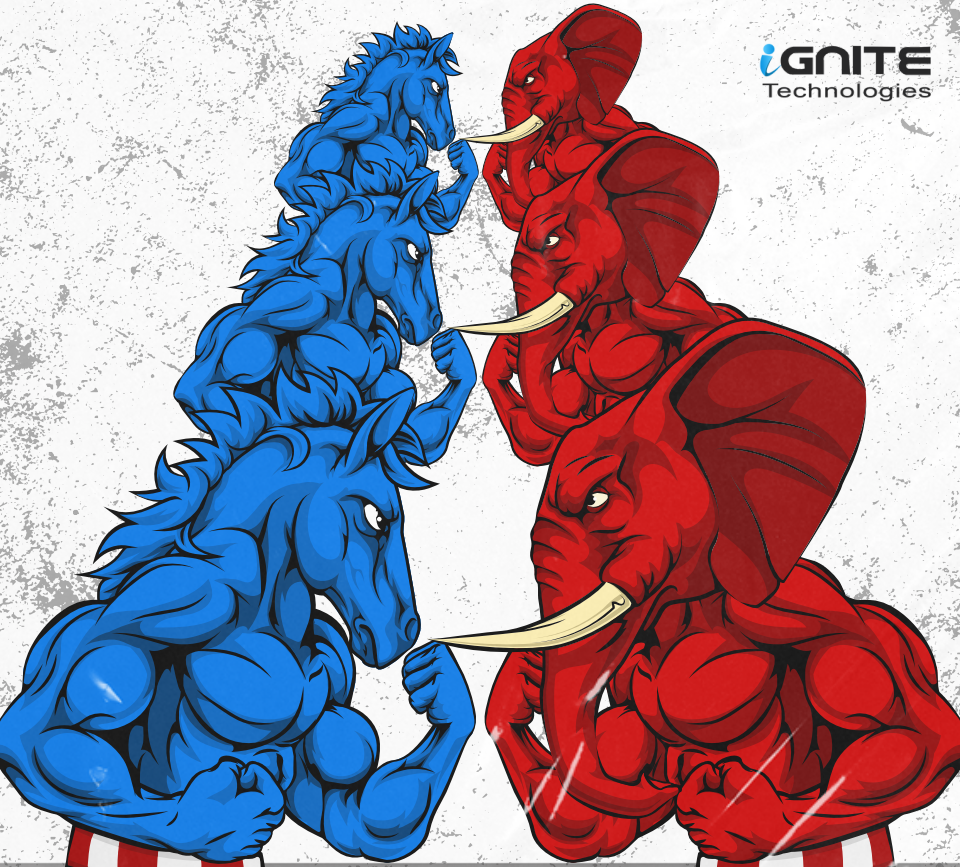
iGNITE Technologies



RED TEAM

OPERATIONS - MITRE ATTACK

INTRO

RED TEAM OPERATION- MITRE APT'S ATTACK

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

The course structure comprises various attacker simulators and industry attack frameworks such as Cyber Kill Chain, Attack Tree and MITRE ATT&CK Framework. Candidates get the opportunity to behave like an adversary and creatively use local, built-in tools to reach business goals while preventing detection.

Furthermore, the course focuses on making use of open-source resources such as tools and scripts and then tweaking them to complement an organization's specific needs. By performing nefarious cyber-attack exercises that simulate real-world threat vectors, trainees will gain hands-on experience.

BENEFITS

- Gain Exposure to Real-Time Pentesting & Red Team
- This course meets the requirements of NIST, MITRE ATTACK, Cyber kill chain and Attack Tree.
- Building in-house lab for threat modelling and Hunting
- Gain in-depth knowledge of APTs attacks such as APT41, and APT28.
- Hands-on exposure to AD tools such as Rubeus and Mimikatz.
- Unique tools and techniques for exploiting AD
- Latest attack such as zero day exploit.

WHO SHOULD JOIN ?

- If you are an ethical hacker with Basic knowledge
- If you are a Network Security Engineer
- If you managed NOC and SOC
- If you are an Information Security Analyst
- If you are a Team leader of the Cyber Security Department
- If you handle the pre-sell department for VAPT services
- If you are a backend developer
- If you are a system administrator

PREREQUISITES

The candidate should have a basic understanding of web and Networking and also know the fundamental approach of system hacking.

