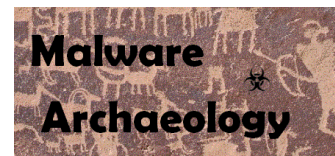


This “**Windows ATT&CK Logging Cheat Sheet**” is intended to help you map the tactics and techniques of the Mitre ATT&CK framework to Windows audit log event IDs in order to know what to collect and harvest, and also what you could hunt for using Windows logging Event IDs.



Sponsored by:



DEFINITIONS:

TACTICS: The eleven (11) focus ATT&CK tactic areas that all techniques are mapped to.

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

TECHNIQUE: The next level of detail that maps the type of item that is misused by the attacker and should be monitored.




TECHNIQUE ID: The Mitre Technique ID used to get more details of the attackers technique and how to defend, detect or hunt for the details. Visit the link below

DATA SOURCES: The detail of what to monitor for, in this case the log event IDs.

RESOURCES: Places to get more information

- Adversarial Tactics, Techniques & Common Knowledge (**ATT&CK**) Framework
 - <https://attack.mitre.org>
- [MalwareArchaeology.com/cheat-sheets](https://www.malwarearchaeology.com/cheat-sheets) for more Windows cheat sheets
- **Log-MD.com** – The **Log Malicious Discovery** tool reads security related log events and settings. Use **Log-MD** to audit your log settings compared to the “**Windows Logging Cheat Sheet**” and Center for Internet Security (CIS) Benchmarks. It is a standalone tool to help those with and without a log management solution find malicious activity.
 -
- Google! – But of course

LEGEND:

-  Coverage of this technique is good.
-  Coverage of this technique is not complete.
-  There is no coverage of this technique.

SETTING AND MEASURING AUDIT LOGGING:

To what to set and the options of Windows logging, refer to the “Windows Logging Cheat Sheet(s)” available at:

- <https://www.malwarearchaeology.com/cheat-sheets/>

To measure the compliance of settings against many industry audit policy standards, use LOG-MD available at:

- <https://www.log-md.com/compare/>

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

TACTIC: COLLECTION

Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.

Tactic	Technique Name	Technique ID	Data Source 1	Data Source 2	Data Source 3	Data Source 4	Data Source 5	Data Source 6	Data Source 7	Data Source 8	Data Source 9	Data Source 10	Data Source 11
Collection	Audio Capture	T1123	4688 Process Execution	4663 File monitoring	API monitoring								
Collection	Automated Collection	T1119	4688 Process CMD Line	4663 File monitoring	Data loss prevention								
Collection	Clipboard Data	T1115	API monitoring										
Collection	Data from Information Repositories	T1213	Application Logs	Authentication logs	Data loss prevention	Third-party application logs							
Collection	Data from Local System	T1005	4688 Process Execution	4688 Process CMD Line	200-500, 4100-4104 PowerShell logs	4663 File monitoring	5861 WMI						
Collection	Data from Network Shared Drive	T1039	4688 Process CMD Line	4688 Process Execution	5140/5145 Share connection	4663 File monitoring							
Collection	Data from Removable Media	T1025	4688 Process Execution	4688 Process CMD Line	4657 Windows Registry	4663 File monitoring	5140/5145 Net Shares						
Collection	Data Staged	T1074	4688 Process CMD Line	4688 Process Execution	4663 File monitoring								
Collection	Email Collection	T1114	4688 Process Execution	5156 Firewall Logs	4624 Authentication logs	4663 File monitoring							
Collection	Man in the Browser	T1185	4624 Authentication logs	4688 Process Execution	API monitoring	Packet capture							
Collection	Screen Capture	T1113	4688 Process Execution	4663 File monitoring	API monitoring								

