MITRE ATT&CK / Linux Matrix

ID:TA0001 - Initial Access

- T1189 Drive-by Compromise
- T1190 - Exploit Public-Facing Application
- T1133 - External Remote Services
- T1200 - Hardware Additions
- T1566 - Phishing
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- T1195 - Supply Chain Compromise
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
  - Compromise Hardware Supply Chain
- T1199 - Trusted Relationship
- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

ID:TA0002 - Execution

- T1059 - Command and Scripting Interpreter
  - Unix Shell
  - Visual Basic
  - Python
  - JavaScript
- T1203 - Exploitation for Client Execution
- T1559 - Inter-Process Communication
- T1106 - Native API
- T1053 - Scheduled Task/Job
  - At
  - Cron
  - Systemd Timers
- T1072 - Software Deployment Tools
- T1569 - System Services
- T1204 - User Execution
  - Malicious Link
  - Malicious File

ID:TA0003 - Persistence

- T1098 - Account Manipulation — SSH Authorized Keys
- T1547 - Boot or Logon Autostart Execution
  - Kernel Modules and Extensions
  - XDG Autostart Entries
- T1037 - Boot or Logon Initialization Scripts — RC Scripts
- T1176 - Browser Extensions
- T1554 - Compromise Client Software Binary
- T1136 - Create Account
  - Local Account
  - Domain Account
- T1543 - Create or Modify System Process — Systemd Service
- T1546 - Event Triggered Execution
  - Unix Shell Configuration Modification
  - Trap
  - Installer Packages
- T1133 - External Remote Services
- T1574 - Hijack Execution Flow — Dynamic Linker Hijacking
- T1556 - Modify Authentication Process
  - Pluggable Authentication Modules
  - Multi-Factor Authentication
- T1542 - Pre-OS Boot
  - Component Firmware
  - Bootkit
- T1053 - Scheduled Task/Job
  - At
  - Cron
  - Systemd Timers
- T1505 - Server Software Component
  - SQL Stored Procedures
  - Transport Agent
  - Web Shell
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

ID:TA0004 - Privilege Escalation

- T1548 - Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Sudo and Sudo Caching
- T1547 - Boot or Logon Autostart Execution
  - Kernel Modules and Extensions
  - XDG Autostart Entries
- T1037 - Boot or Logon Initialization Scripts — RC Scripts
- T1543 - Create or Modify System Process — Systemd Service
- T1611 - Escape to Host
- T1546 - Event Triggered Execution
  - Unix Shell Configuration Modification
  - Trap
  - Installer Packages
- T1068 - Exploitation for Privilege Escalation
- T1574 - Hijack Execution Flow — Dynamic Linker Hijacking
- T1055 - Process Injection
  - Ptrace System Calls
  - Proc Memory
  - VDSO Hijacking
- T1053 - Scheduled Task/Job
  - At
  - Cron
  - Systemd Timers
- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts

ID:TA0005 - Defense Evasion

- T1548 - Abuse Elevation Control Mechanism
  - Setuid and Setgid
  - Sudo and Sudo Caching
- T1622 - Debugger Evasion
- T1140 - Deobfuscate/Decode Files or Information
- T1480 - Execution Guardrails — Environmental Keying
- T1211 - Exploitation for Defense Evasion
- T1222 - File and Directory Permissions Modification — Linux and Mac File and Directory Permissions Modification
- T1564 - Hide Artifacts
  - Hidden Files and Directories
  - Hidden Users
  - Hidden Window
  - Hidden File System
  - Run Virtual Instance
  - VBA Stomping
  - Email Hiding Rules
- T1574 - Hijack Execution Flow — Dynamic Linker Hijacking
- T1562 - Impair Defenses
  - Disable or Modify Tools
  - Impair Command History Logging
  - Disable or Modify System Firewall
  - Indicator Blocking
  - Downgrade Attack
- T1070 - Indicator Removal
  - Clear Linux or Mac System Logs
  - Clear Command History
  - File Deletion
  - Timestomp
  - Clear Network Connection History and Configurations
  - Clear Mailbox Data
  - Clear Persistence
- T1036 - Masquerading
  - Right-to-Left Override
  - Rename System Utilities
  - Masquerade Task or Service
  - Match Legitimate Name or Location
  - Space after Filename
- T1556 - Modify Authentication Process
  - Pluggable Authentication Modules
  - Multi-Factor Authentication
- T1027 - Obfuscated Files or Information
  - Binary Padding
  - Software Packing
  - Steganography
  - Compile After Delivery
  - Indicator Removal from Tools
  - HTML Smuggling
  - Stripped Payloads
  - Embedded Payloads
- T1542 - Pre-OS Boot
  - Component Firmware
  - Bootkit
- T1055 - Process Injection
  - Ptrace System Calls
  - Proc Memory
  - VDSO Hijacking
- T1620 - Reflective Code Loading
- T1014 - Rootkit
- T1553 - Subvert Trust Controls — Install Root Certificate
- T1218 - System Binary Proxy Execution
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1078 - Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
- T1497 - Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion

ID:TA0006 - Credential Access

- T1557 - Adversary-in-the-Middle
  - ARP Cache Poisoning
  - DHCP Spoofing
- T1110 - Brute Force
  - Password Guessing
  - Password Cracking
  - Password Spraying
  - Credential Stuffing
- T1555 - Credentials from Password Stores
  - Securityd Memory
  - Credentials from Web Browsers
  - Password Managers
- T1212 - Exploitation for Credential Access
- T1606 - Forge Web Credentials — Web Cookies
- T1056 - Input Capture
  - Keylogging
  - GUI Input Capture
  - Web Portal Capture
- T1556 - Modify Authentication Process
  - Pluggable Authentication Modules
  - Multi-Factor Authentication
- T1111 - Multi-Factor Authentication Interception
- T1621 - Multi-Factor Authentication Request Generation
- T1040 - Network Sniffing
- T1003 - OS Credential Dumping
  - Proc Filesystem
  - /etc/passwd and /etc/shadow
- T1649 - Steal or Forge Authentication Certificates
- T1558 - Steal or Forge Kerberos Tickets
- T1539 - Steal Web Session Cookie
- T1552 - Unsecured Credentials
  - Credentials In Files
  - Bash History
  - Private Keys

