



 [redcanaryco](#) / [atomic-red-team](#)

 Watch

208

 Star

1,987

 Fork

609

 Code

 Issues 5

 Pull requests 7

 Insights

Join GitHub today

Dismiss

GitHub is home to over 31 million developers working together to host and review code, manage projects, and build software together.

Sign up

Branch: master ▾

[atomic-red-team](#) / [atomics](#) / [linux-index.md](#)

Find file

Copy path

 **MHaggis** T1100 and T1071 (#475)

0c3e47f 25 days ago

5 contributors



287 lines (275 sloc) | 17.5 KB

Raw

Blame

History



Linux Atomic Tests by ATT&CK Tactic & Technique

persistence

- [T1156 .bash_profile and .bashrc](#)
 - Atomic Test #1: Add command to .bash_profile [macos, linux]
 - Atomic Test #2: Add command to .bashrc [macos, linux]
- T1067 Bootkit [CONTRIBUTE A TEST](#)
- [T1176 Browser Extensions](#)
 - Atomic Test #1: Chrome (Developer Mode) [linux, windows, macos]
 - Atomic Test #2: Chrome (Chrome Web Store) [linux, windows, macos]
 - Atomic Test #3: Firefox [linux, windows, macos]
- [T1136 Create Account](#)
 - Atomic Test #1: Create a user account on a Linux system [linux]
 - Atomic Test #5: Create a new user in Linux with `root` UID and GID. [linux]
- [T1158 Hidden Files and Directories](#)
 - Atomic Test #1: Create a hidden file in a hidden directory [linux, macos]
 - Atomic Test #3: Hidden file [macos, linux]
 - Atomic Test #9: Create Visible Directories [macos, linux]
 - Atomic Test #10: Create hidden directories and files [macos, linux]
- T1215 Kernel Modules and Extensions [CONTRIBUTE A TEST](#)
- [T1168 Local Job Scheduling](#)
 - Atomic Test #1: Cron - Replace crontab with referenced file [macos, centos, ubuntu, linux]
 - Atomic Test #2: Cron - Add script to cron folder [macos, centos, ubuntu, linux]
 - Atomic Test #3: Event Monitor Daemon Persistence [macos, centos, ubuntu, linux]
- T1205 Port Knocking [CONTRIBUTE A TEST](#)

- T1108 Redundant Access [CONTRIBUTE A TEST](#)
- [T1166 Setuid and Setgid](#)
 - Atomic Test #1: Setuid and Setgid [macos, centos, ubuntu, linux]
 - Atomic Test #2: Set a SetUID flag on file [macos, centos, ubuntu, linux]
 - Atomic Test #3: Set a SetGID flag on file [macos, centos, ubuntu, linux]
- [T1154 Trap](#)
 - Atomic Test #1: Trap [macos, centos, ubuntu, linux]
- T1078 Valid Accounts [CONTRIBUTE A TEST](#)
- [T1100 Web Shell](#)

discovery

- [T1087 Account Discovery](#)
 - Atomic Test #1: Enumerate all accounts [linux, macos]
 - Atomic Test #2: View sudoers access [linux, macos]
 - Atomic Test #3: View accounts with UID 0 [linux, macos]
 - Atomic Test #4: Show if a user account has ever logged in remotely [linux, macos]
 - Atomic Test #5: Enumerate users and groups [linux, macos]
- [T1217 Browser Bookmark Discovery](#)
 - Atomic Test #1: List Mozilla Firefox Bookmark Database Files on Linux [linux]
- [T1083 File and Directory Discovery](#)
 - Atomic Test #3: Nix File and Directory Discovery [macos, linux]
 - Atomic Test #4: Nix File and Directory Discovery [macos, linux]
- [T1046 Network Service Scanning](#)
 - Atomic Test #1: Port Scan [linux, macos]

- Atomic Test #2: Port Scan Nmap [linux, macos]
- [T1040 Network Sniffing](#)
 - Atomic Test #1: Packet Capture Linux [linux]
- [T1201 Password Policy Discovery](#)
 - Atomic Test #1: Examine password complexity policy - Ubuntu [ubuntu]
 - Atomic Test #2: Examine password complexity policy - CentOS/RHEL 7.x [centos]
 - Atomic Test #3: Examine password complexity policy - CentOS/RHEL 6.x [centos]
 - Atomic Test #4: Examine password expiration policy - All Linux [linux]
- [T1069 Permission Groups Discovery](#)
 - Atomic Test #1: Permission Groups Discovery [macos, linux]
- [T1057 Process Discovery](#)
 - Atomic Test #1: Process Discovery - ps [macos, centos, ubuntu, linux]
- [T1018 Remote System Discovery](#)
 - Atomic Test #4: Remote System Discovery - arp nix [linux, macos]
 - Atomic Test #5: Remote System Discovery - sweep [linux, macos]
- [T1082 System Information Discovery](#)
 - Atomic Test #2: System Information Discovery [linux, macos]
 - Atomic Test #3: List OS Information [linux, macos]
- [T1016 System Network Configuration Discovery](#)
 - Atomic Test #2: System Network Configuration Discovery [macos, linux]
- [T1049 System Network Connections Discovery](#)
 - Atomic Test #3: System Network Connections Discovery Linux & MacOS [linux, macos]
- [T1033 System Owner/User Discovery](#)
 - Atomic Test #2: System Owner/User Discovery [linux, macos]