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Collection	Video Capture	T1125	4688 Process Execution	4663 File monitoring	API monitoring									
Collection,Credential Access	Input Capture	T1056	4657 Windows Registry	4688 Process Execution	Kernel drivers	API monitoring								
Command and Control	Commonly Used Port	T1043	5156 Windows Firewall	4688 Process Execution	Packet capture	Netflow/Enclave netflow								
Command and Control	Communication Through Removable Media	T1092	4657 Registry Monitoring USB Keys	4663 File monitoring	Data loss prevention									
Command and Control	Connection Proxy	T1090	5156 Windows Firewall	4688 Process Execution	Netflow/Enclave netflow	Packet capture								
Command and Control	Custom Command and Control Protocol	T1094	5156 Windows Firewall	4688 Process Execution	Packet capture	Netflow/Enclave netflow								
Command and Control	Custom Cryptographic Protocol	T1024	4688 Process Execution	4688 Process CMD Line	5156 Windows Firewall	Packet capture	Netflow/Enclave netflow	Malware reverse engineering						
Command and Control	Data Encoding	T1132	5156 Windows Firewall	4688 Process Execution	Packet capture	Network protocol analysis								
Command and Control	Data Obfuscation	T1001	4688 Process Execution	5156 Windows Firewall	FW Logs	Network protocol analysis	Packet capture							
Command and Control	Domain Fronting	T1172	SSL/TLS inspection	Packet capture										
Command and Control	Fallback Channels	T1008	4688 Process Execution	5156 Windows Firewall	Malware reverse engineering	Netflow/Enclave netflow	Packet capture							
Command and Control	Multiband Communication	T1026	4688 Process Execution	4688 Process CMD Line	5156 Windows Firewall	Malware reverse engineering	Packet capture	Netflow/Enclave netflow						
Command and Control	Multi-hop Proxy	T1188	Network protocol analysis	Netflow/Enclave netflow										
Command and Control	Multilayer Encryption	T1079	5156 Windows Firewall	4688 Process Execution	Malware reverse engineering	Packet capture								

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Command and Control	Multi-Stage Channels	T1104	5156 Windows Firewall	Network device logs	Network protocol analysis	Packet capture	Netflow/Enclave netflow							
Command and Control	Remote Access Tools	T1219	5156 Windows Firewall	4688 Process Execution	Network intrusion detection system	Network protocol analysis								
Command and Control	Standard Application Layer Protocol	T1071	5156 Windows Firewall	4688 Process Execution	Network intrusion detection system	Network protocol analysis								
Command and Control	Standard Cryptographic Protocol	T1032	5156 Windows Firewall	4688 Process Execution	Malware reverse engineering	SSL/TLS inspection	Packet capture	Netflow/Enclave netflow						
Command and Control	Standard Non-Application Layer Protocol	T1095	5156 Windows Firewall	4688 Process Execution	Malware reverse engineering	Packet capture	Netflow/Enclave netflow							
Command and Control	Uncommonly Used Port	T1065	5156 Windows Firewall	4688 Process Execution	Netflow/Enclave netflow									
Command and Control, Defense Evasion	Web Service	T1102	Host network interface	Netflow/Enclave netflow	Network protocol analysis	Packet capture	SSL/TLS inspection							
Command and Control, Lateral Movement	Remote File Copy	T1105	4663 File monitoring	5156 Windows Firewall	4688 Process Execution	Packet capture	Netflow/Enclave netflow	Network protocol analysis						
Credential Access	Account Manipulation	T1098	4624 Authentication logs	Windows event logs	Packet capture	API monitoring								
Credential Access	Brute Force	T1110	4624 Authentication logs											
Credential Access	Credential Dumping	T1003	4688 Process Execution	4688 Process CMD Line	200-500, 4100-4104 PowerShell logs	Other Event IDs	Memory Forensics	API monitoring						
Credential Access	Credentials in Files	T1081	4663 File monitoring	4688 Process CMD Line										
Credential Access	Credentials in Registry	T1214	4657 Windows Registry	4688 Process CMD Line	4688 Process Execution									

