Penetration Testing and Red Teaming Operations

The offensive approaches to cyber security

@August 2021

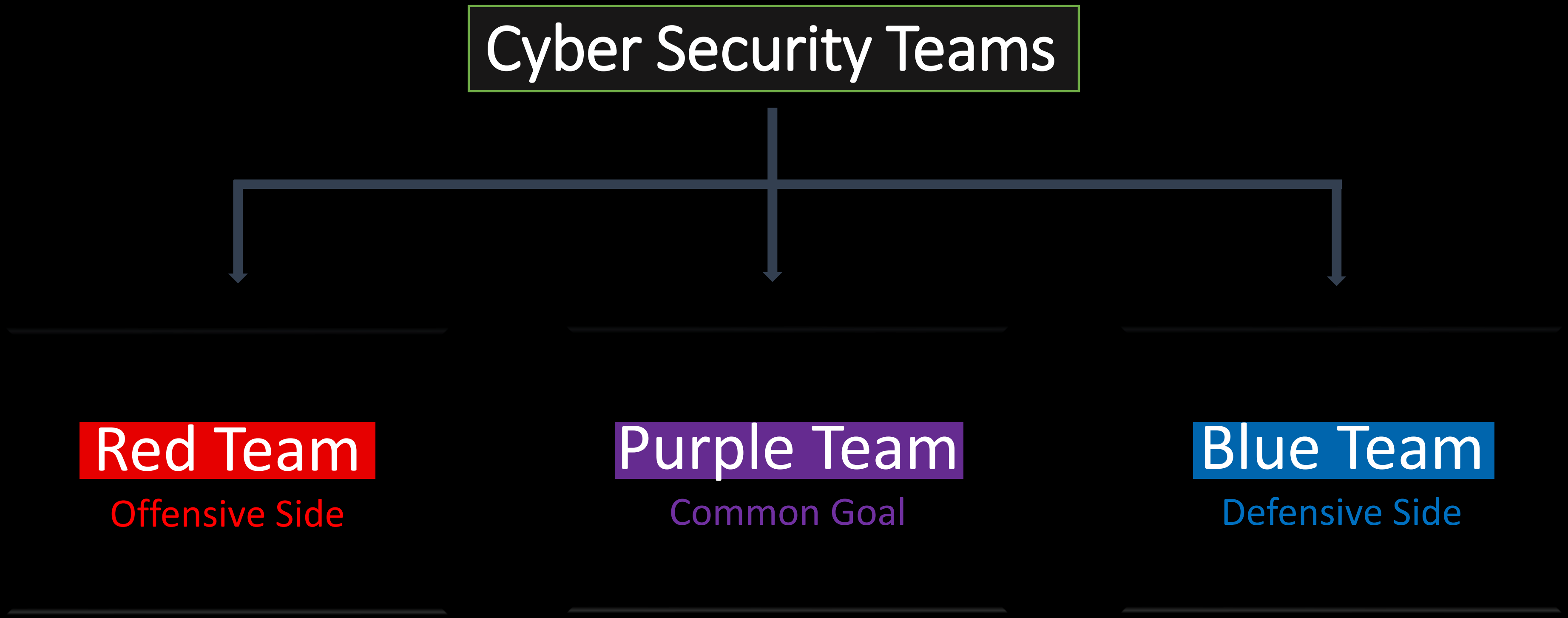
❑ Agenda

- About Me
- Cyber Security Teams and Roles
- Offensive Approaches to Cyber Security
  - Vulnerability Assessment
  - Penetration Testing
  - Red Teaming
- Tactics, Techniques and Procedures (TTPs) - MITRE ATT&CK
- Penetration Testing and Red Teaming Attack Lifecycles
- Command & Control Server (C2) Frameworks
- Required Skills for Red Teamers
- Red Teaming Certifications
- Q&A

❑ About Me

- Name: Phuon, Seang Y
- Title: Cyber Security Consultant @ Global Big-4 Firm
- Certifications:
  - Certified Ethical Hacker (C|EH - Practical)
  - Offensive Security Certified Professional (OSCP)
  - Certified Red Team Operator (CRTO) – Zero-Point Security – UK
  - Bachelor Degree of Computer Science and Engineering (CSE) - RUPP
- More than 5 years of experience in Ethical Hacking – VAPT

❑ Cyber Security Team and Roles



Cyber Security Teams

Red Team
Offensive Side

Purple Team
Common Goal

Blue Team
Defensive Side

@August 2021

❑ Offensive Approaches To Cyber Security

- Vulnerability Assessment
- Penetration Testing
- Red Teaming

❑ Offensive Approaches To Cyber Security

- Vulnerability Assessment

  The process of identifying vulnerabilities without exploitation attempt once identified.