lateral-movement

- T1017 Application Deployment Software [CONTRIBUTE A TEST](#)
- T1210 Exploitation of Remote Services [CONTRIBUTE A TEST](#)
- [T1105 Remote File Copy](#)
 - Atomic Test #1: rsync remote file copy (push) [linux, macos]
 - Atomic Test #2: rsync remote file copy (pull) [linux, macos]
 - Atomic Test #3: scp remote file copy (push) [linux, macos]
 - Atomic Test #4: scp remote file copy (pull) [linux, macos]
 - Atomic Test #5: sftp remote file copy (push) [linux, macos]
 - Atomic Test #6: sftp remote file copy (pull) [linux, macos]
- T1021 Remote Services [CONTRIBUTE A TEST](#)
- T1184 SSH Hijacking [CONTRIBUTE A TEST](#)
- T1072 Third-party Software [CONTRIBUTE A TEST](#)

collection

- [T1123 Audio Capture](#)
- [T1119 Automated Collection](#)
- [T1115 Clipboard Data](#)
- [T1074 Data Staged](#)
 - Atomic Test #1: Stage data from Discovery.sh [linux, macos]
- T1213 Data from Information Repositories [CONTRIBUTE A TEST](#)
- [T1005 Data from Local System](#)

- T1039 Data from Network Shared Drive [CONTRIBUTE A TEST](#)
- T1025 Data from Removable Media [CONTRIBUTE A TEST](#)
- [T1056 Input Capture](#)
- [T1113 Screen Capture](#)
 - Atomic Test #3: X Windows Capture [linux]
 - Atomic Test #4: Import [linux]

exfiltration

- T1020 Automated Exfiltration [CONTRIBUTE A TEST](#)
- [T1002 Data Compressed](#)
 - Atomic Test #3: Data Compressed - nix - zip [linux, macos]
 - Atomic Test #4: Data Compressed - nix - gzip Single File [linux, macos]
 - Atomic Test #5: Data Compressed - nix - tar Folder or File [linux, macos]
- [T1022 Data Encrypted](#)
 - Atomic Test #1: Data Encrypted with zip and gpg [macos, centos, ubuntu, linux]
- [T1030 Data Transfer Size Limits](#)
 - Atomic Test #1: Data Transfer Size Limits [macos, centos, ubuntu, linux]
- [T1048 Exfiltration Over Alternative Protocol](#)
 - Atomic Test #1: Exfiltration Over Alternative Protocol - SSH [macos, centos, ubuntu, linux]
 - Atomic Test #2: Exfiltration Over Alternative Protocol - SSH [macos, centos, ubuntu, linux]
 - Atomic Test #3: Exfiltration Over Alternative Protocol - HTTP [macos, centos, ubuntu, linux]
- T1041 Exfiltration Over Command and Control Channel [CONTRIBUTE A TEST](#)
- T1011 Exfiltration Over Other Network Medium [CONTRIBUTE A TEST](#)
- T1052 Exfiltration Over Physical Medium [CONTRIBUTE A TEST](#)

- T1029 Scheduled Transfer [CONTRIBUTE A TEST](#)

credential-access

- [T1139 Bash History](#)
 - Atomic Test #1: xxxx [linux, macos]
- [T1110 Brute Force](#)
- [T1003 Credential Dumping](#)
- [T1081 Credentials in Files](#)
 - Atomic Test #2: Extract credentials from files [macos, linux]
- T1212 Exploitation for Credential Access [CONTRIBUTE A TEST](#)
- [T1056 Input Capture](#)
- [T1040 Network Sniffing](#)
 - Atomic Test #1: Packet Capture Linux [linux]
- [T1145 Private Keys](#)
 - Atomic Test #2: Discover Private SSH Keys [macos, linux]
 - Atomic Test #3: Copy Private SSH Keys with CP [linux]
 - Atomic Test #4: Copy Private SSH Keys with rsync [macos, linux]
- T1111 Two-Factor Authentication Interception [CONTRIBUTE A TEST](#)

defense-evasion

- [T1009 Binary Padding](#)
 - Atomic Test #1: Pad Binary to Change Hash - Linux/macOS dd [macos, linux]

