

## Part 1.

### a. Exploitation for Privilege Escalation

Technique ID: T1068

Tactic: privilege escalations

The screenshot shows the MITRE ATT&CK matrix interface. The central column is labeled "Techniques" and contains a list of techniques under the heading "Exploitation for Privilege Escalation". This list includes "Hijack Execution Flow", "Process Injection", "Scheduled Task/Job", "Valid Accounts", "Defense Evasion", "Credential Access", "Discovery", "Lateral Movement", "Collection", and "Command and Control". To the left of the matrix is a sidebar with various search filters and categories. To the right is a large list of defensive measures and other techniques, many of which are also circled in red. The top navigation bar includes links for "Matrices", "Tactics", "Techniques", "Defenses", "CTI", "Resources", "Benefactors", "Blog", and "Search".

**Techniques**

- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control

**Techniques (Continued)**

- Exploit for Privilege Escalation
- Impair Defense
- Impersonation
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web

**Defenses**

- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Permissions Modification
- File and Directory Request Generation
- Group Policy Discovery
- Log Enumeration
- Network Sniffing
- OS Credential Dumping
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery

**Benefactors**

- Services
- Clipboard Data
- Data from Cloud Storage
- Data from Removable Media
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

The screenshot shows the detailed view for Technique T1068: Exploitation for Privilege Escalation. The page header includes the MITRE ATT&CK logo and a search bar. Below the header, a message says "ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Register for in-person participation here. Stay tuned for virtual registration!"

**Home > Techniques > Enterprise > Exploitation for Privilege Escalation**

## Exploitation for Privilege Escalation

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.

When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This

**ID:** T1068  
**Sub-techniques:** No sub-techniques  
**Tactic:** Privilege Escalation  
**Platforms:** Containers, Linux, Windows, macOS  
**Permissions Required:** User  
**Effective Permissions:** User  
**Contributors:** David Tayouri; Idan Revivo, @idanr86, Team Nautilus Aqua Security, Joas Antonio dos Santos, @C0d3Cr4zy, Inmetriics; Yaniv Agman, @AgmanYaniv, Team Nautilus Aqua Security

## Mitigation Strategies

1. Patching: To keep the system up to date and its software with latest new patches to fix known vulnerabilities that attacker can exploit.
2. User Account Control: Make efforts to restrict and control excessive privileges on assigned accounts to avert any likely sequences of elevation.

## Detection Strategies

1. Analyze log Files: Examine and dissect some certain types of the logs of the system in search of some failed events regarding elevation of privileges. Like we mostly snort , Splunk tools for this. Or review the system logs to detect failed attempts at privilege escalations.
2. Monitor privilege changes: Safeguard oversight and management of any security monitoring processes and any ‘anomalies’ regarding singular or mass privilege elevation.

## b. Credential Dumping

Technique ID: T1003

Tactic: Credential Access

The screenshot shows the MITRE ATT&CK website. The left sidebar has a tree view under 'TECHNIQUES' with 'OS Credential Dumping' selected. The main content area is titled 'OS Credential Dumping' and shows 'Sub-techniques (8)'. A red oval highlights the right-hand sidebar information, which includes:

- ID: T1003
- Sub-techniques: T1003.001, T1003.002, T1003.003, T1003.004, T1003.005, T1003.006, T1003.007, T1003.008
- Tactic: Credential Access
- Platforms: Linux, Windows, macOS
- Contributors: Ed Williams, Trustwave, SpiderLabs; Tim (Wadhwa) Brown; Vincent Le Toux; Yves Yonan
- Version: 2.2
- Created: 31 May 2017
- Last Modified: 18 April 2024

At the bottom right of the sidebar, there is a link 'Version Permalink'.

### Mitigation strategies:

1. Use Least Privilege Role: Least Privilege Principle (User account should have only the access that they need to perform their specific role, minimizing chance of credential exposure)
2. Use credential Guard: Turn on the Windows Credential Guard to stop credential from being stored in-memory.

### Detection strategies:

1. Regularly Audit access to the processes of LSASS: Examine the LSASS Process Access , Used frequently for credential dumping, look out for processes accessing the LSASS process without permission.
2. Monitoring Memory Access: Detecting processes reading memory from where you store your credentials using tools such as Sysmon.

