APT REREFENCE INDEX

CONTENTS

DEFENSIVE ORIGINS

Defensive Origins: https://www.defensiveorigins.com

ENTERPRISE RECONNAISSANCE

AutoReconSPF: https://github.com/Relkci/AutoSPFRecon
BeenVerified: https://www.beenverified.com
Canary Tokens: https://canarytokens.org/
Facebook: https://www.facebook.com
GitHub: https://www.github.com
Glassdoor: https://www.glassdoor.com
Google: https://www.google.co
Grayhat Warefare Buckets: https://buckets.grayhatwarfare.com/
HackerTarget: https://www.hackertarget.com
Have I been Pwned?L https://haveibeenpwned.com/
LinkedIn: https://www.linkedin.com
Mate: https://www.sslmate.com
Mimecast DMARC Analyzer: https://www.mimecast.com/products/dmarc-analyzer/
Monster.com: https://www.monster.com
MXToolBox: https://www.mxtoolbox.com
PasteBin: https://www.pastebin.com
PowerMeta: https://github.com/dafthack/PowerMeta
Shodan.io: https://www.shodan.io
SSL Hunter.io: https://www.hunter.io
URLCrazy: https://tools.kali.org/information-gathering/urlcrazy

DEFENSE, SECURITY

Canary Tokens: https://canarytokens.org/
Deny Access to This Computer from The Network: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/denyaccess-to-this-computer-from-the-network
Enable SMB Signing Requirements via Group Policy: https://www.blackhillsinfosec.com/an-smb-relay-race-how-to-exploit-llmnr-and-smb-messagesigning-for-fun-and-profit/
How to Disable LLMNR and Why You Want To: https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/
How to Enable SMB Signing in Windows NT: https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt
MITRE ATT&CK Framework: https://attack.mitre.org/techniques/enterprise/
Security Baseline Update for Windows 10-1903: https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-sept2019update-for-windows-10-v1903-and/ba-p/890940

ATTACK TOOLS, METHODS

Active Directory Explorer v1.44: https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer
ADEnumerator: https://github.com/chango77747/AdEnumerator
Atomic Red Team: https://github.com/redcanaryco/atomic-red-team
Atomic Red Team: https://github.com/redcanaryco/atomic-red-team
BloodHoundAD: https://github.com/BloodHoundAD
Cheatsheets: https://www.malwarearchaeology.com/cheat-sheets
Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/
CrackMapExec: https://github.com/byt3bl33d3r/CrackMapExec

Domain Password Spray: https://github.com/dafthack/DomainPasswordSpray
Empire: https://github.com/EmpireProject/Empire
How to Permanently Disable Windows Defender Antivirus https://www.windowscentral.com/how-permanently-disable-windows-defender-antivirus-windows-10
Impacket: https://github.com/SecureAuthCorp/impacket
Installutil.exe: https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool
Inveigh: https://github.com/Kevin-Robertson/Inveigh
John the Ripper: https://www.openwall.com/john/
MailSniper: https://github.com/dafthack/MailSniper
Metasploit: https://www.metasploit.com/
MITRE ATT&CK Framework: https://attack.mitre.org/techniques/enterprise/
MSBuild: https://docs.microsoft.com/en-us/visualstudio/msbuild/msbuild?view=vs-2019
Msiexec: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec
PowerSploit: https://github.com/PowerShellMafia/PowerSploit
PowerUp: https://github.com/HarmJ0y/PowerUp
PowerView: https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon
Python Development Workflow for Humans: https://github.com/pypa/pipenv
Regsvr32: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/regsvr32
Responder: https://github.com/SpiderLabs/Responder
Silent Trinity: https://github.com/byt3bl33d3r/SILENTTRINITY
UACMe: https://github.com/hfiref0x/UACME

GOVERNANCE AND COMPLIANCE

ARIN: https://www.arin.net/
HIPAA -H ITECH Act: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
ICANN: https://www.icann.org/
NIIST CyberSecurity: https://www.nist.gov/topics/cybersecurity
NIST Red Team / Blue Team Approach: https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach
Sarbanes-Oxley Act (SOX): https://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

OPTICS, INFRASTRUCTURE, LOGGING

Advanced Security Audit Policy Settings: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
Amazon AWS: https://aws.amazon.com/
AWS Acceptable Use Policy: https://aws.amazon.com/aup/
Collect Parse Transform and Stream Windows Event Logs and Metrics using Amazon Kinesis Agent for Microsoft Windows: https://aws.amazon.com/blogs/big-data/collect-parse-transform-and-stream-windows-events-logs-and-metrics-using-amazon-kinesis-agent-for-microsoft-windows/
Command Line Process Auditing: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
Detecting Bloodhound: http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html
Detecting Kerberoasting Activity: https://adsecurity.org/?p=3458
Directory Source to S3 Tutorial: https://docs.aws.amazon.com/kinesis-agent-windows/latest/userguide/directory-source-to-s3-tutorial.html
ELasticSearch: https://www.elastic.co/
Event Forwarding Guidance: https://github.com/nsacyber/Event-Forwarding-Guidance
Event Forwarding Guidance: https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6
FileBeatL https://www.elastic.co/beats/filebeat
HELK: https://github.com/Cyb3rWard0g/HELK
Kibana: https://www.elastic.co/kibana
LogStash: https://www.elastic.co/products/logstash
PFSense: https://www.pfsense.org/
Python Development Workflow for Humans: https://github.com/pypa/pipenv
Sigma integration via Elastalert: https://posts.specterops.io/what-the-helk-sigma-integration-via-elastalert-6edf1715b02
SwiftOnSecurity sysmon-config: https://github.com/SwiftOnSecurity/sysmon-config
Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
Sysmon: https://github.com/MotiBa/Sysmon/
Sysmon-Modular: https://github.com/olafhartong/sysmon-modular
Use Windows Event Forwarding to Assist in Intrusion Detection: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
Windows Event Forwarding Survival Guide: https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx
WinLogBeat: https://www.elastic.co/beats/winlogbeat
WLK Log Monitoring: https://www.elastic.co/log-monitoring
WMIOps: https://github.com/FortyNorthSecurity/WMIOps

CONFERENCES

WildWestHackinFest: https://www.wildwesthackinfest.com/
KernelCon: https://kernelcon.org/