COURSE DURATION: 50 HOURS

OBJECTIVE

OBJECTIVE OF RED TEAM EXERCISE

Calculate Risk Factors

Identify the weaknesses and evaluate between high-risk and low-risk variables that can undermine the integrity, then remediate them based on priority.

Improve Security Orientation

Assess the threats in your organization and update your security measures as needed.

Prepare yourself

You will have the tools you need to identify a genuine threat and the knowledge you need to make smart decisions.

Recognize the gaps

Understand the vulnerabilities that can be exploited to expose your data to possible threats. Discover how hackers combine both high- and low-level flaws to carry out prospective attacks.

An Efficiency Test

evaluating the security's efficiency in relation to people and processes

INDEX

Initial Access

(MITRE: TA0001)

Initial access is a tactic used to establish a foothold in a network. This module's objective is to propose the various initial access types described by MITRE while simulating certain real-world attacks.

During Live sessions candidates will get hands-on most famous attack types:

- **Drive-by Compromise/Download:** Used by APTs19, and APT 38 to conduct watering hole attacks to gain access to a system through a user visiting a website over the normal course of browsing.
- **Phishing:** Adversary target outlook application for spear-phishing by enabling macros-based word document, excel sheet and presentation slides.
- **Forced Valid Account:** An adversary may poison a network by running spoof services to obtain user credentials for remote login.
- **Hardware Addition:** Adversaries may introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. The candidate will gain experience in Wi-Fi hacking during Hardware Addition Tactics.

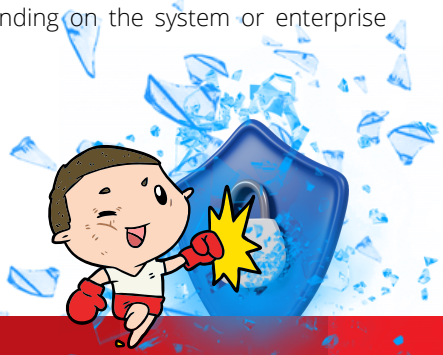
Execution

(MITRE: TA0002)

Execution entails methods that cause adversary-controlled code to run on a local or remote system. In order to accomplish more general objectives, such as network exploration or data theft, techniques that run harmful code are frequently combined with techniques from all other approaches.

The major objective of execution is to create a payload that can be easily executed in a restricted environment in a manner so that an adversary can evade the firewall and AV.

- **Payload obfuscation:** Payloads may be compressed, archived or encrypted in order to avoid detection and bypass antivirus or windows defender.
- **Alternate data streams:** These generally deal with maintaining the confidentiality of the file that is being sent or is at rest on the system.
- **Application Shimming:** It is a technique y to run software on the Windows OS that was not developed on that particular OS.
- **AMSI Bypass:** Antimalware Scan Interface (AMSI) standard that allows a developer to integrate malware defence in his application.
- **Process Doppelganging:** Using process doppelganging, adversaries can implant malicious code into processes to avoid process-based defences and possibly elevate privileges. Process doppelganging is a technique for executing arbitrary code within the address space of a distinct live process.
- **Inter-Process Communication:** An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.



Persistence

(MITRE: TA0003)

Persistence relates to how adversaries sustain access to systems through restarts, credential changes, and other interruptions. Persistence techniques include any access, activity, or configuration changes that allow malware to persist. Changing or hijacking lawful code and adding startup code are examples.

- **Windows Accessibility Features:** These are tools on the logon screen (like Sticky Keys). These are activated by pre-configured keys to help users. APT used these Windows features to backdoor victim systems.
- **Application shimming:** Using application shims, attackers can create persistence and elevate access. Microsoft's Windows Application Compatibility Infrastructure/Framework (Application Shim) allows software backward compatibility as the OS core changes.
- **RID Hijacking:** It is a technique for an adversary to persist inside the victim's system by hijacking the RID Administrator account for the Guest account or another local account.
- **Shortcut modification:** It is a technique in which an attacker can replace the absolute path of an executable bound to be run by a shortcut and masquerade it as a legitimate-looking icon which can be run on startup thus achieving persistence.
- **WinLogon Registry Attack:** each Windows user account is dependent on WinLogon to use the keys under HKEY_CURRENT_USER which is unique for each user account. An attacker may hook a malicious script by modifying registry key to achieving persistence.