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Credential Access	Exploitation for Credential Access	T1212	4624 Authentication logs	4688 Process Execution	1000, 1001 Windows Error Reporting									
Credential Access	Forced Authentication	T1187	5156 Windows Firewall	4663 File monitoring	Network protocol analysis	Network device logs								
Credential Access	Kerberoasting	T1208	4769 Windows event logs											
Credential Access	LLMNR/NBT-NS Poisoning	T1171	4657 Windows Registry	5156 Windows Firewall	Packet capture	Netflow/Enclave netflow								
Credential Access	Network Sniffing	T1040	Network device logs	Host network interface	Netflow/Enclave netflow									
Credential Access	Password Filter DLL	T1174	4688 Process Execution	4657 Windows Registry	Sysmon DLL monitoring	Autoruns								
Credential Access	Private Keys	T1145	4657 File monitoring											
Credential Access	Two-Factor Authentication Interception	T1111	MFA											
Credential Access, Persistence, Privilege Escalation	Hooking	T1179	4688 Process Execution	Windows event logs	Sysmon ID 7 DLL monitoring	Sysmon - ID 7 Loaded DLLs	API monitoring	Binary file metadata						
Defense Evasion	Binary Padding	T1009	4688 Process Execution	4688 Process CMD Line	4663 File monitoring	Binary file metadata								
Defense Evasion	Code Signing	T1116	B9 Binary file metadata	LMD - File Hash										
Defense Evasion	DCShadow	T1207	4624 Authentication logs	Network protocol analysis	Packet capture	API monitoring								
Defense Evasion	Deobfuscate/Decode Files or Information	T1140	4688 Process CMD Line	4688 Process Execution	4663 File monitoring									
Defense Evasion	Disabling Security Tools	T1089	4688 Process CMD Line	4689 Process Term	4657 Windows Registry	4663 File monitoring	7040 Service Changed	API monitoring	Anti-virus					

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Defense Evasion	DLL Side-Loading	T1073	5156 Windows Firewall	4688 Process Execution	Sysmon - ID 7 Loaded DLLs									
Defense Evasion	Exploitation for Defense Evasion	T1211	4688 Process Execution	4663 File monitoring	1000,1001 Windows Error Reporting									
Defense Evasion	File Deletion	T1107	4688 Process CMD Line	4663 File monitoring	B9 Binary file metadata									
Defense Evasion	File System Logical Offsets	T1006	4688 Process Execution	4688 Process CMD Line	200-500, 4100- 4104 PowerShell logs	4663 File monitoring	API monitoring							
Defense Evasion	Indicator Blocking	T1054	4688 Process CMD Line	4688	Sensor health and status									
Defense Evasion	Indicator Removal from Tools	T1066	4688 Process CMD Line	4688 Process Execution	5156 Windows Firewall	Anti-virus	B9 Binary file metadata							
Defense Evasion	Indicator Removal on Host	T1070	4663 File monitoring	4688 Process CMD Line	4688 Process Execution									
Defense Evasion	Indirect Command Execution	T1202	4688 Process CMD Line	4688 Process Execution	Windows event logs	ID 1 & 7 Sysmon								
Defense Evasion	Install Root Certificate	T1130	4657 Reg Audit	SSL/TLS inspection	Digital Certificate Logs									
Defense Evasion	Masquerading	T1036	4688 Process Execution	4663 File monitoring	File Hashing	B9 Binary file metadata								
Defense Evasion	Modify Registry	T1112	4657 Windows Registry	4663 File monitoring	4688 Process Execution	4688 Process CMD Line	LMD Reg Compare							
Defense Evasion	Network Share Connection Removal	T1126	4688 Process Execution	4688 Process CMD Line	5140/5145 Net Shares	4624 Authentication logs	Packet capture							
Defense Evasion	NTFS File Attributes	T1096	4663 File monitoring	Kernel drivers	API monitoring	LMD EA, ADS Hash Compare								