## c. Scheduled Task/Job

Technique ID: T1053

Tactic ID: Execution , Persistence , privilege Escalations

**Scheduled Task/Job**

**Sub-techniques (5)**

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.<sup>[1]</sup>

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to System Binary Proxy Execution, adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.<sup>[2]</sup>

**ID: T1053**  
**Sub-techniques:** T1053.002, T1053.003, T1053.005, T1053.006, T1053.007  
**Tactics:** Execution, Persistence, Privilege Escalation  
**Platforms:** Containers, Linux, Windows, macOS  
**Permissions Required:** Administrator, SYSTEM, User  
**Effective Permissions:** Administrator, SYSTEM, User  
**Supports Remote:** Yes  
 Contributors: Alain Homewood, Insomnia Security; Andrew Northern, @ex\_raritas; Bryan Campbell, @bry\_campbell; Leo Loobek,

## Mitigation Strategies:

1. Make clean, Audit scheduled tasks: Allows admins to review their scheduled tasks for unexpected changes or malicious additions.
2. Restrict task scheduler usage: Allow only system administrators to create or change scheduled tasks.

## Detections Strategies:

1. Analyze Logs and its Modifications: Pay attention to any changes in the scheduled tasks that may indicate a bad activity.
2. Monitoring task Creations: use the windows event logs for generating new scheduled tasks (Event ID 4698)

## d. Remote Services ( RDP, SSH,etc)

Technique ID: T1021

Tactic: Lateral Movement

The screenshot displays two pages from the MITRE ATT&CK website, both titled "Remote Services".

**Top Page (Remote Services: SSH):**

- Techniques Sidebar:** SSH is selected.
- Content Area:** Sub-techniques include Other sub-techniques of Remote Services (8), Valid Accounts, SSH, and Remote Desktop Protocol.
- Right Panel:** Details for T1021.004:
  - ID: T1021.004
  - Sub-technique of: T1021
  - Tactic: Lateral Movement
  - Platforms: Linux, macOS
  - System Requirements: An SSH server is configured and running.
  - Version: 1.2
  - Created: 11 February 2020
  - Last Modified: 11 August 2023

**Bottom Page (Remote Services: Remote Desktop Protocol):**

- Techniques Sidebar:** Remote Desktop Protocol is selected.
- Content Area:** Sub-techniques include Other sub-techniques of Remote Services (8), Valid Accounts, and Remote Desktop Protocol.
- Right Panel:** Details for T1021.001:
  - ID: T1021.001
  - Sub-technique of: T1021
  - Tactic: Lateral Movement
  - Platforms: Windows
  - System Requirements: RDP service enabled, account in the Remote Desktop Users group
  - Contributors: Matthew Demaske, Adaptforward
  - Version: 1.2
  - Created: 11 February 2020
  - Last Modified: 07 August 2023

## Mitigation Strategies:

1. Disable unused remote services: Disable unnecessary services like RDP or SSH as it reduces potential attack surfaces.
2. Enable MFA: Add a second layer of security to your remote services; single sign on + another factor is less guessable than just the password.

## Detection Strategies:

1. Log your remote login attempts: Monitor unsuccessful and out-of-the-norm successful remote logins from unusual IPs.
2. Monitor network traffic: Network monitoring tools are used to discover rogue remote service connections.

## E. Process Injections:

Technique ID: T1055

Tactic: Defense Evasion, Privilege Escalations

The screenshot shows the MITRE ATT&CK website. The left sidebar has a 'TECHNIQUES' section with 'Process Injection' selected, showing various sub-techniques like Dynamic-link Library Injection, Portable Executable Injection, Thread Execution Hijacking, etc. The main content area is titled 'Process Injection' and describes the technique. It includes sections for 'Sub-techniques (12)', 'Adversaries may inject code into processes...', 'There are many different ways to inject code...', and 'More sophisticated samples...'. On the right, there's a detailed view of the technique with fields for 'ID: T1055', 'Sub-techniques: T1055.001, T1055.002, T1055.003, T1055.004, T1055.005, T1055.008, T1055.009, T1055.011, T1055.012, T1055.013, T1055.014, T1055.015', 'Tactics: Defense Evasion, Privilege Escalation', 'Platforms: Linux, Windows, macOS', 'Defense Bypassed: Anti-virus, Application control', and 'Contributors: Anastasios Pingios, Christian Beek, @ChristiaanBeek; Ryan Beecwar'. Two red boxes highlight the 'Sub-techniques' section and the 'Tactics' and 'Platforms' sections.

