L-M Saxton – Unit 2 Activity
Attack Enterprise Matrix
https://attack.mitre.org/matrices/enterprise/#

Active Scanning (3)
- Scanning IP Blocks
- Vulnerability Scanning
- Wordlist Scanning

Gather Victim Host Information (4)
- Hardware
- Software
- Firmware
- Client Configurations

Gather Victim Identity Information (3)
- Credentials
- Email Addresses
- Employee Names

Gather Victim Network Information (6)
- Domain Properties
- DNS
- Network Trust Dependencies
- Network Topology
- IP Addresses
- Network Security Appliances

Gather Victim Org Information (4)
- Determine Physical Locations
- Business Relationships
- Identify Business Tempo
- Identify Roles

Phishing for Information (3)
- Spearphishing Service
- Spearphishing Attachment
- Spearphishing Link

Search Closed Sources (2)
- Threat Intel Vendors
- Purchase Technical Data

Search Open Technical Databases (5)
- DNS/Passive DNS
- WHOIS
- Digital Certificates
- CDNs
- Scan Databases

Search Open Websites/Domains (3)
- Social Media
- Search Engines
- Code Repositories

Search Victim-Owned Websites

Acquire Infrastructure (7)
- Domains
- DNS Server
- Virtual Private Server
- Server
- Botnet
- Web Services
- Serverless

Compromise Accounts (3)
- Social Media Accounts
- Email Accounts
- Cloud Accounts

Compromise Infrastructure (7)
- Domains
- DNS Server
- Virtual Private Server
- Server
- Botnet
- Web Services
- Serverless

Develop Capabilities (4)
- Malware
- Code Signing Certificates
- Digital Certificates
- Exploits

Establish Accounts (3)
- Social Media Accounts
- Email Accounts
- Cloud Accounts

Obtain Capabilities (6)
- Malware
- Tool
- Code Signing Certificates
- Digital Certificates
- Exploits
- Vulnerabilities

Stage Capabilities (6)
- Upload Malware
- Upload Tool
- Install Digital Certificate
- Drive-by Target
- Link Target

SEO Poisoning

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Phishing (3)
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service

Replication Through Removable Media

Supply Chain Compromise (3)
- Compromise Software Dependencies and Development Tools
- Compromise Software Supply Chain
- Compromise Hardware Supply Chain

Trusted Relationship

Valid Accounts (4)
- Default Accounts
- Domain Accounts
- Local Accounts
- Cloud Accounts

Command and Scripting Interpreter (8)
- PowerShell
- AppleScript
- Windows Command Shell
- Unix Shell
- Visual Basic
- Python
- JavaScript
- Network Device CLI

Container Administration Command

Deploy Container

Exploitation for Client Execution

Inter-Process Communication (3)
- Component Object Model
- Dynamic Data Exchange
- XPC Services

Native API

Scheduled Task/Job (5)
- At
- Cron
- Scheduled Task
- Systemd Timers
- Container Orchestration Job

Serverless Execution

Shared Modules

Software Deployment Tools

System Services (2)
- Launchctl
- Service Execution

User Execution (3)
- Malicious Link
- Malicious File
- Malicious Image

Windows Management Instrumentation

Account Manipulation (5)
- Additional Cloud Credentials
- Additional Email Delegate Permissions
- Additional Cloud Roles
- SSH Authorized Keys
- Device Registration

BITS Jobs

Boot or Logon Autostart Execution (14)
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- Kernel Modules and Extensions
- Re-opened Applications
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Print Processors
- XDG Autostart Entries
- Active Setup
- Login Items

Boot or Logon Initialization Scripts (5)
- Logon Script (Windows)
- Logon Hook
- Network Logon Script
- RC Scripts
- Startup Items

Browser Extensions

Compromise Client Software Binary

Create Account (3)
- Local Account
- Domain Account
- Cloud Account

Create or Modify System Process (4)
- Launch Agent
- Systemd Service
- Windows Service
- Launch Daemon

