
Red Teaming & Offensive Security
By Harsh Tandel @ Hack-X MIT WPU Club

$whoami

- CVE 2022-334
- Security Consultant
- P1 Warrior Bugcrowd
- Intigriti Globally Top 1000
- Certified Blockchain Security Examiner
- Certified in Cyber Warfare and Terrorism
- Speaker & Writer

Red Teaming 101

- A red team in the military is a group that pretends to be an enemy and attempts to breach an organization's defenses, either physically or digitally. The red team then reports back on their findings so the organization can improve their defenses.

Attack is the secret of defence; defence is the planning of an attack

-The Art of War, Sun Tzu

RED TEAM

- The term "red team" comes from military exercises where the red team takes on the role of the enemy and the blue team defends their position. The same concept is used in cybersecurity, where the red team simulates cyber attacks to test an organization's digital defenses.
- Here we try to simulate attacks done by attackers like APT(Advanced Persistent Threat) ,Malicious hacker groups.To prevent and secure against actual attacks using TTP(Tactics, Techniques and Procedures).

Red Teaming Approach

We will follow the “Lockheed Martin cyber kill chain” Model

As it is most recognised and used model in industry.

Step 1: Recon

Step 2: Weaponization

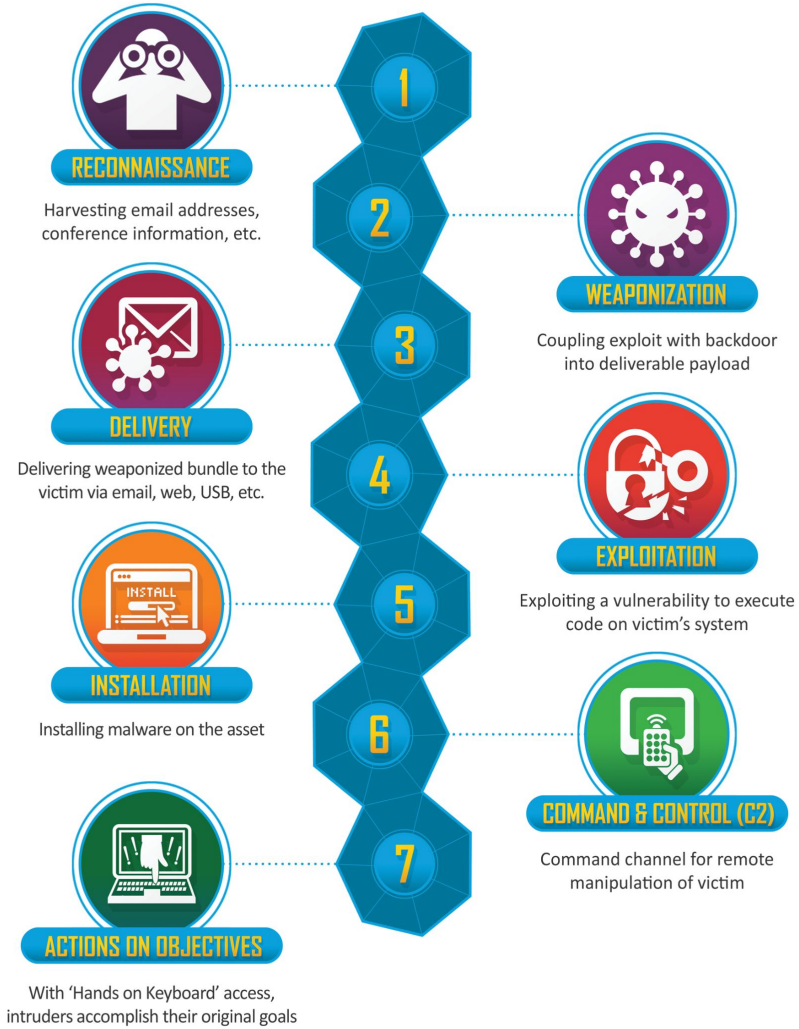
Step 3: Delivery

Step 4: Exploitation

Step 5: Installation

Step 6: Command and Control

Step 7: Actions on Objectives



Practical approach

Reconnaissance: Tools that gather information about the target environment, such as IP addresses, open ports, and network configurations.Also use OSINT to increase attack surface and hidden grounds

Exploitation: Tools that exploit vulnerabilities to gain unauthorized access to systems.Also use social engineering to exploit the organisation.

Privilege Escalation: Tools that elevate the attacker's permissions to gain higher-level access within the environment.

Lateral Movement: Tools that facilitate movement across the network, allowing the attacker to explore and compromise additional systems.

Exfiltration: Tools that enable the extraction of sensitive data from the target environment.

Post-Exploitation: Tools that maintain persistence, clean tracks, or further exploit compromised systems.

