What is the difference between red team hacking and penetration testing?

So you want to be a Red Teamer?

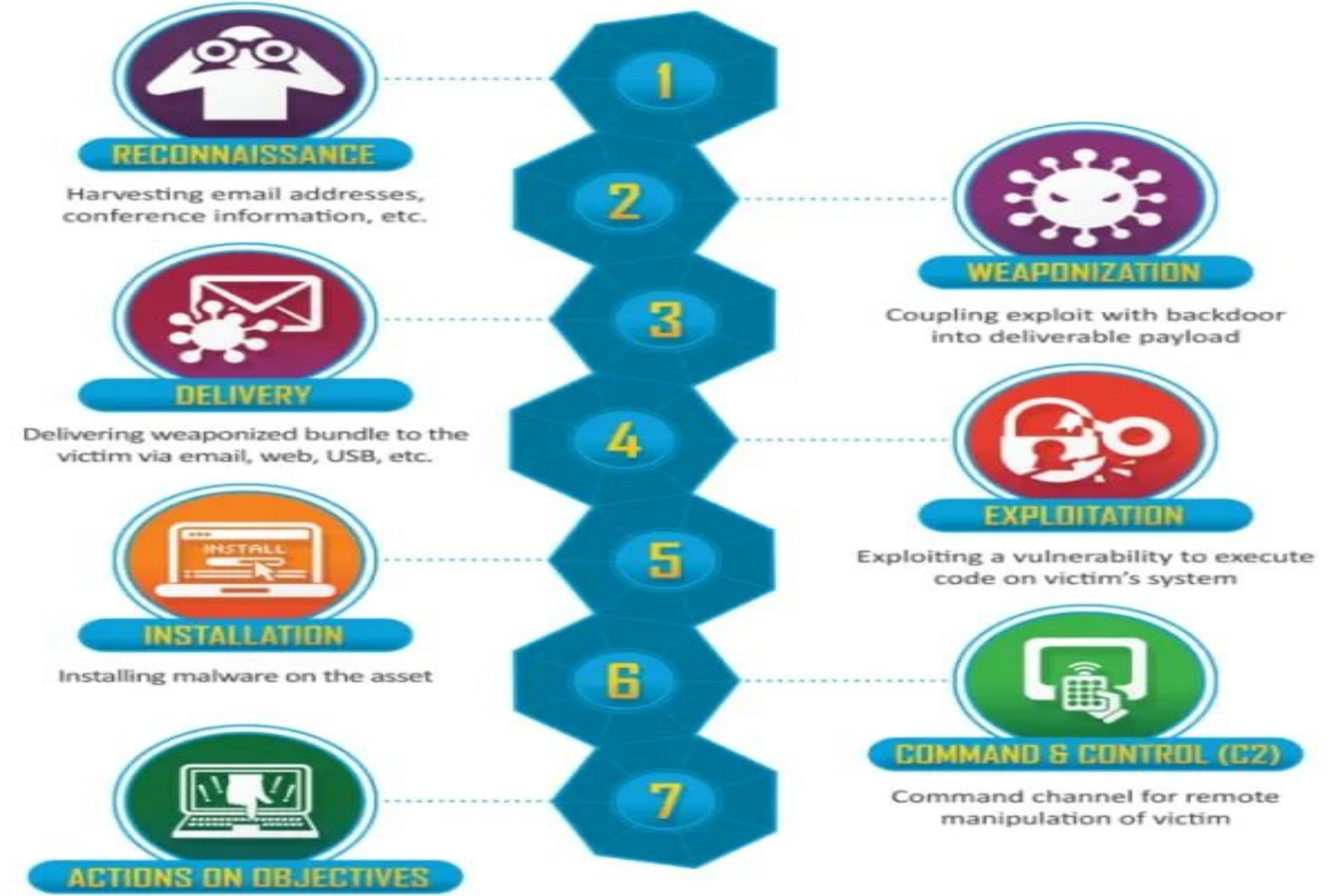
Intro to Red Teaming

Red Teaming

- Hacking engagements can be categorized using military metrics of red, blue and white team hacking.
- Red team is offensive, blue is defensive and white is the entity responsible for defining the Rules of Engagement (ROE) and acting as links to the company management.
- Red teamers attack systems to find entry points/ ways to compromise.
- Mostly operate without the knowledge of the blue team or other staff/employees, to test the company detection and response system and general security posture.

Adversary emulation and TTPs

- APT - Advanced Persistent Threats
- TTPs- Tactics(Objective), technique(How?) and Procedures(steps to) used by known APTs.
- Blue teamers usually use different cyber kill chains to track down APT behaviour and monitor for suspicious activities. Such kill chains include the Lockheed Martin, Unified and Varonis each with a different adversary tactics.
- Red teamers emulate the TTPs that attackers use guided by the cyber kill chain frameworks.