Event Triggered Execution (16)
- Change Default File Association
- Screensaver
- Windows Management Instrumentation Event Subscription
- Unix Shell Configuration Modification
- Trap
- LC_LOAD_DYLIB Addition
- Netsh Helper DLL
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Image File Execution Options Injection
- PowerShell Profile
- Emond
- Component Object Model Hijacking
- Installer Packages

External Remote Services

Hijack Execution Flow (12)
- DLL Search Order Hijacking
- DLL Side-Loading
- Dylib Hijacking
- Executable Installer File Permissions Weakness
- Dynamic Linker Hijacking
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness
- COR_PROFILER
- KernelCallbackTable

Implant Internal Image

Modify Authentication Process (7)
- Domain Controller Authentication
- Password Filter DLL
- Pluggable Authentication Modules
- Network Device Authentication
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity

Office Application Startup (6)
- Office Template Macros
- Office Test
- Outlook Forms
- Outlook Home Page
- Outlook Rules
- Add-ins

Pre-OS Boot (5)
- System Firmware
- Component Firmware
- Bootkit
- ROMMONkit
- TFTP Boot

Scheduled Task/Job (5)
- At
- Cron
- Scheduled Task
- Systemd Timers
- Container Orchestration Job

Server Software Component (5)
- SQL Stored Procedures
- Transport Agent
- Web Shell
- IIS Components
- Terminal Services DLL

Traffic Signaling (2)
- Port Knocking
- Socket Filters

Valid Accounts (4)
- Default Accounts
- Domain Accounts
- Local Accounts
- Cloud Accounts

Abuse Elevation Control Mechanism (4)
- Setuid and Setgid
- Bypass User Account Control
- Sudo and Sudo Caching
- Elevated Execution with Prompt

Access Token Manipulation (5)
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection

Boot or Logon Autostart Execution (14)
- Registry Run Keys / Startup Folder
- Authentication Package
- Time Providers
- Winlogon Helper DLL
- Security Support Provider
- Kernel Modules and Extensions
- Re-opened Applications
- LSASS Driver
- Shortcut Modification
- Port Monitors
- Print Processors
- XDG Autostart Entries
- Active Setup
- Login Items

Boot or Logon Initialization Scripts (5)
- Logon Script (Windows)
- Logon Hook
- Network Logon Script
- RC Scripts
- Startup Items

Create or Modify System Process (4)
- Launch Agent
- Systemd Service
- Windows Service
- Launch Daemon

Domain Policy Modification (2)
- Group Policy Modification
- Domain Trust Modification

Escape to Host

Event Triggered Execution (16)
- Change Default File Association
- Screensaver
- Windows Management Instrumentation Event Subscription
- Unix Shell Configuration Modification
- Trap
- LC_LOAD_DYLIB Addition
- Netsh Helper DLL
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- Application Shimming
- Image File Execution Options Injection
- PowerShell Profile
- Emond
- Component Object Model Hijacking
- Installer Packages

Exploitation for Privilege Escalation

Hijack Execution Flow (12)
- DLL Search Order Hijacking
- DLL Side-Loading
- Dylib Hijacking
- Executable Installer File Permissions Weakness
- Dynamic Linker Hijacking
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness

COR_PROFILER
KernelCallbackTable

Process Injection (12)
- Dynamic-link Library Injection
- Portable Executable Injection
- Thread Execution Hijacking
- Asynchronous Procedure Call
- Thread Local Storage
- Ptrace System Calls
- Proc Memory
- Extra Window Memory Injection
- Process Hollowing
- Process Doppelgänging
- VDSO Hijacking
- ListPlanting

Scheduled Task/Job (5)
- At
- Cron
- Scheduled Task
- Systemd Timers
- Container Orchestration Job

Valid Accounts (4)
- Default Accounts
- Domain Accounts
- Local Accounts
- Cloud Accounts