- [T1146 Clear Command History](#)
 - Atomic Test #1: Clear Bash history (rm) [linux, macos]
 - Atomic Test #2: Clear Bash history (echo) [linux, macos]
 - Atomic Test #3: Clear Bash history (cat dev/null) [linux, macos]
 - Atomic Test #4: Clear Bash history (ln dev/null) [linux, macos]
 - Atomic Test #5: Clear Bash history (truncate) [linux]
 - Atomic Test #6: Clear history of a bunch of shells [linux, macos]
- [T1089 Disabling Security Tools](#)
 - Atomic Test #1: Disable iptables firewall [linux]
 - Atomic Test #2: Disable syslog [linux]
 - Atomic Test #3: Disable Cb Response [linux]
 - Atomic Test #4: Disable SELinux [linux]
- T1211 Exploitation for Defense Evasion [CONTRIBUTE A TEST](#)
- [T1107 File Deletion](#)
 - Atomic Test #1: Delete a single file - Linux/macOS [linux, macos]
 - Atomic Test #2: Delete an entire folder - Linux/macOS [linux, macos]
 - Atomic Test #3: Overwrite and delete a file with shred [linux]
 - Atomic Test #12: Delete Filesystem - Linux [linux, centos, ubuntu]
- [T1222 File Permissions Modification](#)
 - Atomic Test #8: chmod - Change file or folder mode (numeric mode) [macos, linux]
 - Atomic Test #9: chmod - Change file or folder mode (symbolic mode) [macos, linux]
 - Atomic Test #10: chmod - Change file or folder mode (numeric mode) recursively [macos, linux]
 - Atomic Test #11: chmod - Change file or folder mode (symbolic mode) recursively [macos, linux]
 - Atomic Test #12: chown - Change file or folder ownership and group [macos, linux]

- Atomic Test #13: chown - Change file or folder ownership and group recursively [macos, linux]
- Atomic Test #14: chown - Change file or folder mode ownership only [macos, linux]
- Atomic Test #15: chown - Change file or folder ownership recursively [macos, linux]
- Atomic Test #16: chattr - Remove immutable file attribute [macos, linux]
- [T1148 HISTCONTROL](#)
 - Atomic Test #1: Disable history collection [linux, macos]
 - Atomic Test #2: Mac HISTCONTROL [macos, linux]
- [T1158 Hidden Files and Directories](#)
 - Atomic Test #1: Create a hidden file in a hidden directory [linux, macos]
 - Atomic Test #3: Hidden file [macos, linux]
 - Atomic Test #9: Create Visible Directories [macos, linux]
 - Atomic Test #10: Create hidden directories and files [macos, linux]
- T1066 Indicator Removal from Tools [CONTRIBUTE A TEST](#)
- [T1070 Indicator Removal on Host](#)
 - Atomic Test #3: rm -rf [macos, linux]
 - Atomic Test #4: Overwrite Linux Mail Spool [linux]
 - Atomic Test #5: Overwrite Linux Log [linux]
- [T1130 Install Root Certificate](#)
 - Atomic Test #1: Install root CA on CentOS/RHEL [linux]
- [T1036 Masquerading](#)
 - Atomic Test #2: Masquerading as Linux crond process. [linux]
- [T1027 Obfuscated Files or Information](#)
 - Atomic Test #1: Decode base64 Data into Script [macos, linux]
- T1205 Port Knocking [CONTRIBUTE A TEST](#)
- [T1055 Process Injection](#)

- Atomic Test #3: Shared Library Injection via /etc/ld.so.preload [linux]
- T1108 Redundant Access [CONTRIBUTE A TEST](#)
- [T1014 Rootkit](#)
 - Atomic Test #1: Loadable Kernel Module based Rootkit [linux]
 - Atomic Test #2: Loadable Kernel Module based Rootkit [linux]
- [T1064 Scripting](#)
 - Atomic Test #1: Create and Execute Bash Shell Script [macos, linux]
- [T1151 Space after Filename](#)
- [T1099 Timestomp](#)
 - Atomic Test #1: Set a file's access timestamp [linux, macos]
 - Atomic Test #2: Set a file's modification timestamp [linux, macos]
 - Atomic Test #3: Set a file's creation timestamp [linux, macos]
 - Atomic Test #4: Modify file timestamps using reference file [linux, macos]
- T1078 Valid Accounts [CONTRIBUTE A TEST](#)
- T1102 Web Service [CONTRIBUTE A TEST](#)

execution

- [T1059 Command-Line Interface](#)
 - Atomic Test #1: Command-Line Interface [macos, centos, ubuntu, linux]
- T1203 Exploitation for Client Execution [CONTRIBUTE A TEST](#)
- T1061 Graphical User Interface [CONTRIBUTE A TEST](#)
- [T1168 Local Job Scheduling](#)
 - Atomic Test #1: Cron - Replace crontab with referenced file [macos, centos, ubuntu, linux]
 - Atomic Test #2: Cron - Add script to cron folder [macos, centos, ubuntu, linux]