## Mitigation Strategies

1. Use Data Execution Prevention (DEP): DEP is a security feature that prevents the execution of code from system memory locations.
2. Enforce code signing: Make sure only signed code is allowed to run in the memory, this way you lessen the threat of process injection.

## Detection Strategies

1. Monitor api calls : Look for suspicious API called such as Write Process Memory, Create Remote Thread that are used in process injection.
2. Tracking memory access patterns: to identify abnormal read/write operations on the processes that could have been related with process injection techniques.

## Part 2:

Navigator to <https://mitre-attack.github.io/attack-navigator/v2/enterprise/>

Layer											selection controls			layer controls			technique controls				
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement		Collection	Command And Control	Exfiltration	Impact									
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items										
Drive-by Compromise	AppleScript	.bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal										
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction										
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITs Jobs	Brute Force	Browser Bookmark Discovery	Clipboard Data	Component Object Model and Distributed COM	Data from Local System	Connection Proxy	Data Encrypted	Data Encrypted for Impact									
Hardware Additions	Compiled HTML File	Component Object Model and Distributed COM	AppCert DLLs	Appinit DLLs	Clear Command History	Component Object Model and Distributed COM	Custom Command and Control Protocol	Custom Command and Control Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Defacement									
Replication Through Removable Media	Control Panel Items	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Data from Network Shared Drive	Data from Network Shared Drive	Data from Network Shared Drive	Data Obfuscation	Data Transfer Size Limits	Disk Content Wipe									
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in File	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	Disk Structure Wipe									
Spearphishing Link	Execution through API	BITS Jobs	Dylib Hijacking	Compiled HTML File	Compile After Delivery	Credentials in Registry	Internal Spearphishing	Internal Spearphishing	Internal Spearphishing	Internal Spearphishing	Internal Spearphishing	Endpoint Denial of Service									
Spearphishing via Service	Execution through Module Load	Bootkit	Component Firmware	Component Object Model and Distributed COM	Component Object Model and Distributed COM	Compromised Credentials	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Logon Scripts	Firmware Corruption									
Supply Chain Compromise	Exploitation for Client Execution	Change Default File Association	Elevated Execution with Prompt	Forced Authentication	Forced Authentication	Forced Authentication	Pass the Hash	Pass the Hash	Pass the Hash	Pass the Hash	Pass the Hash	Inhibit System Recovery									
Trusted Relationship	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Hooking	Hooking	Hooking	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Peripheral Device Discovery	Network Denial of Service									
Valid Accounts	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Emond	Emond	Emond	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	Resource Hijacking									
	Launchctl	Create Account	Deobfuscate/Decode Files or Information	DCShadow	Input Capture	Input Capture	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	Runtime Data Manipulation									
	Local Job Scheduling	DLL Search Order Hijacking	File System Permissions Weakness	DKRoberoasting	Query Registry	Query Registry	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	Service Stop									
	LSASS Driver	DLL Side-Loading	DLL Side-Loading	Keychain	Remote System Discovery	Remote System Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	File and Directory Discovery	Stored Data Manipulation									
	Mshta	Dylib Hijacking	Hooking	Man in the Browser	Man in the Browser	Man in the Browser	Multi-Stage Channels	Multi-Stage Channels	Multi-Stage Channels	Multi-Stage Channels	Multi-Stage Channels	System Shutdown/Reboot									
	PowerShell	Emond	Image File	Network Sniffing	Network Sniffing	Network Sniffing	Network Sniffing	Network Sniffing	Network Sniffing	Network Sniffing	Network Sniffing	Transmitted Data									
				>Password Filter DLL	Third-party	Third-party	Port Knocking	Port Knocking	Port Knocking	Port Knocking	Port Knocking	legend									

