Introduction to common

Red Team Attacks & Blue Team Defenses

Brought to you by

NETSPI™

Common Red Team Attack Vectors and Techniques

Common Attack Kill Chain

Common Blue Team Detective and Preventative Controls

RED TEAM

BLUE TEAM

Common Variations		Endpoint	Network	Process
Find Emails & Users LinkedIn.com Data.com Google.com Bing.com **Verify Emails & Users** SMTP Server Cmds Send Test Emails HTTP with NTLM Office365 OWA MS APIs **Create Phishing Payloads & Sites** Create Content-Filter Exceptions Buy Expired Domains	**Prepare Phishing Attacks** from public resources	NA	Deny / log VRY requests Deny / log EXPN requests Log RCPT commands executed sequentially Large numbers of HTTP NTLM requests	User awareness training Track company's point of presence and employee exposure. Monitor domain expirations
Email Sources Spoofed Internal Domain Spoofed External Domain Domain Similar to Company Hacked Account **Email Targets** Mass Mailing Targeted Mailing **Email Content** Pretext Scenario Malicious Links Malicious Files & Embedding	**Send Phishing Emails** to employee addresses	NA	Email filters, thresholds, and spam rules Email source verification Blacklist checks SPF record checks Logs / SEIM / Alerts	User awareness training Incident response procedures
Malicious Links Port Scan Geo Locate Phish Web Site **Website Components** Credential Collection Form Java Applet ClickOnce HTA Brower Exploit Browser Add-On Exploit **Files** Common exec file formats Office Docs + Macros	**Deliver the Payloads** to employee systems	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy Mail client configurations MS Office Security Settings Web browser configurations Logs / SEIM / Alerts	Email filters, thresholds, and spam rules Deny / log relay requests Secure caching provider Web filtering / white listing Authenticated HTTP proxies Logs / SEIM / Alerts	User awareness training Incident response procedures
Common Payload Command Types **Commands** cmd, wmi, wrm, ftp, net, etc **Binaries** Executable, Installer, Library **Scripts** PS, VB, VBS, JS, Bat **Standard Code** C, C++, C# **Assembly Code** shellcode **Byte Code** Java, .Net	**Run the Payload Commands** on employee systems	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts	NA	User awareness training Incident response procedures
Common Local Persistence Methods PW / Pvt Key PW Hash Kerb Ticket Custom Providers File, Registry, & Application Autoruns Windows Service Scheduled Task WMI Event Trigger Code / File Modification Driver BIOS	**Maintain Local Persistence** on employee systems	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts FIM / WMI event triggers	NA	User awareness training Incident response procedures
Egress Ports TCP UDP IPv4 IPv6 **Common Protocols** HTTP HTTPS DNS ICMP NTP SSH Telnet Rlogin FTP NFS SMB Torrent IM SMTP **Common Types** Beacon Bind Shell Reverse Shell Web Shell	**Obtain Command & Control Channel** from employee systems	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts	Firewall Rules / Segmentation NIDs / NIPs Fix Up Protocols Web Filtering / White Listing Authenticated HTTP Proxies Logs / SEIM / Alerts	User awareness training Incident response procedures
Weak Configurations Weak Password or Password Storage Method Insecure Service Insecure Schtask Insecure GPO Insecure Protocol Excessive Privilege **Local Exploits** OS APP	**Escalate Local Privileges** on employee systems	Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts DEP / ASLR / SEH Micro virtualizing / sandboxes	Logs / SEIM / Alerts	Admin awareness training Incident response procedures
Steal Authentication Tokens Password / Private Key Password Hash (PTH) Kerberos Ticket (PTT) **Common local Targets** OS, Domain, & Network Information Users & Groups Cache & Logs Services & Processes Installed Apps Files & Registry	**Perform Local Recon / Discovery** on employee systems	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts	Logs / SEIM / Alerts	Admin awareness training Incident response procedures