❑ Offensive Approaches To Cyber Security

- Penetration Testing

  The process of identifying vulnerabilities and exploit the vulnerabilities once identified.

❑ Offensive Approaches To Cyber Security

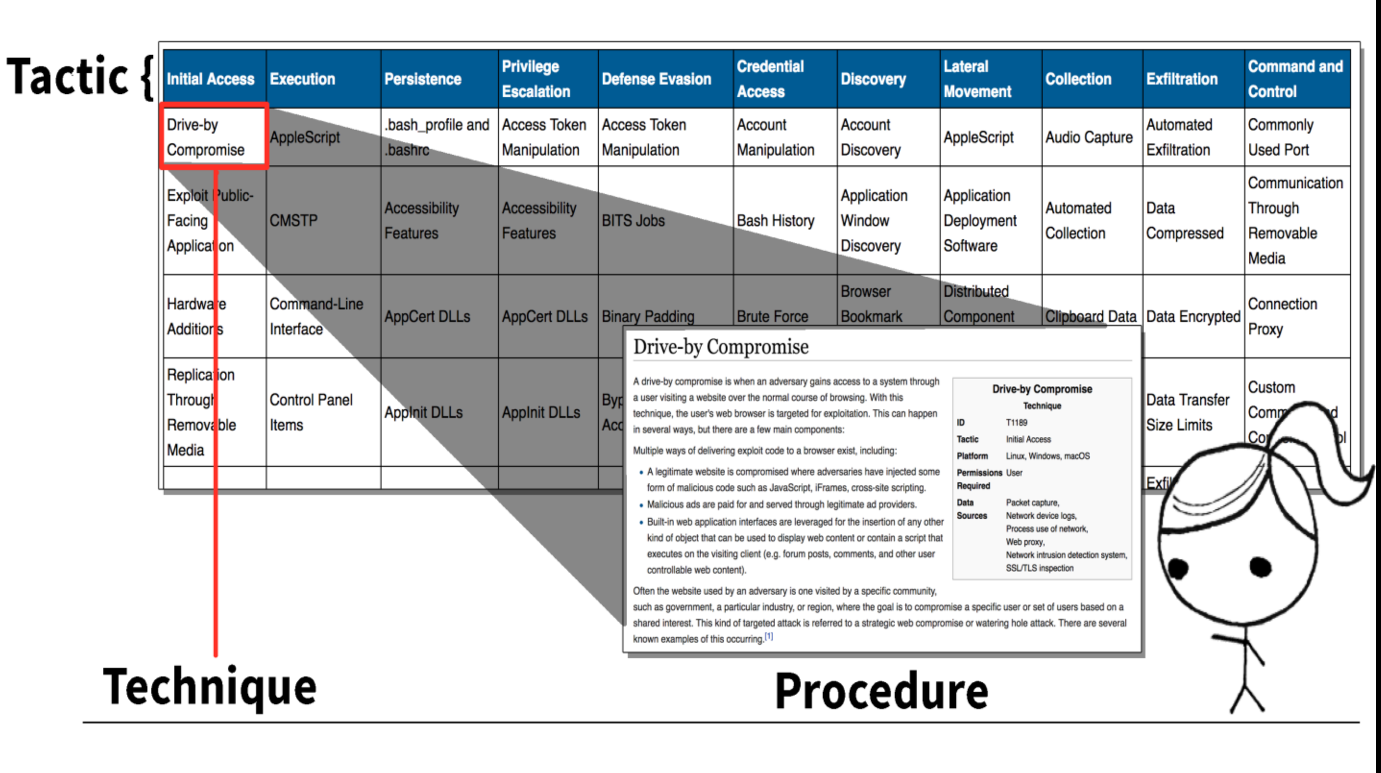
- Red Teaming

  The process of using Tactics, Techniques, and Procedures (TTPs) to emulate real-world threats with the goal of training and measuring the effectiveness of the people, processes, and technology used to defend an environment.