a) Create an APT17 layer

APT17							MITRE ATT&CK® Navigator								
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	selection controls			layer controls			technique controls		
							Threat Groups			Exfiltration			Impact		
11 items	34 items	62 items	32 items	69 items	21 items	23 items	admin@338	view	select	deselect	APT1	view	select	deselect	
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	APT12	view	select	deselect	APT16	view	select	deselect	
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Application Window Discovery	Brute Force	APT17	view	select	deselect	APT18	view	select	deselect	
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Bypass User Account Control	Browser Bookmark Discovery	APT19	view	select	deselect	Domain Trust Discovery	view	select	deselect	
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Clear Command History	Credential Dumping	File and Directory Discovery	File Network Service Scan	SPARA RAT	view	select	deselect	File Network Share Discovery	view	select	deselect
Replication Through Removable Media	Component Object Model and Distributed COM	Application Shimming	CMSTP	Credentials from Web Browsers	Network Service Scan	Network Share Discovery	4H RAT	view	select	deselect	Network Sniffing	view	select	deselect	
Spearphishing Attachment	Control Panel Items	Bypass User Account Control	Code Signing	Credentials in Files	Network Sniffing	>Password Policy Disclosure	abudup	ADVSTORESHELL	view	select	deselect	Exploitation for Credential Access	view	select	deselect
Spearphishing Link API	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compiled HTML File	Peripherals Device Discovery	Peripheral Device Discovery	Agent Tesla	Agent.btz	view	select	deselect	Endpoint Denial of Service	view	select	deselect
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Component Firmware	Forced Authentication	Permission Groups Discovery	Arg	Arg	view	select	deselect	Firmware Corruption	view	select	deselect
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Object Model Hijacking	Forced Authentication	Process Discovery	Agent.btz	Browser	view	select	deselect	Inhibit System Recovery	view	select	deselect
Trusted Relationship	Graphical User Interface	Browser Extensions	Emond	Connection Proxy	Hooking	Query Registry	Replication Through Removable Media	Browser	view	select	deselect	Network Denial of Service	view	select	deselect
Valid Accounts	Exploitation for Client Execution	Change Default File Association	EDmond	Control Panel Items	Input Capture	Remote System Discovery	Multi-Stage Channels	Browser	view	select	deselect	Resource Hijacking	view	select	deselect
Local Job Scheduling	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Input Prompt	Security Software Discovery	Shared Webroot	Browser	view	select	deselect	Runtime Data Manipulation	view	select	deselect
	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Kerberoasting	Software Discovery	Video Capture	Browser	view	select	deselect	Service Stop	view	select	deselect
	Launchcht!	Create Account	File System Permissions Weakness	Disabling Security Tools	Keychain	System Information Discovery	Multi-band Communication	Browser	view	select	deselect	Stored Data Manipulation	view	select	deselect
LSASS Driver	DLL Search Order Hijacking	DLL Side-Loading	DLL Search Order Hijacking	LMMNR/NBT-NS Poisoning and Relay	SSH Hijacking	Taint Shared Content	Multilayer Encryption	Browser	view	select	deselect	System Shutdown/Reboot	view	select	deselect
Mshta	Dylib Hijacking	Hooking	Execution Guardrails	Network Sniffing	System Network Configuration Discovery	Transmitted Data	Port Knocking	Browser	view	select	deselect	Transmitter	view	select	deselect

and assign the first two numbers of our student ID which is 10 as a score.

MITRE ATT&CK® Navigator

AP17

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Bypass User Account Control	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	Appinit DLLs	Clear Command History	Credential Dumping	Domain Trust Discovery	Data from Information Repositories	Data from Local System	Custom Command and Control Protocol
Replication Through Removable Media	Component Object Model and Distributed COM	Appinit DLLs	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Exploitation of Remote Services	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Code Signing	Credentials in Files	Network Service Scanning	Internal Spearphishing	Data from Network Shared Drive	Custom Command and Control Channel
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Network Share Discovery	Logon Scripts	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	BITS Jobs	Dylib Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Sniffing	Pass the Hash	Data from Removable Media	Firmware Corruption
Spearphishing via Service	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Firmware	Forced Authentication	Peripheral Device Discovery	Pass the Ticket	Domain Fronting	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Component Object Model Hijacking	Control Panel Items	Connection Proxy	Process Discovery	Remote Desktop Protocol	Data Staged	Network Denial of Service
Trusted Relationship	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Hooking	Remote File Copy	Remote File Copy	Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Forced Authentication	Query Registry	Remote Services	Multi-hop Proxy	Runtime Data Manipulation
	Launchctl	Create Account	Kerberoasting	Keychain	File System Permissions	Remote System Discovery	Replication Through Removable Media	Multi-Stage Channels	Service Stop
	Local Job Scheduling	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	System Information	Screen Capture	Screen Capture	Multiband Communication	Stored Data Manipulation
	LSASS Driver	Dylib Hijacking	DLL Side-Loading	SSH Hijacking	Taint Shared Content	Video Capture	Video Capture	Multilayer Encryption	System Shutdown/Reboot
	Mshta	Hooking	Execution Guardrails						