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Lockheed martin cyber kill chain

Reconnaissance: Obtain information on the target. E.g. Harvesting emails, OSINT

Weaponization: Combine the objective with an exploit. Commonly results in a deliverable payload. E.g. Exploit with backdoor, malicious office document, hta,

Delivery: How will the weaponized function be delivered to the target. E.g. Email, web, USB

Exploitation: Exploit the target's system to execute code. E.g. MS17-010, Zero-Logon, etc.

Installation: Install malware or other tooling. E.g Mimikatz, Rubeus, etc.

Command & Control Control: the compromised asset from a remote central controller. E.g Empire, Cobalt Strike, etc.

Actions on Objectives: Any end objectives: ransomware, data exfiltration, etc. e.g.Conti, LockBit2.0, etc.

Red Team CTI and OPSEC

- CTI - Cyber threat Intelligence
- This is basically gathering information about a certain subject from online resources using OSINT.
- In relation to red teaming CTI would be used to build a profile about the target company and gather as much information as possible.
- CTI in relation to red teaming involves observing and imitating attackers behaviours.
- Involve collecting information such as IOCs (Domains, IP, Hashes etc) about attackers. From Blue team POV they use the info to defend against the adversaries.

Red Team CTI and OPSEC

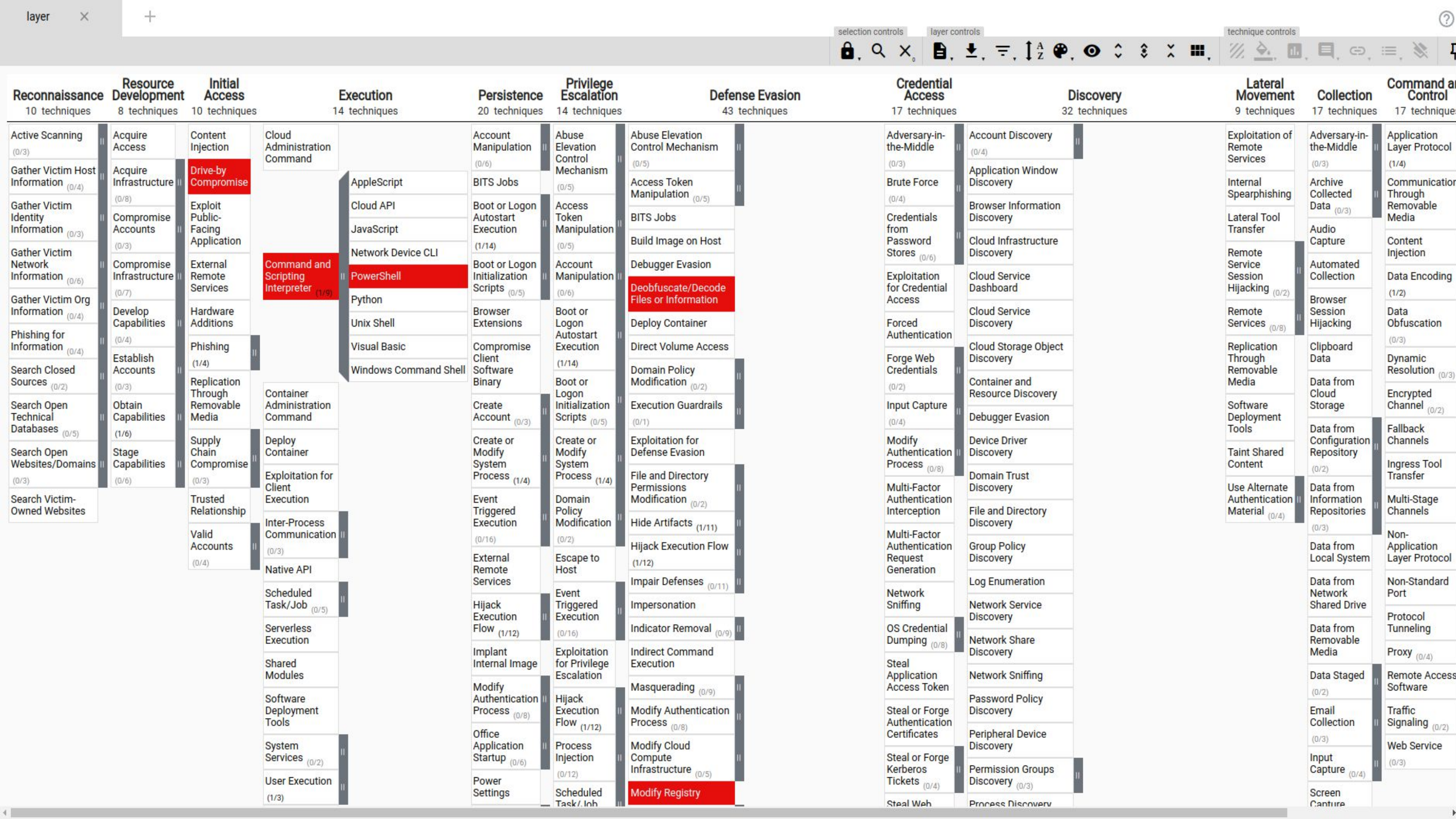
NOTE: CTI is entirely evidence-based. Conducting CTI should be based on evidence collected and not hypothesis.