Abuse Elevation Control Mechanism (4)
- Setuid and Setgid
- Bypass User Account Control
- Sudo and Sudo Caching
- Elevated Execution with Prompt

Access Token Manipulation (5)
- Token Impersonation/Theft
- Create Process with Token
- Make and Impersonate Token
- Parent PID Spoofing
- SID-History Injection

BITS Jobs

Build Image on Host

Debugger Evasion

Deobfuscate/Decode Files or Information

Deploy Container

Direct Volume Access

Domain Policy Modification (2)
- Group Policy Modification
- Domain Trust Modification

Execution Guardrails (1)
- Environmental Keying
- Exploitation for Defense Evasion

File and Directory Permissions Modification (2)
- Windows File and Directory Permissions Modification
- Linux and Mac File and Directory Permissions Modification

Hide Artifacts (10)
- Hidden Files and Directories
- Hidden Users
- Hidden Window
- NTFS File Attributes
- Hidden File System
- Run Virtual Instance
- VBA Stomping
- Email Hiding Rules
- Resource Forking
- Process Argument Spoofing

Hijack Execution Flow (12)
- DLL Search Order Hijacking
- DLL Side-Loading
- Dylib Hijacking
- Executable Installer File Permissions Weakness
- Dynamic Linker Hijacking
- Path Interception by PATH Environment Variable
- Path Interception by Search Order Hijacking
- Path Interception by Unquoted Path
- Services File Permissions Weakness
- Services Registry Permissions Weakness
- COR_PROFILER
- KernelCallbackTable

Impair Defenses (9)
- Disable or Modify Tools
- Disable Windows Event Logging
- Impair Command History Logging
- Disable or Modify System Firewall
- Indicator Blocking
- Disable or Modify Cloud Firewall
- Disable Cloud Logs
- Safe Mode Boot
- Downgrade Attack

Indicator Removal (9)
- = Clear Windows Event Logs
- = Clear Linux or Mac System Logs
- Clear Command History
- File Deletion
- Network Share Connection Removal
- Timestomp
- Clear Network Connection History and Configurations
- Clear Mailbox Data
- Clear Persistence
- Indirect Command Execution

Masquerading (7)
- Invalid Code Signature
- = Right-to-Left Override
- Rename System Utilities
- Masquerade Task or Service
- Match Legitimate Name or Location
- Space after Filename
- Double File Extension

Modify Authentication Process (7)
- Domain Controller Authentication
- = Password Filter DLL
- Pluggable Authentication Modules
- Network Device Authentication
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity

Modify Cloud Compute Infrastructure (4)
- Create Snapshot
- = Create Cloud Instance
- Delete Cloud Instance
- Revert Cloud Instance

Modify Registry

Modify System Image (2)
- Patch System Image
- = Downgrade System Image

Network Boundary Bridging (1)
- Network Address Translation Traversal

Obfuscated Files or Information (9)
- Binary Padding
- = Software Packing
- Steganography
- Compile After Delivery
- Indicator Removal from Tools
- HTML Smuggling
- Dynamic API Resolution
- Stripped Payloads
- Embedded Payloads

Plist File Modification

Pre-OS Boot (5)
- System Firmware
- = Component Firmware
- Bootkit
- ROMMONkit
- TFTP Boot

Process Injection (12)
- Dynamic-link Library Injection
- = Portable Executable Injection
- Thread Execution Hijacking
- Asynchronous Procedure Call
- Thread Local Storage
- Ptrace System Calls
- Proc Memory
- Extra Window Memory Injection
- Process Hollowing
- Process Doppelgänging
- VDSO Hijacking
- ListPlanting

Reflective Code Loading

Rogue Domain Controller

Rootkit

Subvert Trust Controls (6)
- Gatekeeper Bypass
- = Code Signing
- SIP and Trust Provider Hijacking
- Install Root Certificate
- Mark-of-the-Web Bypass
- Code Signing Policy Modification