@https://redteam.guide/docs/definition-lexicon/

@August 2021

❑ Tactics, Techniques and Procedures (TTPs)



Tactic {

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark	Distributed Component	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Byp Acc					Data Transfer Size Limits	Custom Comm d Co l
									Exfil	

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.[1]

Drive-by Compromise	
Technique	
ID	T1189
Tactic	Initial Access
Platform	Linux, Windows, macOS
Permissions Required	User
Data Sources	Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection

Technique

Procedure

MITRE | ATT&CK®

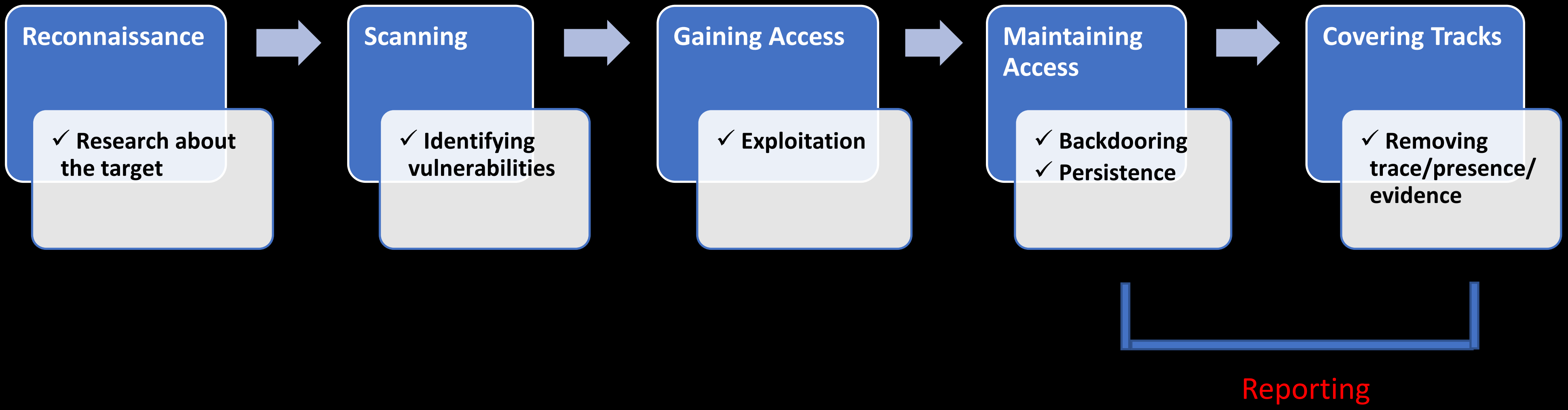
ATT&CK®

@https://attack.mitre.org/
@https://redteam.guide/docs/concepts/mitre_attack/

@August 2021

❑ Penetration Testing and Red Teaming Attack Lifecycles

➢ Penetration Testing Phases/Lifecycle



Reconnaissance
- ✓ Research about the target

Scanning
- ✓ Identifying vulnerabilities

Gaining Access
- ✓ Exploitation

Maintaining Access
- ✓ Backdooring
- ✓ Persistence

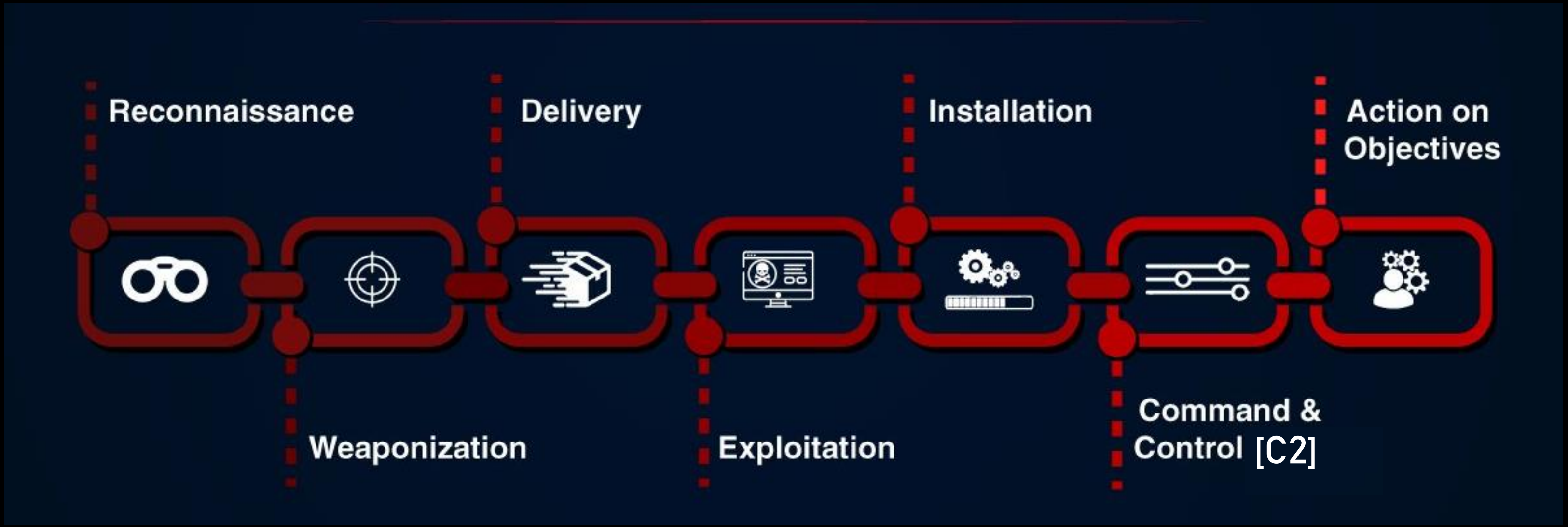
Covering Tracks
- ✓ Removing trace/presence/ evidence