- Threat Intelligence Campaign:
  - Select a framework and general campaign - e.g. Mitre Att&ck
  - Select adversary group
  - Identify TTPs and IOCs
  - TTPs mapping to cyber kill chain
  - Document an engagement plan and resources

CTI and OPSEC

Types of CTI:

- Tactical - indicators and behaviours done for network level protection. Simple IOCs and such for IT team. Short lifespan, IOCs keep changing
- Operational - work done by threat hunters and incident responders to collect info about threat actor behaviour, advice on remediation and describe threat hunting process. Helps SOC in monitoring and threat analysis. Longer lifespan because it analyses TTPs
- Strategic - describing calculated impact of threat actors to business operations. To be used by executives and business owners.



Reconnaissance
10 techniques

- Active Scanning (0/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (1/6)
- Stage Capabilities (0/6)

Initial Access
10 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/4)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (1/9)
  - AppleScript
  - Cloud API
  - JavaScript
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/3)

Persistence
20 techniques

- Account Manipulation (0/6)
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (1/4)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (1/12)
- Implant Internal Image
- Modify Authentication Process (0/8)
- Office Application Startup (0/6)
- Power Settings

Privilege Escalation
14 techniques

- Abuse Elevation Control Mechanism (0/5)
- Access Token Manipulation (0/5)
- Account Manipulation (0/6)
- Boot or Logon Autostart Execution (1/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (1/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (1/12)
- Process Injection (0/12)
- Scheduled Task/Job

Defense Evasion
43 techniques

- Abuse Elevation Control Mechanism (0/5)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (1/11)
- Hijack Execution Flow (1/12)
- Impair Defenses (0/11)
- Impersonation
- Indicator Removal (0/9)
- Indirect Command Execution
- Masquerading (0/9)
- Modify Authentication Process (0/8)
- Modify Cloud Compute Infrastructure (0/5)
- Modify Registry

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/6)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web

Discovery
32 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/8)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture

Command a Control
17 technique

- Application Layer Protocol (1/4)
- Communication Through Removable Media
- Content Injection
- Data Encoding (1/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

CTI and OPSEC

OPSEC from a red team perspective

- Remain undetected by blue team during the whole operation
- Host and detection evasion techniques
- Use info from recon and CTI to structure your opsec
- Create countermeasures against risks your face in your red team Op

CTI and OPSEC

Three levels of OPSEC

- Understand your CI, your targets and risks you face
- Protect against adversaries
- Go undetected by blue teams

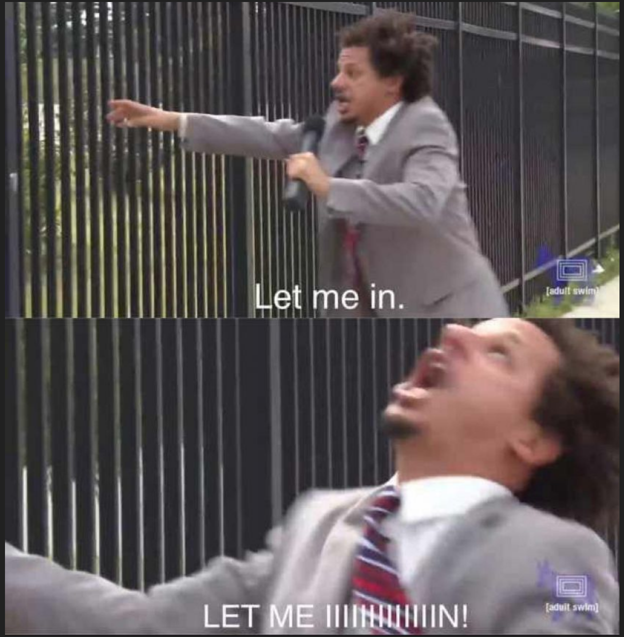
Let’s get our hands dirty

Recon with recon-ng

- Create workspace
- Databases: Domains, hosts, repos, ports etc
- Working with modules
- Marketplace

Demo

- Emulate a certain APTs technique
- MITRE ATT&CK Navigator as guide
- Use a windows vm as target
- Try out various techniques for initial access



Resources

- https://www.ired.team/
- https://redteam.guide/
- https://www.youtube.com/live/ujaoOWmkGLY?si=WN6fm9QddVb7BXoc
- Red team series by hackersploit
- Curiosity!

THANK YOU FOR JOINING

Reach me on twitter: @deanjeager