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Defense Evasion	Obfuscated Files or Information	T1027	5156 Windows Firewall	4688 Process CMD Line	Windows event logs	4663 - File Auditing File monitoring	B9 Binary file metadata	Malware reverse engineering	Environment variable	Network protocol analysis	Network intrusion detection system	Email gateway	SSL/TLS inspection
Defense Evasion	Process Doppelg?nging	T1186	4688 Process Execution	API monitoring									
Defense Evasion	Process Hollowing	T1093	4688 Process Execution	LMD - B9	API monitoring								
Defense Evasion	Rootkit	T1014	4688 Process Execution	LOG-MD AutoRuns	LOG-MD Windows Registry Compare	LOG-MD File Hash Compare	BIOS	MBR	System calls				
Defense Evasion	Software Packing	T1045	LOG-MD - B9 Binary file metadata										
Defense Evasion	Timestomp	T1099	4688 Process CMD Line	4688 Process Execution	4663 File monitoring								
Defense Evasion,Execution	CMSTP	T1191	4688 Process Execution	4688 Process CMD Line									
Defense Evasion,Execution	Control Panel Items	T1196	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	Windows event logs	API monitoring	Binary file metadata	DLL monitoring				
Defense Evasion,Execution	InstallUtil	T1118	4688 Process Execution	4688 Process CMD Line	ID 1 & 7 Sysmon								
Defense Evasion,Execution	Mshhta	T1170	4688 Process Execution	4688 Process CMD Line	ID 1 & 7 Sysmon								
Defense Evasion,Execution	Regsvcs/Regasm	T1121	4688 Process Execution	4688 Process CMD Line	ID 1 & 7 Sysmon								
Defense Evasion,Execution	Regsvr32	T1117	4688 Process CMD Line	4688 Process Execution	ID - 7 Sysmon Loaded DLLs	4657 Windows Registry							
Defense Evasion,Execution	Rundll32	T1085	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	Binary file metadata							

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Defense Evasion,Execution	Scripting	T1064	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	LMD - Hash Compare								
Defense Evasion,Execution	Signed Binary Proxy Execution	T1218	4688 Process Execution	4688 Process CMD Line										
Defense Evasion,Execution	Signed Script Proxy Execution	T1216	4688 Process Execution	4688 Process CMD Line										
Defense Evasion,Execution	Trusted Developer Utilities	T1127	4688 Process Execution	4688 Process CMD Line										
Defense Evasion,Persistence	BITS Jobs	T1197	BITS Logs Windows event logs	4688 Process CMD Line	API monitoring	Packet capture								
Defense Evasion,Persistence	Component Firmware	T1109	4688 Process CMD Line	4663 File Monitoring										
Defense Evasion,Persistence	Component Object Model Hijacking	T1122	4688 Process CMD Line	DLL monitoring	Loaded DLLs	LOG-MD Windows Registry Compare								
Defense Evasion,Persistence	Hidden Files and Directories	T1158	4663 File monitoring	4688 Process Execution	4688 Process CMD Line	LMD Hash Compae								
Defense Evasion,Persistence	Redundant Access	T1108	4688 Process Execution	5156 Windows Firewall	4663 File monitoring	Login - 4624 Auth Logs	LMD - B9 Binary file metadata	Network protocol analysis	Packet capture					
Defense Evasion,Persistence	SIP and Trust Provider Hijacking	T1198	4688 Process Execution	4657 Windows Registry	Windows event logs	Loaded DLLs	DLL monitoring	API monitoring	Application Logs					
Defense Evasion,Persistence,Privilege Escalation	DLL Search Order Hijacking	T1038	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	Sysmon - ID 7 DLL monitoring								
Defense Evasion,Persistence,Privilege Escalation	Image File Execution Options Injection	T1183	4688 Process Execution	4657 Windows Registry	Windows event logs	LMD - Autoruns								
Defense Evasion,Persistence,Privilege Escalation,Initial Access	Valid Accounts	T1078	4624 Authentication logs	4688 Process Execution										