Reporting

@August 2021

❑ Penetration Testing and Red Teaming Attack Lifecycles

- Red Teaming Attack Phases/Lifecycle – Cyber Kill Chain

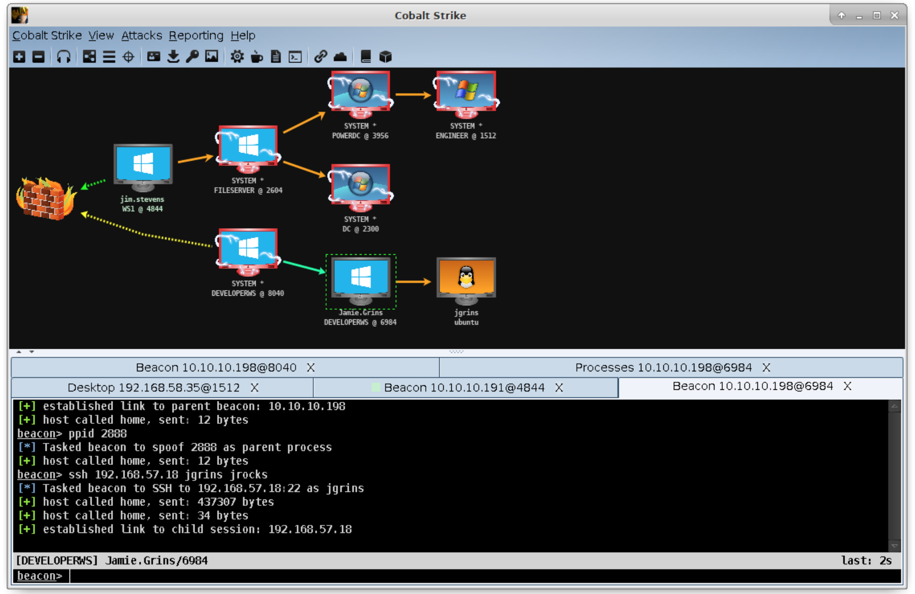


@https://www.eccouncil.org/
@https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

@August 2021

❑ Command & Control Server (C2) Frameworks

- C2 Frameworks
  - Cobalt Strike
  - PowerShell Empire
  - Metasploit Framework
  - Covenant C2
  - Others



```
[+] established link to parent beacon: 10.10.10.198
[+] host called home, sent: 12 bytes
beacon> ppid 2888
[*] Tasked beacon to spoof 2888 as parent process
[+] host called home, sent: 12 bytes
beacon> ssh 192.168.57.18 jgrins jrocks
[*] Tasked beacon to SSH to 192.168.57.18:22 as jgrins
[+] host called home, sent: 437307 bytes
[+] host called home, sent: 34 bytes
[+] established link to child session: 192.168.57.18

[DEVELOPERWS] Jamie.Grins/6984                                    last: 2s
beacon>
```

@August 2021

Required Skills for Red Teamers

Skills and Mindset

- Adversary/Hacker’s Mindset
- Hacking Experience – Bypassing Defense (AV, AMSI, AppLocker and CLM etc.), Lateral Movement/Pivoting (Proxying – Tunneling/Socks and Port Forwarding), Active Directory and MSSQL Attacks
- Programing Knowledge and Coding Experience – C#, PowerShell, Python and Others

@https://github.com/tcostam/awesome-command-control

❑ Red Teaming Certifications

➢ Trainings and Certifications

- Certified Red Team Operator (CRTO) – Zero-Point Security
- Certified Red Team Professional (CRTP) – PenTesterAcademy
- Certified Red Team Expert (CRTE) – PenTesterAcademy
- eLearnSecurity Certified Penetration Tester eXtreme (eCPTX) – eLearnSecurity

➢ Others

@OffensiveSecurity

@EC-Council

❑ Question & Answer (Q&A)

Follow Me on Facebook Pages @:

- ភួន សៀងអ៊ី - Phuon Seang Y
- THECybOrg Lab

THE CYBORG LAB

@August 2021