System Binary Proxy Execution (13)
- Compiled HTML File
- Control Panel
- CMSTP
- InstallUtil
- Mshta
- Msiexec
- Odbcconf
- Regsvcs/Regasm
- Regsvr32
- Rundll32
- Verclsid
- Wuauclt
- MMC

System Script Proxy Execution (1)
- PubPrn

Template Injection

Traffic Signaling (2)
- Port Knocking
- Socket Filters

Trusted Developer Utilities Proxy Execution (1)
- MSBuild

Unused/Unsupported Cloud Regions

Use Alternate Authentication Material (4)
- Application Access Token
- Pass the Hash
- Pass the Ticket
- Web Session Cookie

Valid Accounts (4)
- Default Accounts
- Domain Accounts
- Local Accounts
- Cloud Accounts

Virtualization/Sandbox Evasion (3)
- System Checks
- User Activity Based Checks
- Time Based Evasion

Weaken Encryption (2)
- Reduce Key Space
- Disable Crypto Hardware

XSL Script Processing

Adversary-in-the-Middle (3)
- LLMNR/NBT-NS Poisoning and SMB Relay
- ARP Cache Poisoning
- DHCP Spoofing

Brute Force (4)
- Password Guessing
- Password Cracking
- Password Spraying
- Credential Stuffing

Credentials from Password Stores (5)
- Keychain
- Securityd Memory
- Credentials from Web Browsers
- Windows Credential Manager
- Password Managers

Exploitation for Credential Access

Forced Authentication

Forge Web Credentials (2)
- Web Cookies
- SAML Tokens

Input Capture (4)
- Keylogging
- GUI Input Capture
- Web Portal Capture
- Credential API Hooking

Modify Authentication Process (7)
- Domain Controller Authentication
- Password Filter DLL
- Pluggable Authentication Modules
- Network Device Authentication
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity

Multi-Factor Authentication Interception

Multi-Factor Authentication Request Generation

Network Sniffing

OS Credential Dumping (8)
- LSASS Memory
- Security Account Manager
- NTDS
- LSA Secrets
- Cached Domain Credentials
- DCSync
- Proc Filesystem
- /etc/passwd and /etc/shadow

Steal Application Access Token

Steal or Forge Authentication Certificates

Steal or Forge Kerberos Tickets (4)
- Golden Ticket
- Silver Ticket
- Kerberoasting
- AS-REP Roasting

Steal Web Session Cookie

Unsecured Credentials (7)
- Credentials In Files
- Credentials in Registry
- Bash History
- Private Keys
- Cloud Instance Metadata API
- Group Policy Preferences
- Container API

Account Discovery (4)
- Local Account
- Domain Account
- Email Account
- Cloud Account

Application Window Discovery

Browser Bookmark Discovery

Cloud Infrastructure Discovery

Cloud Service Dashboard

Cloud Service Discovery

Cloud Storage Object Discovery

Container and Resource Discovery

Debugger Evasion

Domain Trust Discovery

File and Directory Discovery

Group Policy Discovery

Network Service Discovery

Network Share Discovery

Network Sniffing

Password Policy Discovery

Peripheral Device Discovery

Permission Groups Discovery (3)
- Local Groups
- Domain Groups
- Cloud Groups

Process Discovery

Query Registry

Remote System Discovery

Software Discovery (1)
- Security Software Discovery

System Information Discovery

System Location Discovery (1)
- System Language Discovery

System Network Configuration Discovery (1)
- Internet Connection Discovery

System Network Connections Discovery

System Owner/User Discovery

System Service Discovery

System Time Discovery

Virtualization/Sandbox Evasion (3)
- System Checks
- User Activity Based Checks
- Time Based Evasion

Exploitation of Remote Services

Internal Spearphishing

Lateral Tool Transfer

Remote Service Session Hijacking (2)
- SSH Hijacking
- RDP Hijacking

Remote Services (6)
- Remote Desktop Protocol
- SMB/Windows Admin Shares
- Distributed Component Object Model
- SSH
- VNC
- Windows Remote Management