ID:TA0007 - Discovery

- T1087 - Account Discovery
  - Local Account
  - Domain Account
- T1010 - Application Window Discovery
- T1217 - Browser Bookmark Discovery
- T1622 - Debugger Evasion
- T1083 - File and Directory Discovery
- T1046 - Network Service Discovery
- T1135 - Network Share Discovery
- T1040 - Network Sniffing
- T1201 - Password Policy Discovery
- T1120 - Peripheral Device Discovery
- T1069 - Permission Groups Discovery
  - Local Groups
  - Domain Groups
- T1057 - Process Discovery
- T1018 - Remote System Discovery
- T1518 - Software Discovery — Security Software Discovery
- T1082 - System Information Discovery
- T1614 - System Location Discovery — System Language Discovery
- T1016 - System Network Configuration Discovery — Internet Connection Discovery
- T1049 - System Network Connections Discovery
- T1033 - System Owner/User Discovery
- T1007 - System Service Discovery
- T1497 - Virtualization/Sandbox Evasion
  - System Checks
  - User Activity Based Checks
  - Time Based Evasion

ID:TA0008 - Lateral Movement

- T1210 - Exploitation of Remote Services
- T1534 - Internal Spearphishing
- T1570 - Lateral Tool Transfer
- T1563 - Remote Service Session Hijacking — SSH Hijacking
- T1021 - Remote Services
  - SSH
  - VNC
- T1072 - Software Deployment Tools
- T1080 - Taint Shared Content

ID:TA0009 - Collection

- T1557 - Adversary-in-the-Middle
  - ARP Cache Poisoning
  - DHCP Spoofing
- T1560 - Archive Collected Data
  - Archive via Utility
  - Archive via Library
  - Archive via Custom Method
- T1123 - Audio Capture
- T1119 - Automated Collection
- T1115 - Clipboard Data
- T1213 - Data from Information Repositories
- T1005 - Data from Local System
- T1039 - Data from Network Shared Drive
- T1025 - Data from Removable Media
- T1074 - Data Staged
  - Local Data Staging
  - Remote Data Staging
- T1114 - Email Collection — Email Forwarding Rule
- T1056 - Input Capture
  - Keylogging
  - GUI Input Capture
  - Web Portal Capture
- T1113 - Screen Capture
- T1125 - Video Capture

ID:TA0010 - Exfiltration

- T1020 - Automated Exfiltration
- T1030 - Data Transfer Size Limits
- T1048 - Exfiltration Over Alternative Protocol
  - Exfiltration Over Symmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
  - Exfiltration Over Unencrypted Non-C2 Protocol
- T1041 - Exfiltration Over C2 Channel
- T1011 - Exfiltration Over Other Network Medium — Exfiltration Over Bluetooth
- T1052 - Exfiltration Over Physical Medium — Exfiltration over USB
- T1567 - Exfiltration Over Web Service
  - Exfiltration to Code Repository
  - Exfiltration to Cloud Storage
- T1029 - Scheduled Transfer

ID:TA0011 - Command and Control

- T1071 - Application Layer Protocol
  - Web Protocols
  - File Transfer Protocols
  - Mail Protocols
  - DNS
- T1092 - Communication Through Removable Media
- T1132 - Data Encoding
  - Standard Encoding
  - Non-Standard Encoding
- T1001 - Data Obfuscation
  - Junk Data
  - Steganography
  - Protocol Impersonation
- T1568 - Dynamic Resolution
  - Fast Flux DNS
  - Domain Generation Algorithms
  - DNS Calculation
- T1573 - Encrypted Channel
  - Symmetric Cryptography
  - Asymmetric Cryptography
- T1008 - Fallback Channels
- T1105 - Ingress Tool Transfer
- T1104 - Multi-Stage Channels
- T1095 - Non-Application Layer Protocol
- T1571 - Non-Standard Port
- T1572 - Protocol Tunneling
- T1090 - Proxy
  - Internal Proxy
  - External Proxy
  - Multi-hop Proxy
  - Domain Fronting
- T1219 - Remote Access Software
- T1205 - Traffic Signaling
  - Port Knocking
  - Socket Filters
- T1102 - Web Service
  - Dead Drop Resolver
  - Bidirectional Communication
  - One-Way Communication

ID:TA0040 - Impact

- T1531 - Account Access Removal
- T1485 - Data Destruction
- T1486 - Data Encrypted for Impact
- T1565 - Data Manipulation
  - Stored Data Manipulation
  - Transmitted Data Manipulation
  - Runtime Data Manipulation
- T1491 - Defacement
  - Internal Defacement
  - External Defacement
- T1561 - Disk Wipe
  - Disk Content Wipe
  - Disk Structure Wipe
- T1499 - Endpoint Denial of Service
  - OS Exhaustion Flood
  - Service Exhaustion Flood
  - Application Exhaustion Flood
  - Application or System Exploitation
- T1495 - Firmware Corruption
- T1490 - Inhibit System Recovery
- T1498 - Network Denial of Service
  - Direct Network Flood
  - Reflection Amplification
- T1496 - Resource Hijacking
- T1489 - Service Stop
- T1529 - System Shutdown/Reboot