b. Create a second layer of APT18

MITRE ATT&CK® Navigator

AP17 AP18

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Threat Groups	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	admin@338	9 items	16 items
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	APT1	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	APT12	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Bypass User Account Control	Brute Force	Browser Bookmark Discovery	APT16	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Appinit DLLs	Clear Command History	Credential Dumping	Domain Trust Discovery	APT17	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Appinit DLLs	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	APT18	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Code Signing	Credentials in Files	Network Service Scanning	File and Directory Discovery	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Credentials in Registry	Network Share Discovery	SPARA RAT	Endpoint Denial of Service	Endpoint Denial of Service
Spearphishing Link	Execution through API	BITS Jobs	Dylib Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Sniffing	4H RAT	Firmware Corruption	Firmware Corruption
Spearphishing via Service	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Component Firmware	Forced Authentication	Peripheral Device Discovery	adbupd	Inhibit System Recovery	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Component Object Model Hijacking	Control Panel Items	Connection Proxy	Process Discovery	ADVSTORESHELL	Network Denial of Service	Network Denial of Service
Trusted Relationship	Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	DCShadow	Hooking	Remote System Discovery	Agent Tesla	Scheduled Transfer	Resource Hijacking
Valid Accounts	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Input Capture	Query Registry	Replication Through Removable Media	agent.btz	Runtime Data Manipulation	Runtime Data Manipulation
	Launchctl	Create Account	Kerberoasting	Deobfuscate/Decode Files or Information	Input Prompt	Security Software Discovery	arp	Service Stop	Service Stop
	Local Job Scheduling	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Disabling Security Tools	File System Permissions Weakness	Shared Webroot	ADVSTORESHELL	Stored Data Manipulation	Stored Data Manipulation
	LSASS Driver	Dylib Hijacking	DLL Side-Loading	Network Sniffing	System Information Discovery	System Network Configuration Discovery	Agent Tesla	System Shutdown/Reboot	System Shutdown/Reboot
	Mshta	Hooking	Execution Guardrails			Taint Shared Content	agent.btz		

and assign the last two numbers of our student ID as a score which is 34.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Technique Details
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items
Drive-by Compromise	AppleScript	.bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Extraction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Account Access Removal
External Remote Services	Command-Line Interface	Account Manipulation	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Data from Information Repositories	Connection Proxy	Data Compressed
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	Credential Dumping	Domain Trust Discovery	Data from Local System	Custom Command and Control Protocol	Custom Cryptographic Protocol	Custom Command and Control Protocol	Data Destruction
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	File and Directory Discovery	Exploitation of Remote Services	Custom Command and Control Protocol	Custom Cryptographic Protocol	Custom Command and Control Protocol	Data Encrypted
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Code Signing	Filesystem Discovery	Data from Network Shared Drive	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Data Encrypted for Impact
Spearphishing Link API	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Filesystem Discovery	Data Encoding	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Defacement
Spearphishing Link API	Execution through API	BITS Jobs	Dylib Hijacking	Component Firmware	Filesystem Discovery	Data Obfuscation	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Disk Content Wipe
Spearphishing via Service	Execution through Module Load	Bootkit	Elevated Execution with Hijacking	Component Object Model Hijacking	Filesystem Discovery	Data from Removable Media	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Elevated Execution with Prompt	Forced Authentication	Filesystem Discovery	Data Staged	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Endpoint Denial of Service
Trusted Relationship	Change Default File Association	Emond	Control Panel Items	Hooking	Filesystem Discovery	Domain Generation Algorithms	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Firmware Corruption
Valid Accounts	Component Object Model Hijacking	Extra Window Memory Injection	DCShadow	Input Capture	Filesystem Discovery	Fallback Channels	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Inhibit System Recovery
	InstallUtil	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Input Prompt	Filesystem Discovery	Multi-hop Proxy	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Network Denial of Service
	Launchctl	Kerberosting	Disabling Security Tools	Input Registry	Filesystem Discovery	Multi-stage Channels	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Resource Hijacking
	Create Account	Keychain	LLMNR/NBT-NS Poisoning and Relay	Input Services	Filesystem Discovery	Multi-band Communication	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Runtime Data Manipulation
	DLL Search Order Hijacking	Software Discovery	System Information Discovery	Man in the Browser	Filesystem Discovery	Multilayer Encryption	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Service Stop
	LSASS Driver	Shared Webroot	SSH Hijacking	Screen Capture	System Network Configuration Discovery	Port Knocking	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Custom Cryptographic Protocol	Stored Data Manipulation
	DLL Side-Loading	Taint Shared Content	Video Capture							System Shutdown/Reboot
	Mshta	Network Sniffing								Transmitted Data

c. Combine the two using “Create Layer from other layers” using the expression “ $a + b$ ”