Tools

Reconnaissance: `Nmap`, `Masscan`, `Recon-ng`, `Amass`, `Sublist3r`

Exploitation: `Metasploit`, `Impacket`, `Responder`, `SQLmap`

Privilege Escalation: `WinPEAS`, `PowerUp`, `BloodHound`, `Kerbrute`

Lateral Movement: `PSExec`, `WMIC`, `Rubeus`, `CrackMapExec`

Persistence: `Empire`, `Cobalt Strike`, `Mimikatz`

Data Exfiltration: `DNSCat`, `Powershell Empire`, `HTTPS Tunnels`

AWS Red Teaming

1. **Reconnaissance:**
    - Enumerate AWS assets (EC2, S3, IAM, RDS).
    - Identify exposed services, misconfigurations, and leaked credentials.
    - Use OSINT tools like `CloudMapper` and `AWSRecon`.
2. **Initial Access:**
    - Exploit misconfigured IAM policies, S3 buckets, or leaked AWS keys.
    - Utilize SSRF or web application vulnerabilities to gain access.
    - Tools: `Pacu`, `nimbostratus`, `ScoutSuite`.
3. **Privilege Escalation:**
    - Exploit weak IAM roles, policies, or credentials.
    - Abuse IAM trust policies or escalate privileges via Lambda functions.
    - Tools: `AWSPX`, `WeirdAAL`.
4. **Lateral Movement:**
    - Pivot across AWS services (EC2 instances, RDS, Lambda).
    - Access and compromise additional AWS accounts using `AssumeRole`.
    - Tools: `Pacu`, `AWS CLI`.
5. **Persistence:**
    - Create backdoors (new IAM users, access keys, EC2 instances).
    - Use CloudFormation templates or Lambda functions for stealthy persistence.
    - Tools: `BackdoorFactory`, `AWS Shell`.
6. **Exfiltration and Cleanup:**
    - Exfiltrate sensitive data (e.g., S3 buckets, RDS snapshots).
    - Cover tracks by deleting CloudTrail logs and modifying AWS CloudWatch configurations.
    - Tools: `S3Copy`, `CloudGoat`.

EDR Bypass Techniques

1. **Living off the Land (LotL):**
   - Leverage built-in tools and legitimate binaries (LOLBAS) like `PowerShell`, `MSHTA`, `WMI`, and `CertUtil` to perform malicious activities.
   - Example: Using `PowerShell` scripts for fileless malware execution.
2. **Obfuscation:**
   - Obfuscate payloads or scripts to avoid signature-based detection.
   - Techniques: `Base64` encoding, string manipulation, and dynamic code execution.
   - Tools: `Invoke-Obfuscation`, `Invoke-DOSfuscation`.
3. **In-Memory Execution:**
   - Load and execute payloads directly in memory without touching disk, reducing the chances of being detected by EDR.
   - Techniques: `Reflective DLL Injection`, `Process Hollowing`, `Shellcode Injection`.
   - Tools: `Cobalt Strike`, `Donut`, `SharpSploit`.
4. **Process Injection:**
   - Inject malicious code into legitimate processes to mask the activity.
   - Techniques: `DLL Injection`, `APC (Asynchronous Procedure Call) Injection`, `Remote Thread Injection`.
   - Tools: `Mimikatz`, `Cobalt Strike`, `Metasploit`.
5. **Fileless Malware:**
   - Use techniques that don't rely on writing files to the disk, like `malicious macros` in documents or `script-based attacks`.
   - Example: Utilizing `HTA` (HTML Application) or `JavaScript` for initial payload delivery.
6. **EDR Hooking Evasion:**
   - Unhook or restore original system DLLs to remove EDR userland hooks that monitor API calls.
   - Tools: `GhostPack's Seatbelt`, `SysWhispers`, `Hollow's Trick`.
7. **Signed Binary Abuse (BYOI - Bring Your Own Interpreter):**
   - Abuse signed binaries to execute malicious code (e.g., `rundll32.exe`, `msiexec.exe`).
   - Example: Using `InstallUtil.exe` to run malicious scripts.
8. **Disabling EDR:**
   - Identify and exploit misconfigurations or vulnerabilities to disable or manipulate EDR services.
   - Techniques: `Service Stop/Deletion`, `Tampering with EDR Registry Entries`.

Automating Red Teaming

In the era of AI and ML automation is the important part we need to learn so here are some automation tools which can help in gathering attack surface and automating basic assessment.

Reconnaissance

Rengine

OSINT

SpiderFoot

Assessment

Caldera From Mitre

Atomic Red Team By **Red Canary**

RTA by Elastic/ Endgame Inc

Offensive Security

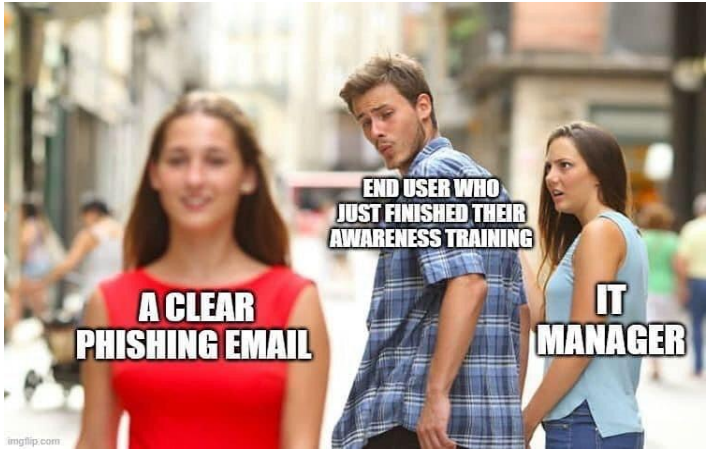
Vulnerability Assessment :- Scan the infrastructure/Network/Cloud with known vulnerabilities and CVEs with automated scanner like Nessus and Qualys etc.

Penetration Testing :- Validate the vulnerabilities found in VA and Manually try to penetrate the application on network using tools like burp suite and postman etc.

Cloud Security Testing :- Cloud Security testing involves cloud pentesting,Configuration review and DevSecOps.

Social Engineering:- Here Con Artists Will Engaged With client Employees and extract Information from them.use Spear -Phishing ,Pharming, Vishing ,Tail getting and others.

"**Wickets And Strongest Chain of Defence Is Humans Mind** "



That’s All for Now

Thank You All