30 Initial MITRE Techniques to Cover

1. **T1548** - Abuse Elevation Control Mechanism
   Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Several methods can be used.

2. **T1595.001** - Active Scanning - Scanning IP Blocks
   Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organisations by block, or a range of sequential addresses.

3. **T1071.004** - Application Layer Protocol - DNS
   Adversaries may communicate using the DNS applications layer protocol to avoid detection/network filtering by blending in with existing traffic.

4. **T1010** - Application Window Discovery
   Adversaries may attempt to get a listing of open windows. Window listings could convey information about how the system is used. For example, information about application windows could be used to identify potential data to collect as well as identifying security tooling to evade.

5. **T1499** - Endpoint Denial of Service
   Adversaries may perform Endpoint Denial of Service attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources whose services are hosted on or exploiting the system to cause a persistent crash condition.

6. **T1565** - Data Manipulation - Transmitted Data Manipulation
   Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.

7. **T1001.003** - Data Obfuscation - Protocol or Service Impersonation
   Adversaries may impersonate legitimate protocols or web service traffic to disguise command and control activity and thwart analysis efforts. By impersonating legitimate protocols or web services, adversaries can control traffic to blend in with legitimate network traffic.

8. **T1587.001** - Develop Capabilities - Malware
   Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors, packers, C2 protocols, and the creation of infected removable media. These could then be used as a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviours.

9. **T1048.003** - Exfiltration Over Alternative Protocol - Exfiltration Over Unencrypted Non-C2 Protocol
   Adversaries may steal data by exfiltrating it over an unencrypted network protocol other than that of the existing command control channel. The data may also be sent to an alternate network location from the main command and control server.

10. **T1567.002** - Exfiltration Over Web Service - Exfiltration to Cloud Storage
    Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the internet.

11. **T1590** - Gather Victim Network Information
    Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data as well as specifics regarding its topology and operations.

12. **T1574.011** - Hijack Execution Flow - Service Registry Permissions Weakness
    Adversaries may execute their own malicious payloads by hijacking the registry entries used by services. Flaws in the permissions for registry keys related to services can allow adversaries to redirect the originally specific executable to one they control, launching their own code when a service starts.

13. **T1070** - Indicator Removal
    Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analysed by defenders.

14. **T1056.001** - Input Capture - Keylogging
    Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when OS Credential Dumping efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. Adversaries may also perform actions such as clearing browser cookies to force users to reauthenticate systems to increase the likelihood of capturing credentials quickly.

15. **T1137.003** - Office Application Startup - Outlook Forms
    Adversaries may abuse Microsoft Outlook forms to obtain persistence on a compromised system. Outlook forms are used as templates for presentation and functionality in Outlook messages. Custom Outlook forms can be created that will execute code when a specifically crafted email is sent by an adversary utilizing the same custom Outlook form.

16. **T1201** - Password Policy Discovery

Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through brute force. This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adhere to the policy.

17. **T1566.001** - Phishing - Spearphising Attachment
    Adversaries may send spearphishing emails with malicious attachment in an attempt to gain access to victim systems. Spearphising attachment is a specific variant of spearphishing, it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry.

18. **T1542.003** - Pre-OS Boot - Bootkit
    Adversaries may use bootkits to persist on systems. A bootkit is a malware variant that modifies the boot sectors of a hard drive, allowing malicious code to execute before a computer's OS has loaded. Bootkits reside at a layer below the OS and may make it difficult to perform full remediation unless an organisation suspects one was used and can act accordingly.

19. **T1572** - Protocol Tunnelling
    Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunnelling involves explicitly encapsulating a protocol within another. This behaviour may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN).

20. **T1090.002** - Proxy - External Proxy
    Adversaries may use an external proxy to act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap. Adversaries use these types of proxies to manage command and control communications.

21. **T1558.003** - Steal or Forge Kerberos Tickets - Kerberoasting
    Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to brute force.

22. **T1539** - Steal Web Session Cookie
    An adversary may steal web application or service session cookies and use them to gain access to web applications or internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.

23. **T1220** - XSL Script Processing
    Adversaries may bypass application control and obscure execution of code by embedding scripts inside XSL files. XSL files are commonly used to describe the

processing and rendering of data within XML files. To support complex operations, the XSL standard includes support for embedded scripting in various languages.

24. **T1059.005** - Command and Scripting Interpreter - Visual Basic
    Adversaries may abuse Visual Basic for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as Component Object Model and the Native API through the Windows API.

25. **T1074.001** - Data Staged - Local Data Staging
    Adversaries may stage collected data in a central location or directory on the local system prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data. Interactive command shells may be used, and common functionality within cmd and bash may be used to copy data into a staging location.

26. **T1078.001** - Valid Accounts - Default Accounts
    Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built into an OS, such as the Guest or Administrator accounts on Windows systems.

27. **T1127** - Trusted Developer Utilities Proxy Execution
    Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering. These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

28. **T1218** - System Binary Proxy Execution
    Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the OS. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation.

29. **T1490** - Inhibit System Recovery
    Adversaries may delete or remove built-in data and turn off services designed to aid in recovery of a corrupted system to prevent recovery. This may deny access to available backups and recovery options.

30. **T1555** - Credentials from Password Stores
    Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to

manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.