Privilege Escalation
(MITRE: TA0004)

Privilege Escalation involves gaining higher-level permissions on a system or network. Adversaries can explore a network with unprivileged access but need elevated permissions to complete their goals. System flaws, misconfigurations, and vulnerabilities are often exploited.

- **Windows kernel:** A privilege escalation vulnerability exists in the os kernel on the remote host. If exploited successfully, a locally authorized attacker might execute a specially built kernel-mode program and take control of the machine.
- **Registry Run Keys:** If an attacker finds a service that has all permission and its bind with the Registry run key then he can perform privilege escalation or persistence attacks. When a legitimate user signs in, the service link with the registry will be executed automatically.
- **SeBackupPrivilege:** This specific privilege escalation is based on the act of assigning a user SeBackupPrivilege. It was designed for allowing users to create backup copies of the system.
- **Print Spooler:** The vulnerability allows an unprivileged user to create arbitrary and writeable directories by configuring the SpoolDirectory attribute on a printer. Since an unprivileged user is allowed to add remote printers, an attacker can create a remote printer and grant EVERYONE the right to manage this printer.

Defense Evasion
(MITRE: TA0005)

When an adversary attempts to infiltrate your system, they employ several methods of defence evasion to remain undetected. Defence evasion techniques include removing/disabling security software and encrypting/obfuscating data and scripts. In order to conceal and disguise their infection, adversaries make advantage of and misuse trusted processes.

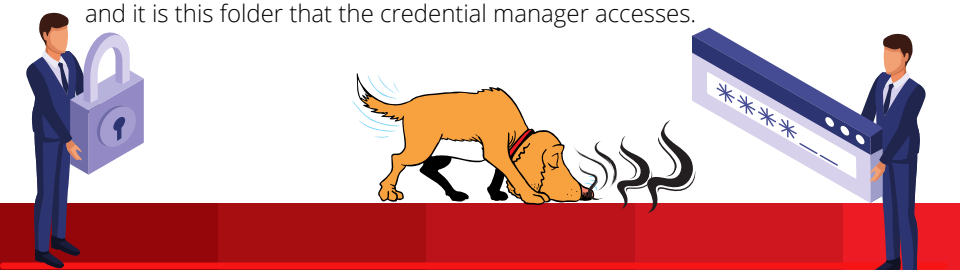
- **Hid Artifacts:** Operating systems have a function to hide these artefacts to avoid interrupting user work environments and to prevent users from modifying system files or features. By masking these artefacts, however, an attacker is able to elude detection and thereby carry out his malicious intentions.
- I**ndirect Command Execution:** It is a defence evasion tactic commonly utilised by Red Teams in which an adversary attempts to circumvent specific protection filters that may prevent certain types of scripts/executables from running. Various Windows utilities can be used to run commands without having to invoke cmd. For example, if a firewall prevents DLL execution, it can be circumvented using the procdump approach.
- **Parent PID Spoofing:** It counters that detection. PPID method tries to trick an AV/EDR solution into thinking that a legit process like lsass.exe has spawned that activity. It does that by spoofing the PID of the process to match that of its parent.
- **Process Hollowing:** It's a code injection technique, an attacker creates a new process in a suspended state, its image is then unmapped (hollowed) from the memory, a malicious binary gets written instead and finally, the program state is resumed which executes the injected code.
- **Windows Event Logging:** To restrict the amount of data that can be used for detection and audits, an attacker can disable Windows event logging. Login attempts, process development, and other user and device behaviour are all recorded in Windows event logs.

Credential Access

(MITRE: TA0006)

Credential Access is a collection of strategies for obtaining credentials, such as account names and passwords, hashes, and Kerberos tickets. Among the methods used to obtain credentials is keylogging and credential dumping. Using authentic credentials can grant adversaries access to systems, make them more difficult to detect, and allow them to create additional accounts to achieve their objectives.