**Create New Layer** Create a new empty layer

**Open Existing Layer** Load a layer from your computer or a URL

**Create Layer from other layers** Choose layers to inherit properties from

score expression  
a + b

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found [here](#). Leave blank to initialize scores to 0.

coloring

Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.

comments

Choose which layer to import comments from. Leave blank to initialize with no comments.

states

Choose which layer to import enabled/disabled states from. Leave blank to initialize all to enabled.

filters

Choose which layer to import filters - stages and platforms - from. Leave blank to initialize with no filters.

APT17 x APT18 x APT17 + APT18 x +

selection controls layer controls technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	platforms	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	Windows	9 items	16 items
Drive-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture		Linux	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Applications	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Application Window Discovery	Application Deployment Software	Automated Collection		macOS	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Bash History	Browser Bookmark Discovery	Clipboard Data		AWS	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	Component Object Model and Distributed COM	Data from Information Repositories		Azure	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credential Dumping	Domain Trust Discovery	Data from Local System		Azure AD	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange Package	Authentication Package	DLL Search Order Hijacking	Compiled HTML File	Clear Command History	Credentials in Files	Data from Network Share		Office 365	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	Elevated Execution with Prompt	Code Signing	Credentials in Registry	File and Directory Discovery	Data from Network Share		SaaS	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through Module Load	Bootkit	Component Object Model Hijacking	Compiled HTML File	Compiled After Delivery	File and Directory Discovery	Logon Scripts		Cloud	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Change Default File Association	Component Object Model Hijacking	Component Firmware	Exploitation for Credential Access	Pass the Hash		Cloud	Inhibit System Recovery	Network Denial of Service
Trusted Relationship	Graphic User Interface	Component Firmware	Component Object Model Hijacking	Connection Proxy	Component Object Model Hijacking	File and Directory Discovery	Remote Desktop Protocol		Cloud	Network Denial of Service	Resource Hijacking
<b>Valid Accounts</b>	InstallUtil	Component Object Model Hijacking	Extra Window Memory Injection	Component Object Model Hijacking	Forced Authentication	File and Directory Discovery	Remote Desktop Protocol		Cloud	Scheduled Transfer	Runtime Data Manipulation
	Launchctl	Create Account	Disabling Security Tools	Connection Proxy	Forced Authentication	File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	Service Stop
	Local Job Scheduling	DLL Search Order Hijacking	File System Permissions Weakness	Control Panel Items	Forced Authentication	File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	Stored Data Manipulation
	LSASS Driver	DLL Side-Loading	File System Permissions Weakness	DCHShadow	Forced Authentication	File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	System Shutdown/Reboot
	Mshta	Dylib Hijacking	Hooking	DLL Side-Loading	Forced Authentication	File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	Transferred Data
	PowerShell	Emend	Execution Guardrails	Execution Guardrails	Forced Authentication	File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	Transferred Data
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	legend
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Domain Generation Algorithms	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Fallback Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-hop Proxy	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multi-Stage Channels	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multiband Communication	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Multilayer Encryption	
						File and Directory Discovery	Remote Desktop Protocol		Cloud	Port Knocking	
	</td										

f. Explain how this information can be useful to the SOC team.

1. Threat Analysis:

Understanding which tactics and techniques are shared between the diverse set of APT groups works to highlight those areas of interest most often targeted by threat actors. This will help in striking the balance between which techniques to monitor and defend.

2. Improving Detection:

When some of the techniques utilized by multiple groups, concentrating on them can enhance the overall detection capabilities in Security Operations Center (SOC). It makes possible to create more specific detection rules and alerts.

3. Enhancing Defense Strategies:

The SOC team can then begin creating or updating defenses to prevent these techniques, as well as find other cases that overlap in usage and work together with Security Engineering to develop a specific coverage for the technique. Offensive: This can range from patching to bolstering configuration settings or increasing user education.

4. Resource Allocation:

There are numerous techniques being used, and knowing what common practices will assist in spending resources properly. As an example, if a method is religiously practiced.