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Defense Evasion,Privilege Escalation	Access Token Manipulation	T1134	4688 Process CMD Line	API monitoring	Access Tokens									
Defense Evasion,Privilege Escalation	Bypass User Account Control	T1088	4688 Process Execution	4688 Process CMD Line	4624 Authentication logs	System calls								
Defense Evasion,Privilege Escalation	Extra Window Memory Injection	T1181												
Defense Evasion,Privilege Escalation	Process Injection	T1055	4657 Windows Registry	4663 File monitoring	4688 Process Execution	DLL monitoring	Named Pipes	API monitoring						
Discovery	Account Discovery	T1087	4688 Process CMD Line	4688 Process Execution	API monitoring									
Discovery	Application Window Discovery	T1010	4688 Process Execution	4688 Process CMD Line	API monitoring									
Discovery	Browser Bookmark Discovery	T1217	4663 File monitoring	4688 Process CMD Line	4688 Process Execution	API monitoring								
Discovery	File and Directory Discovery	T1083	4663 File monitoring	4688 Process CMD Line	4688 Process Execution									
Discovery	Network Service Scanning	T1046	4688 Process CMD Line	5156 Windows Firewall	Netflow/Encla ve netflow	Network protocol analysis	Packet capture							
Discovery	Network Share Discovery	T1135	4688 Process Execution	4688 Process CMD Line	5156 Windows Firewall	5140/5145 Net Shares	Network protocol analysis							
Discovery	Password Policy Discovery	T1201	4688 Process CMD Line	4688 Process Execution										
Discovery	Peripheral Device Discovery	T1120	4688 Process CMD Line	4688 Process Execution										
Discovery	Permission Groups Discovery	T1069	4688 Process CMD Line	4688 Process Execution	API monitoring									
Discovery	Process Discovery	T1057	4688 Process CMD Line	4688 Process Execution										
Discovery	Query Registry	T1012	4688 Process Execution	4688 Process CMD Line	Windows Registry									

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Discovery	Remote System Discovery	T1018	4688 Process Execution	4688 Process CMD Line	5156 Win Firewall	Network protocol analysis								
Discovery	Security Software Discovery	T1063	4663 File monitoring	4688 Process CMD Line	4688 Process Execution									
Discovery	System Information Discovery	T1082	4688 Process CMD Line	4688 Process Execution										
Discovery	System Network Configuration Discovery	T1016	4688 Process Execution	4688 Process CMD Line	200-500, 4100-4104 PowerShell	5861 WMI								
Discovery	System Network Connections Discovery	T1049	4688 Process CMD Line	4688 Process Execution										
Discovery	System Owner/User Discovery	T1033	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	PowerShell	4624 WMI Auth							
Discovery	System Service Discovery	T1007	4688 Process Execution	4688 Process CMD Line	5861 WMI									
Discovery	System Time Discovery	T1124	4688 Process Execution	4688 Process CMD Line	API monitoring									
Execution	Command-Line Interface	T1059	4688 Process CMD Line	4688 Process Execution										
Execution	Dynamic Data Exchange	T1173	4688 Process Execution	4657 Windows Registry	Windows event logs	DLL monitoring	API monitoring							
Execution	Execution through API	T1106	4688 Process Execution	API monitoring										
Execution	Execution through Module Load	T1129	4688 Process Execution	4663 File monitoring	DLL monitoring	API monitoring								
Execution	Exploitation for Client Execution	T1203	4688 Process Execution	5156 Windows Firewall	Anti-virus	System calls								
Execution	Graphical User Interface	T1061	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	B9 Binary file metadata								
Execution	PowerShell	T1086	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	4663 File monitoring								

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Execution	Service Execution	T1035	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	7045 New Service	7040 Service Change							
Execution	User Execution	T1204	4688 Process CMD Line	4688 Process Execution	Anti-virus									
Execution	Windows Management Instrumentation	T1047	4688 Process CMD Line	4688 Process Execution	4624 Authentication logs	Netflow/Enclave netflow								
Execution,Lateral Movement	Third-party Software	T1072	4688 Process Execution	5156 Windows Firewall	4663 File monitoring	4657 Windows Registry	Binary file metadata	Third-party application logs						
Execution,Lateral Movement	Windows Remote Management	T1028	4688 Process CMD Line	4688 Process Execution	5156 Windows Firewall	5140/5145 Net Shares	4663 File monitoring	4624 Authentication logs	Netflow/Encla ve netflow					
Execution,Persistence	LSASS Driver	T1177	4688 Process Execution	4663 File monitoring	DLL monitoring	Loaded DLLs	Sysmon - ID 6 Kernel drivers	API monitoring						
Execution,Persistence,Privileg e Escalation	Scheduled Task	T1053	4688 Process CMD Line	4688 Process Execution	4663 File monitoring	Windows event logs								
Exfiltration	Automated Exfiltration	T1020	4688 Process Execution	4688 Process CMD Line	5156 Windows Firewall	4663 File monitoring								
Exfiltration	Data Compressed	T1002	4688 Process Execution	4688 Process CMD Line	4663 File Monitoring	5156 Windows Firewall	IDS/IPS	DLP	Binary file metadata					
Exfiltration	Data Encrypted	T1022	4688 Process Execution	4688 Process CMD Line	4663 File monitoring	Binary file metadata	IDS/IPS	DLP	Network protocol analysis					
Exfiltration	Data Transfer Size Limits	T1030	5156 Windows Firewall	4688 Process Execution	Packet capture	Netflow/Enclave netflow								
Exfiltration	Exfiltration Over Alternative Protocol	T1048	4688 Process Execution	5156 Windows Firewall	Packet capture	Netflow/Enclave netflow	Network protocol analysis	User interface						
Exfiltration	Exfiltration Over Command and Control Channel	T1041	4688 Process Execution	5156 Windows Firewall	LMD - SRUM	User interface								
Exfiltration	Exfiltration Over Other Network Medium	T1011	4688 Process Execution	4688 Process CMD Line	5156 Windows Firewall	User interface								