- Golden Tickets are forged Ticket-Granting Tickets (TGTs), also called authentication tickets. Since a Golden Ticket is a forged TGT, it is sent to the Domain Controller as part of the TGS-REQ to get a service ticket.
- Local Security Authority (LSA): It is a protected system process that authenticates and logs users onto the local computer. Domain credentials are used by the operating system and authenticated by the Local Security Authority (LSA). Red Teamer tries to abuse LSA for dumping stored password hashes.
- Phishing Windows Credential: For security purposes, Windows makes it essential to validate user credentials for various authentications, such as Outlook, User Account Control, or to sign in to Windows from the lock screen. An attacker may use a file-less payload to dump the credentials after establishing a foothold on the target system.
- Abusing SAM Password: SAM is short for Security Account Manager, which manages all the user accounts and their passwords. It acts as a database. All the passwords are hashed and then stored in SAM.
- Credential Manager: It is like a digital vault to keep all of your credentials safe. All of the credentials are stored in a credentials folder which you will find at this location: %Systemdrive%\Users\\AppData\Local\Microsoft\Credentials and it is this folder that the credential manager accesses.



Lateral Movement

(MITRE: TA0008)

Lateral Movement is a set of attacks used to access and control remote network systems. Exploring the network to find their target and obtaining access to it is usually required to achieve their main aim. To accomplish their goals, individuals must often use many systems and accounts. Adversaries can install their own remote access tools or use the natural network and operating system technologies to accomplish Lateral Movement.

- **Crackmapexec:** Also known as CME, is a post-exploitation tool. The developer of the tool describes it as a Swiss army knife for pen-testing networks. It also offers us numerous modules such as mimikatz, web delivery, wdigest, etc. to make dumping of credentials and getting a session easy.
- **RDP Hijacking:** Adversaries may use RDP session hijacking to take a valid user's remote session. When someone tries to steal a user's session, the user is usually warned. An attacker with System permissions and Terminal Services Console can hijack a session without requiring credentials or prompting the user.
- **Remote Services:** Lateral Movement using Remote Services, i.e., services that can help in code/command execution on remote systems by taking a valid set of credentials.
- **Workstation Hijacking:** PetitPotam can be used in conjunction with NTLM Relay+WebDAV abuse to cause lateral movement by creating machine accounts first, and then using Resource-Based Constrained Delegation to generate tickets for any user. Using PetitPotam or PrinterBug, an HTTP authentication can be coerced and relayed to LDAP(S) on domain controllers.
- **SSH Tunnelling:** Tunneling permits secret data sharing between two networks. An attacker can tunnel or pivot into an unreachable network (centre point). It's an assault that exploits a different network's system.

Command & Control

(MITRE: TA0009)

Command and Control is how adversaries communicate with systems in a victim network. To avoid detection, attackers often imitate normal communications. Depending on the victim's network structure and defences, an adversary can establish command and control in stealthy methods.

- **Application Layer Protocol:** Adversaries may communicate using the Domain Name System (DNS) application layer protocol to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
- **Encrypted C&C:** Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.
- **Non-Application Layer Protocol:** Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. Specific examples include the use of network-layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), and session layer protocols, such as Socket Secure (SOCKS).
- **C&C Framework:** Metasploit, PowerShell Empire and Covenant

Exfiltration

(MITRE: TA0009)

Exfiltration refers to procedures used by adversaries to steal data from your network. When attackers collect data, they frequently bundle it to evade discovery while discarding it. Compression and encryption are two examples. Transferring data out of a target network often entails transferring it across their command-and-control channel or an alternate channel, as well as imposing size constraints on the transmission.

- Data Transfer Size Limits: An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.
- Exfiltration Over Unencrypted Non-C2 Protocol: Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.
- Data Exfiltration with Steganography: Cloakify Factory transforms any filetype (e.g .zip, .exe, .xls,etc.) into a list of harmless-looking string. This hides the file in plain sight and transfer it without triggering alerts. It even defeats signature-based malware detection tools.
- Exfiltration Over Alternative Protocol: Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Contact us

PHONE

+91-9599387841 | +91 11 4510 3130

WHATSAPP

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/Ignitetechnologies