Part 3:

- a. Navigate to the OWASP Top 10 (<https://owasp.org/Top10>).

The screenshot shows the homepage of the OWASP Top 10:2021 website. The header is blue with the text "OWASP Top 10:2021". On the right side of the header are icons for GitHub (4.2k), LinkedIn (824), and a search bar. Below the header, there's a sidebar on the left containing a navigation menu with links like "Home", "Notice", "Introduction", "How to use the OWASP Top 10 as a standard", "How to start an AppSec program with the OWASP Top 10", "About OWASP", "Top 10:2021 List", and specific items A01 through A07. The main content area features a large "Introduction" heading, a "Welcome to the OWASP Top 10 - 2021" message, and the prominent OWASP Top 10 logo. To the right of the logo is a "Table of contents" sidebar with links to various sections such as "Welcome to the OWASP Top 10 - 2021", "What's changed in the Top 10 for 2021", "Methodology", "How the categories are structured", etc.

b. At the time of this writing, the draft of latest list of Top 10 was published in 2021.

Review the Top 10 categories. Pick 3 categories out of the Top 10. In the table below, list your chosen categories. Then briefly describe the category and some of the ways to prevent attacks in the category.

Top 10 Category	Description	Prevention
A02: Cryptographic Failure	Cryptographic shortcomings, formerly named “Sensitive Data Exposure,” are works that involve abuse of, or erroneous implementation or processing of, any algorithm, protocol, or mechanism regarding the conversion of one form of information into a secure format in which the disclosure of information is not possible. Such a category incorporates weak encryption, poor key handling and other issues where data is not protected sufficiently.	Use Strong Encryption: Strong modern criteria and protocols should be used for the cryptographic treatment of sensitive data in active and passive states.  Key Management: Best practices in key management should be employed including safe storage, key rotation, and key life cycle management  Secure Protocols: Secure transport protocols such as TLS should be utilized and updated timely and correctly.
A05: Security Misconfigurations	Security Misconfiguration: Security misconfigurations is a risk that may arise as a result of improper structures within an application, server, or other system components. Misconfigurations means improper design or inappropriate security lets, excess access control, administration interfaces, and vulnerability in the security settings. This will in most cases result to loss of data, access to personal and sensitive information or other critical vulnerabilities.	Start with the most secure configuration possible: Address that default settings and credentials can give rise to certain vulnerabilities.  Disable Unnecessary Features: Disable all of the features and services that cannot be used for the scope of the application or the environment to reduce the attack vectors.  Apply security patches
A03: Injection	Injection flaws take place when a malicious user is allowed to inject ill-sourced data into a certain system which is then run by the application or server. This is common when user information is accepted without sufficient checking or cleansing. Types of injection attacks include SQL Injection, Command Injection and XML Injection, among others. Each of these can result in data leakage, unauthorized information or even total control of the system.	Prepared Statements: Use parameterized queries or prepared statements while dealing with database. This way it is ensured that input data is treated as a normal data rather than as an executable code.  Sanitize Input: All data provided by the user should be normalized and cleansed appropriately or else none of these formats should be accepted.

## Step 2: OWASP Community Pages

The OWASP Community Pages allows security-related contributions from the community. In this part, you will review the Vulnerabilities pages to investigate the attack techniques reported by the contributors.

- a. Navigate to the OWASP Community Page for Vulnerabilities. (<https://owasp.org/www-community/vulnerabilities/>).

OWASP defines a vulnerability as flaw in the application that a threat actor can exploit.

*Question:*

Review the List of Vulnerabilities and pick 3. In the table below, list your chosen vulnerabilities. Briefly describe the vulnerability and some of the ways to prevent exploitation.

The screenshot shows a web browser displaying the OWASP Community Page for Vulnerabilities. The URL in the address bar is highlighted with a red oval. The page itself has a header with the OWASP logo and navigation links for Projects, Chapters, Events, About, and a search bar. Below the header, there's a call-to-action for donations and a section for 'Important Community Links' which includes links to Community, Attacks, Vulnerabilities (which is the current page), and Controls. A sidebar on the right provides information about the OWASP Foundation's mission to improve software security through open source projects and community education.

**Vulnerabilities**

**What is a vulnerability?**

A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application.

Please do not post any actual vulnerabilities in products, services, or web applications. Those disclosure reports should be posted to bugtraq or full-disclosure mailing lists.