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Exfiltration	Exfiltration Over Physical Medium	T1052	4657 Registry - USB Keys	219, 441 Registry - USB/PnP IDs	Data loss prevention	File monitoring								
Exfiltration	Scheduled Transfer	T1029	5156 Windows Firewall	4688 Process Execution	100-200 Scheduled Tasks	Netflow/Enclave netflow								
Initial Access	Drive-by Compromise	T1189	4688 Process Execution	5156 Windows Firewall	Web proxy	Network intrusion detection system	SSL/TLS inspection	Packet capture	Network device logs					
Initial Access	Exploit Public-Facing Application	T1190	Application logs	Packet capture	Web logs	Web application firewall logs								
Initial Access	Hardware Additions	T1200	Asset Management	Data loss prevention										
Initial Access	Spearphishing Attachment	T1193	4688 Process Execution	4663 File monitoring	Packet capture	Mail server	Network intrusion detection system	Detonation chamber	Email gateway					
Initial Access	Spearphishing Link	T1192	Packet capture	Web proxy	Email gateway	Detonation chamber	SSL/TLS inspection	DNS records	Mail server					
Initial Access	Spearphishing via Service	T1194	SSL/TLS inspection	Anti-virus	Web proxy									
Initial Access	Supply Chain Compromise	T1195	4663 File monitoring	Web proxy										
Initial Access	Trusted Relationship	T1199	Application Logs	Authentication logs	Third-party application logs									
Lateral Movement	Application Deployment Software	T1017	4688 Process Execution	4688 Process CMD Line	5156 Windows Firewall	4663 File monitoring								
Lateral Movement	Distributed Component Object Model	T1175	4688 Process Execution	4657 Windows Registry	Authentication logs	Windows event logs	DLL monitoring	API monitoring	Packet capture					
Lateral Movement	Exploitation of Remote Services	T1210	4688 Process Execution	4663 File monitoring	1000, 1001 Windows Error Reporting									
Lateral Movement	Pass the Hash	T1075	4624 Authentication logs											

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Lateral Movement	Pass the Ticket	T1097	4624 Authenticati on logs											
Lateral Movement	Remote Desktop Protocol	T1076	4688 Process Execution	4624 Authentication logs	Netflow/Enclave netflow									
Lateral Movement	Remote Services	T1021	4624, 4625 Authenticati on logs	21, 23, 25, 41 RDP Logs										
Lateral Movement	Shared Webroot	T1051	4663 File monitoring	4688 Process Execution										
Lateral Movement	Taint Shared Content	T1080	4663 File monitoring	4688 Process Execution										
Lateral Movement	Windows Admin Shares	T1077	5156 Windows Firewall	4624 Authentication logs	4688 Process CMD Line	4688 Process Execution								
Lateral Movement, Credential Access, Initial Access	Replication Through Removable Media	T1091	219, 421, 4657 USB/PnP - IDs	4657 Windows Registry	4663 File monitoring	Data loss prevention								
Lateral Movement, Persistence	Logon Scripts	T1037	4688 Process Execution	4663 File monitoring										
Persistence	Authentication Package	T1131	4657 Windows Registry	Loaded DLLs	DLL monitoring									
Persistence	Bootkit	T1067	API monitoring	MBR	VBR									
Persistence	Browser Extensions	T1176	5156 Windows Firewall	4688 Process Execution	File Audit - 4663	Network protocol analysis	Packet capture	System calls	Browser extensions					
Persistence	Change Default File Association	T1042	4657 Windows Registry	4688 Process CMD Line	4688 Process Execution									
Persistence	Create Account	T1136	4688 Process Execution	4688 Process CMD Line	4624 Authentication logs	Windows event logs								
Persistence	External Remote Services	T1133	4624 Authenticati on logs											
Persistence	Hypervisor	T1062	System calls											

