RANGEFORCE

RANGEFORCE TRAINING MODULE COVERAGE FOR MITRE'S ATT&CK™ 2019

MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK™) is a curated framework for understanding typical cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. RangeForce's Training Modules are mapped to the ATT&CK Framework as an effective means for security leaders to manage training priorities for team members. In many cases, multiple training modules fall under a single section of the framework. An example being RangeForce's WASE Module, which includes training and simulations on SQL Injection, NoSQL Injection, and Command Injection, all of which all fall into the "Exploit Public-Facing Application" section, "Initial Access" category of ATT&CK Framework. The RangeForce development team uses the ATT&CK Framework to help prioritize training module development, and as coverage increases with new module delivery, coverage mapping will be updated.

LINUX COVERAGE 2019

Initial Access
Drive-by Compromise
Exploit Public-Facing Application
Hardware Additions
Spearphishing Attachment
Spear Phishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
Command-Line Interface
Exploitation for Client Execution
Graphical User Interface
Local Job Scheduling
Scripting
Source
Space after Filename
Third-party Software
Trap
User Execution

Persistence
.bash_profile and .bashrc
Bootkit
Browser Extensions
Create Account
Hidden Files and Directories
Kernel Modules and Extensions
Local Job Scheduling
Port Knocking
Redundant Access
Setuid and Setgid
Systemd Service
Trap
Valid Accounts
Web Shell

Privilege Escalation
Exploitation for Privilege Escalation
Process Injection
Setuid and Setgid
Sudo
Sudo Caching
Valid Accounts
Web Shell

Defense Evasion
Binary Padding
Clear Command History
Compile After Delivery
Disabling Security Tools
Execution Guardrails
Exploitation for Defense Evasion
File Deletion
File Permissions Modification
Hidden Files and Directories
HISTCONTROL
Indicator Removal from Tools
Indicator Removal on Host
Install Root Certificate
Masquerading
Obfuscated Files or Information
Port Knocking
Process Injection
Redundant Access
Rootkit
Scripting
Space after Filename
Timestomp
Valid Accounts
Web Shell

Credential Access
Bash History
Brute Force
Credential Dumping
Credentials in Files
Exploitation for Credential Access
Input Capture
Network Sniffing
Private Keys
Two-Factor Authentication Interception

Discovery
Account Discovery
Browser Bookmark Discovery
File and Directory Discovery
Network Service Scanning
Network Sniffing
Password Policy Discovery
Permission Groups Discovery
Process Discovery
Remote System Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery

Lateral Movement
Application Deployment Software
Exploitation of Remote Services
Remote File Copy
Remote Services
SSH Hijacking
Third-party Software

Collection
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Input Capture
Screen Capture

Command And Control
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

Exfiltration
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

Impact
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Stored Data Manipulation
Transmitted Data Manipulation

MITRE ATT&CK™

www.rangeforce.com

RANGEFORCE

RANGEFORCE TRAINING MODULE COVERAGE FOR MITRE'S ATT&CK™ 2019

MICROSOFT COVERAGE 2019

Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spear Phishing Attachment
Spear Phishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Third-party Software
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management
XSL Script Processing

Persistence
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Logon Scripts
LSASS Driver
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup
Path Interception
Port Monitors
Redundant Access
Registry Run Keys / Startup Folder
Scheduled Task
Screensaver
Security Support Provider
Service Registry Permissions Weakness
Shortcut Modification
SIP and Trust Provider Hijacking
System Firmware
Time Providers
Valid Accounts
Web Shell
Windows Management Instrumentation Event Subscription
Winlogon Helper DLL

Privilege Escalation
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
New Service
Path Interception
Port Monitors
Process Injection
Scheduled Task
Service Registry Permissions Weakness
SID-History Injection
Valid Accounts
Web Shell

Defense Evasion
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
CMSTP
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File Deletion
File Permissions Modification
File System Logical Offsets
Group Policy Modification
Hidden Files and Directories
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Indirect Command Execution
Install Root Certificate
InstallUtil
Masquerading
Modify Registry
Mshta
Network Share Connection Removal
NTFS File Attributes
Obfuscated Files or Information
Process Doppelganging
Process Hollowing
Process Injection
Redundant Access
Regsvcs/Regasm
Regsvr32
Rootkit
Rundll32
Scripting
Signed Binary Proxy Execution
Signed Script Proxy Execution
SIP and Trust Provider Hijacking
Software Packing
Template Injection
Timestomp
Trusted Developer Utilities
Valid Accounts
Virtualization/Sandbox Evasion
Web Service
XSL Script Processing

Credential Access
Account Manipulation
Brute Force
Credential Dumping
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Two-Factor Authentication Interception

Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion

Lateral Movement
Application Deployment Software
Distributed Component Object Model
Exploitation of Remote Services
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

Collection
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture

Command And Control
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service

Exfiltration
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

Impact
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
Transmitted Data Manipulation

MITRE ATT&CK™

www.rangeforce.com