**Examples of vulnerabilities**

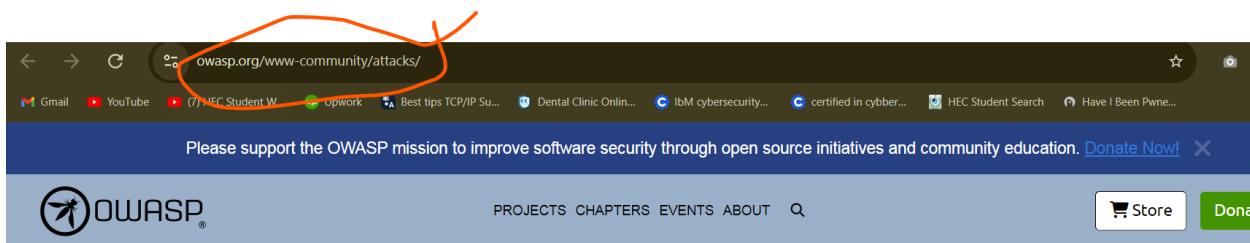
- Lack of input validation on user input
- Lack of sufficient logging mechanism
- Fail-open error handling
- Not closing the database connection properly

For a great overview, check out the [OWASP Top Ten Project](#). You can read about the top vulnerabilities and download a paper that covers them in detail. Many organizations and agencies use the Top Ten as a way of creating awareness about

Vulnerabilities	Descriptions	Preventions
Insecure Deserializations	When someone exploit flaws in the deserialization it will leading to the remote code executions or some other malicious attack	Avoiding from Untrusted data, use secure data serializations libraries that are safe and validate all input data.
Broken Authentications	Bugs or flaws in authentications mechanisms allow attackers to compromise user accounts or perform unwanted or unauthorized actions.	Implement to 2FA authentications and using secure passwords storage processes and limit login attempts.
Misconfigured Security Headers	Not correct security headers can expose applications to attacks such as xss , and clickjacking.	Implement security header proper like CSP – content security policy, X-frame-options

- b. Navigate to the OWASP Community Page for Attacks. (<https://owasp.org/www-community/attacks>).

According to OWASP, an attack is a technique used to exploit application vulnerabilities. Review the **List of Attacks** and pick 3. In the table below, list your chosen attacks. Then briefly describe the attack and some of the ways to prevent it.



The screenshot shows the OWASP homepage. The URL 'owasp.org/www-community/attacks/' is circled in red at the top left. The page features a navigation bar with links for 'PROJECTS', 'CHAPTERS', 'EVENTS', 'ABOUT', and a search bar. A sidebar on the right contains sections for 'The OWASP® Foundation', 'Important Community Links' (Community, Attacks, Vulnerabilities, Controls), and 'Upcoming OWASP Global Events'.

## Attacks

### What is an attack?

Attacks are the techniques that attackers use to exploit the vulnerabilities in applications. Attacks are often confused with vulnerabilities, so please try to be sure that the attack you are describing is something that an attacker would do, rather than a weakness in an application.

### List of Attacks

- [Binary Planting](#)
- [Blind SQL Injection](#)
- [Blind XPath Injection](#)
- [Brute Force Attack](#)
- [Buffer Overflow via Environment Variables](#)
- [Buffer Overflow Attack](#)
- [CORS OriginHeaderScrutiny](#)
- [CORS RequestPreflightScrutiny by Dominique RIGHETTO](#)
- [CSV Injection by Timo Goosen, Albinowax](#)

The OWASP® Foundation works to improve the security of software through its community, open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

### Important Community Links

- [Community](#)
- [Attacks \(You are here\)](#)
- [Vulnerabilities](#)
- [Controls](#)

### Upcoming OWASP Global Events

[Go to Settings to add...](#)

Attacks	Descriptions	Preventions
CSRF-Cross-Site Request Forgery	The attackers tricks a user into performing actions on a web chrome applications where they are authenticated without the user or victims consent.	Using anti-token of the CSRF , validate referrer headers, and implement user expirations controls.
SQL Injections	In this the attacker Injects some malicious SQL payload into an application's query , it will leading to unauthorized access to the database.	Validate and sanitize user inputs, also use parametrize queries.
Cross site scripting	Some malicious scripts are injected into the input field in the trusted websites which will executed in a user' browsers.	Take output in encoding use input validations, employee content security policy and avoid includes not trusted data in HTML.