Replication Through Removable Media

Software Deployment Tools

Taint Shared Content

Use Alternate Authentication Material (4)
- Application Access Token
- Pass the Hash
- Pass the Ticket
- Web Session Cookie

Adversary-in-the-Middle (3)
- LLMNR/NBT-NS Poisoning and SMB Relay
- ARP Cache Poisoning
- DHCP Spoofing

Archive Collected Data (3)
- Archive via Utility
- Archive via Library
- Archive via Custom Method

Audio Capture

Automated Collection

Browser Session Hijacking

Clipboard Data

Data from Cloud Storage

Data from Configuration Repository (2)
- SNMP (MIB Dump)
- Network Device Configuration Dump

Data from Information Repositories (3)
- Confluence
- Sharepoint
- Code Repositories

Data from Local System

Data from Network Shared Drive

Data from Removable Media

Data Staged (2)
- Local Data Staging
- Remote Data Staging

Email Collection (3)
- Local Email Collection
- Remote Email Collection
- Email Forwarding Rule

Input Capture (4)
- Keylogging
- GUI Input Capture
- Web Portal Capture
- Credential API Hooking

Screen Capture

Video Capture

Application Layer Protocol (4)
- Web Protocols
- File Transfer Protocols
- Mail Protocols
- DNS

Communication Through Removable Media

Data Encoding (2)
- Standard Encoding
- Non-Standard Encoding

Data Obfuscation (3)
- Junk Data
- Steganography
- Protocol Impersonation

Dynamic Resolution (3)
- Fast Flux DNS
- Domain Generation Algorithms
- DNS Calculation

Encrypted Channel (2)
- Symmetric Cryptography
- Asymmetric Cryptography

Fallback Channels

Ingress Tool Transfer

Multi-Stage Channels

Non-Application Layer Protocol

Non-Standard Port

Protocol Tunneling

Proxy (4)
- Internal Proxy
- External Proxy
- Multi-hop Proxy
- Domain Fronting

Remote Access Software

Traffic Signaling (2)
- Port Knocking
- Socket Filters

Web Service (3)
- Dead Drop Resolver
- Bidirectional Communication
- One-Way Communication

Automated Exfiltration (1)
- Traffic Duplication

Data Transfer Size Limits

Exfiltration Over Alternative Protocol (3)
- Exfiltration Over Symmetric Encrypted Non-C2 Protocol
- Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- Exfiltration Over Unencrypted Non-C2 Protocol

Exfiltration Over C2 Channel

Exfiltration Over Other Network Medium (1)
- Exfiltration Over Bluetooth

Exfiltration Over Physical Medium (1)
- Exfiltration over USB

Exfiltration Over Web Service (2)
- Exfiltration to Code Repository
- Exfiltration to Cloud Storage

Scheduled Transfer

Transfer Data to Cloud Account

Account Access Removal

Data Destruction

Data Encrypted for Impact

Data Manipulation (3)
- Stored Data Manipulation
- Transmitted Data Manipulation
- Runtime Data Manipulation

Defacement (2)
- Internal Defacement
- External Defacement

Disk Wipe (2)
- Disk Content Wipe
- Disk Structure Wipe

Endpoint Denial of Service (4)
- OS Exhaustion Flood
- Service Exhaustion Flood
- Application Exhaustion Flood
- Application or System Exploitation

Firmware Corruption

Inhibit System Recovery

Network Denial of Service (2)
- Direct Network Flood
- Reflection Amplification

Resource Hijacking

Service Stop

System Shutdown/Reboot

Did you have any issues or challenges with the literature search/audit on software sites and the national vulnerabilities database?
No issues; CAPEC has been used in other reports – it was helpful to have the CVE report list penetration test categories.

How did you overcome them?
No issues; CAPEC has been used in other reports – it was helpful to have the CVE report list penetration test categories.

How will they affect your final report?
Here is a good benchmark for various attacks that can come up during a penetration test.