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Persistence	Modify Existing Service	T1031	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	4663 File monitoring	7040 Service Change							
Persistence	Netsh Helper DLL	T1128	4688 Process Execution	4657 Windows Registry	DLL monitoring									
Persistence	Office Application Startup	T1137	4688 Process Execution	4688 Process CMD Line	4657 Windows Registry	4663 File monitoring								
Persistence	Registry Run Keys / Start Folder	T1060	4657 Windows Registry	4663 File monitoring										
Persistence	Screensaver	T1180	4688 Process Execution	4688 Process CMD Line	4657 Windows Registry	4663 File monitoring								
Persistence	Security Support Provider	T1101	4657 Windows Registry	Loaded DLLs	DLL monitoring									
Persistence	Shortcut Modification	T1023	4688 Process Execution	4688 Process CMD Line	4663 File monitoring									
Persistence	System Firmware	T1019	BIOS	EFI	API monitoring									
Persistence	Time Providers	T1209	4688 Process Execution	4663 File monitoring	DLL monitoring	Loaded DLLs	API monitoring	Binary file metadata						
Persistence	Windows Management Instrumentation Event Subscription	T1084	5861 WMI Objects											
Persistence	Winlogon Helper DLL	T1004	4688 Process Execution	4657 Windows Registry	4663 File monitoring	LOG-MD Hash Compare	AutoRuns							
Persistence,Privilege Escalation	Accessibility Features	T1015	4688 Process Execution	4657 Windows Registry	4663 File monitoring	AutoRuns								
Persistence,Privilege Escalation	AppCert DLLs	T1182	4688 Process Execution	4657 Windows Registry	Loaded DLLs									
Persistence,Privilege Escalation	AppInit DLLs	T1103	4688 Process Execution	4657 Windows Registry	Loaded DLLs									

WINDOWS ATT&CK LOGGING CHEAT SHEET - Win 7 - Win 2012

Persistence,Privilege Escalation	Application Shimming	T1138	4688 Process CMD Line	4688 Process Execution	4657 Windows Registry	Loaded DLLs	System calls							
Persistence,Privilege Escalation	File System Permissions Weakness	T1044	4663 File monitoring	4688 Process CMD Line	7040, 7045 Services									
Persistence,Privilege Escalation	New Service	T1050	4657 Windows Registry	4688 Process Execution	4688 Process CMD Line									
Persistence,Privilege Escalation	Path Interception	T1034	4688 Process Execution	4663 File monitoring	8000-8027, 866 Whitelist Failures									
Persistence,Privilege Escalation	Port Monitors	T1013	4688 Process Execution	4657 Windows Registry	4663 File monitoring	AutoRuns	DLL monitoring	API monitoring						
Persistence,Privilege Escalation	Service Registry Permissions Weakness	T1058	4688 Process CMD Line	7040, 7045 Services	4657 Windows Registry									
Persistence,Privilege Escalation	Web Shell	T1100	4688 Process Execution	4663 File monitoring	4624, 4625 Authentication logs	Netflow/Enclave netflow	Anti-virus							
Privilege Escalation	Exploitation for Privilege Escalation	T1068	1000, 1001 Windows Error Reporting	4688 Process Execution	Application Logs									
Privilege Escalation	SID-History Injection	T1178	4624, 4625 Authentication logs	Windows event logs	API monitoring									