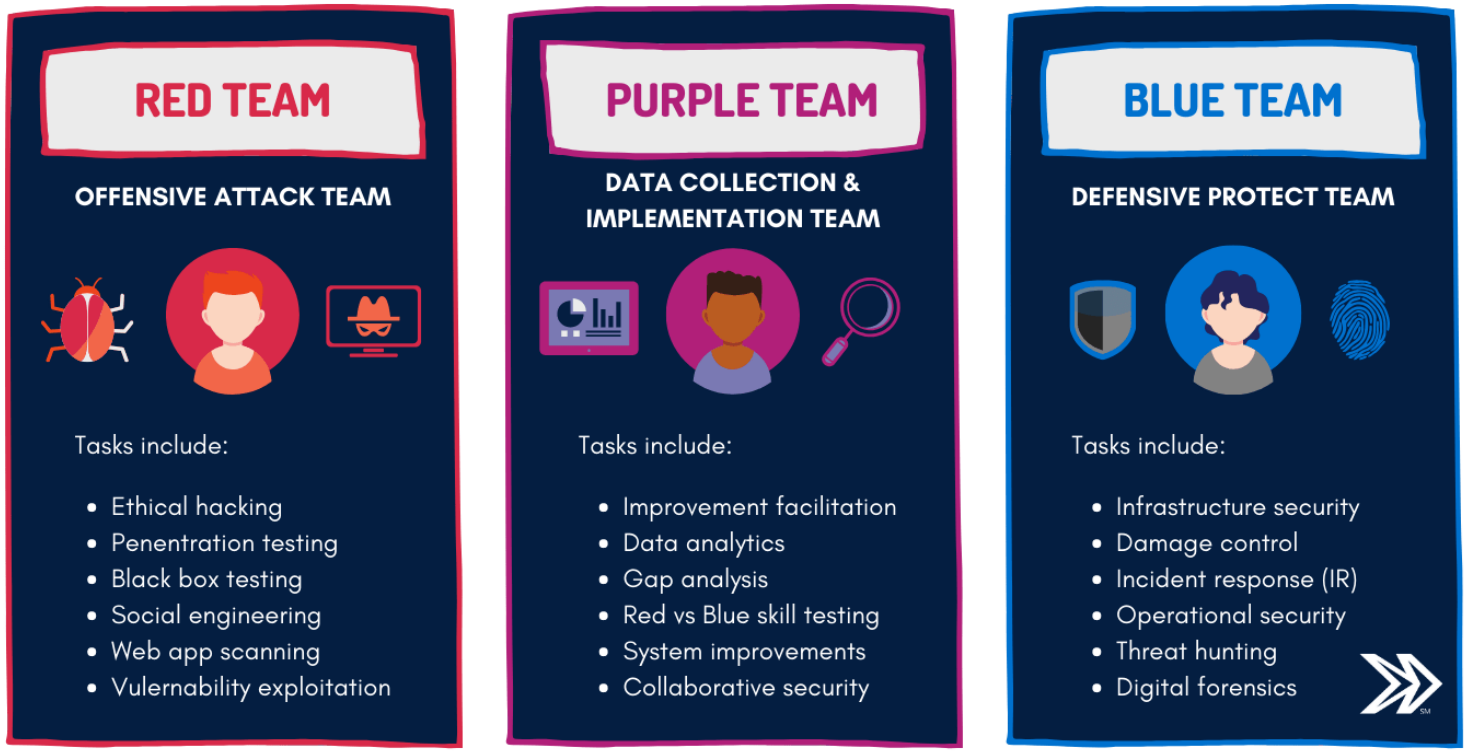
https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/



Red vs Blue and Purple team

The Purple Team is, unsurprisingly, the joining of the insights from Red and Blue.

In the purple team, the offensive and defensive professionals work in sync. For instance, a purple team might decide to work on a particular security section; say, broken authentication. The offensive security professionals don't just start scouting for vulnerabilities. They work together with the defense to find out weak points and patch the vulnerabilities that might arise.



https://gomindsight.com/insights/blog/red-team-vs-blue-team/

Observation: PenTester vs Red Team

- The main objective of penetration tests is to identify exploitable vulnerabilities and gain access to a system. On the other hand, in a red-team exercise, the goal is to access specific systems or data by emulating a real-world adversary and using tactics and techniques throughout the attack chain, including privilege escalation and exfiltration.

	Penetration testing	Red teaming
Objective	Identify exploitable vulnerabilities and gain access to a system.	Access specific systems or data by emulating a real-world adversary.
Timeframe	Short: One day to a few weeks.	Longer: Several weeks to more than a month.
Toolset	Commercially available pen-testing tools.	Wide variety of tools, tactics and techniques, including custom tools and previously unknown exploits.
Awareness	Defenders know a pen test is taking place.	Defenders are unaware a red team exercise is underway.
Vulnerabilities	Known vulnerabilities.	Known and unknown vulnerabilities.
Scope	Test targets are narrow and pre-defined, such as whether a firewall configuration is effective or not.	Test targets can cross multiple domains, such as exfiltrating sensitive data.
Testing	Security system is tested independently in a pen test.	Systems targeted simultaneously in a red team exercise.
Post-breach activity	Pen testers don't engage in post-breach activity.	Red teamers engage in post-breach activity.
Goal	Compromise an organization's environment.	Act like real attackers and exfiltrate data to launch further attacks.
Results	Identify exploitable vulnerabilities and provide technical recommendations.	Evaluate overall cybersecurity posture and provide recommendations for improvement.

https://www.ibm.com/blog/red-teaming-101-what-is-red-teaming/