- Atomic Test #3: Event Monitor Daemon Persistence [macos, centos, ubuntu, linux]
- [T1064 Scripting](#)
 - Atomic Test #1: Create and Execute Bash Shell Script [macos, linux]
- [T1153 Source](#)
 - Atomic Test #1: Execute Script using Source [macos, linux]
 - Atomic Test #2: Execute Script using Source Alias [macos, linux]
- [T1151 Space after Filename](#)
- T1072 Third-party Software [CONTRIBUTE A TEST](#)
- [T1154 Trap](#)
 - Atomic Test #1: Trap [macos, centos, ubuntu, linux]
- T1204 User Execution [CONTRIBUTE A TEST](#)

command-and-control

- T1043 Commonly Used Port [CONTRIBUTE A TEST](#)
- T1092 Communication Through Removable Media [CONTRIBUTE A TEST](#)
- [T1090 Connection Proxy](#)
 - Atomic Test #1: Connection Proxy [macos, linux]
- T1094 Custom Command and Control Protocol [CONTRIBUTE A TEST](#)
- T1024 Custom Cryptographic Protocol [CONTRIBUTE A TEST](#)
- [T1132 Data Encoding](#)
 - Atomic Test #1: Base64 Encoded data. [macos, linux]
- T1001 Data Obfuscation [CONTRIBUTE A TEST](#)
- T1172 Domain Fronting [CONTRIBUTE A TEST](#)
- T1008 Fallback Channels [CONTRIBUTE A TEST](#)

- T1104 Multi-Stage Channels [CONTRIBUTE A TEST](#)
- T1188 Multi-hop Proxy [CONTRIBUTE A TEST](#)
- T1026 Multiband Communication [CONTRIBUTE A TEST](#)
- T1079 Multilayer Encryption [CONTRIBUTE A TEST](#)
- T1205 Port Knocking [CONTRIBUTE A TEST](#)
- T1219 Remote Access Tools [CONTRIBUTE A TEST](#)
- [T1105 Remote File Copy](#)
 - Atomic Test #1: rsync remote file copy (push) [linux, macos]
 - Atomic Test #2: rsync remote file copy (pull) [linux, macos]
 - Atomic Test #3: scp remote file copy (push) [linux, macos]
 - Atomic Test #4: scp remote file copy (pull) [linux, macos]
 - Atomic Test #5: sftp remote file copy (push) [linux, macos]
 - Atomic Test #6: sftp remote file copy (pull) [linux, macos]
- [T1071 Standard Application Layer Protocol](#)
 - Atomic Test #2: Malicious User Agents - Nix [linux, macos]
- T1032 Standard Cryptographic Protocol [CONTRIBUTE A TEST](#)
- T1095 Standard Non-Application Layer Protocol [CONTRIBUTE A TEST](#)
- [T1065 Uncommonly Used Port](#)
 - Atomic Test #2: Testing usage of uncommonly used port [linux, macos]
- T1102 Web Service [CONTRIBUTE A TEST](#)

initial-access

- T1189 Drive-by Compromise [CONTRIBUTE A TEST](#)

- T1190 Exploit Public-Facing Application [CONTRIBUTE A TEST](#)
- T1200 Hardware Additions [CONTRIBUTE A TEST](#)
- [T1193 Spearphishing Attachment](#)
- T1192 Spearphishing Link [CONTRIBUTE A TEST](#)
- T1194 Spearphishing via Service [CONTRIBUTE A TEST](#)
- T1195 Supply Chain Compromise [CONTRIBUTE A TEST](#)
- T1199 Trusted Relationship [CONTRIBUTE A TEST](#)
- T1078 Valid Accounts [CONTRIBUTE A TEST](#)

privilege-escalation

- T1068 Exploitation for Privilege Escalation [CONTRIBUTE A TEST](#)
- [T1055 Process Injection](#)
 - Atomic Test #3: Shared Library Injection via /etc/ld.so.preload [linux]
- [T1166 Setuid and Setgid](#)
 - Atomic Test #1: Setuid and Setgid [macos, centos, ubuntu, linux]
 - Atomic Test #2: Set a SetUID flag on file [macos, centos, ubuntu, linux]
 - Atomic Test #3: Set a SetGID flag on file [macos, centos, ubuntu, linux]
- [T1169 Sudo](#)
 - Atomic Test #1: Sudo usage [macos, linux]
- [T1206 Sudo Caching](#)
 - Atomic Test #1: Unlimited sudo cache timeout [macos, linux]
 - Atomic Test #2: Disable tty_tickets for sudo caching [macos, linux]
- T1078 Valid Accounts [CONTRIBUTE A TEST](#)

- [T1100 Web Shell](#)