Passive Recon Sniffing **Active Discovery** Trace Route Ping & Port Scanning DNS & ADS Queries Share & Logon Scanning DB, SP & Mail Svr Scanning **Locate Domain, Ent. & Forest Admins** Domain GPOs & SPN Remote Sessions & Processes	**Perform Network Recon / Discovery** on internal networks	HIDs / HIPs Logs / SEIM / Alerts Canaries - Local & Domain User Accounts - Domain Computer Accounts - Local and Network Files File Auditing	Firewall rules / segmentation NIDs / NIPs Honey pots Tarpits Canary networks, systems, & accounts Logs / SEIM / Alerts	Admin awareness training Incident response procedures
Stolen Authentication Tokens Password / Private Key Password Hash (PTH) Kerberos Ticket (PTT) **Common Methods** MGMT Services Windows Service Sched Task File Share DB, App & VM Servers Remote Exploit, Physical GPO, SCCM	**Perform Lateral Movement** between systems/networks	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts Host-based Firewall	Firewall Rules / Segmentation NIDs / NIPs Honey Pots Tarpits Canary networks, systems, & accounts Logs / SEIM / Alerts	Don't use shared local accounts Use a separate domain user and server admin accounts Maintain secure configs Incident response procedures
Steal Admin Authentication Tokens Password / Private Key Password Hash (PTH) Kerberos Ticket (PTT) **Attack DCs** Exploits, Kerberoast & GPP **Escalate to Root Domain** Shared Password Delegated Privs Nested Groups Domain Trusts & SID History Exploits Kerberoast GPO	**Escalate Domain Privileges** via common vectors	Asset / config / patch mgmt. Anti-virus / HIDs / HIPs Secure group policy settings Application white listing Least privilege enforcement Logs / SEIM / Alerts Host-based Firewall	Firewall Rules / Segmentation NIDs / NIPs Honey Pots Tarpits Canary networks, systems, & accounts Logs / SEIM / Alerts	Don't use shared local accounts Use a separate domain user and server admin accounts Maintain secure configs Incident response procedures
Common Data Stores Mail Servers File Servers Database Servers Code Repositories **Common Data Targets** PII PHI CHD IP & Research Financial Data Insider Trading Info	**Find and Access Sensitive Data** in common data stores	Least Privilege Enforcement Two-Factor Authentication Data Encryption and Secure Key Management File, Application, and Database Auditing Host DLP / Logs / SEIM / Alerts	Firewall Rules / Segmentation NIDs / NIPs Honey Pots Tarpits Canary networks, systems, & accounts Logs / SEIM / Alerts	User awareness training Incident response procedures Manage keys securely Consolidate and isolate sensitive data stores
Common Protocols TCP/UDP, v4/6 LAN & Wireless Common & Uncommon Ports Standard & Custom Protocols C2 and Alternative Channels **Data Handling** Staged & not Staged Large & Small Files Compression Encoding Encryption **Physical Media** USB & SD CD DVD	**Exfiltrate Sensitive Data** using common channels	HIDs / HIPs Host DLP Large file upload detection Mail client/server settings Logs / SEIM / Alerts	Firewall Rules / Segmentation Email Server Configuration Network DLP Fix Up Protocols Web Filtering / Auth Proxy Canary Data Samples Logs / SEIM / Alerts	User awareness training Incident response procedures
Stolen Authentication Tokens Password / Private Key Password Hash (PTH) Kerberos Ticket (PTT) **Two Factor** Private Key Token Seed Skeleton Key **Common Internet Facing Interfaces** VPN RDP SSH VDE Web Shells Office365 Azure AWS Web Based Citrix & TS	**Maintain Remote Access Without a C2** using common interfaces	Enforce Two-factor authentication on all external interfaces Limit Terminal Service, Citrix, and VDE access to specific groups during specific hours Geo / IP limiting	Firewall rules / segmentation NIDs / NIPs Canary networks, systems, applications, and accounts Logged events / SEIM / alerts	Admin awareness training Incident response procedures Enforce strong account policies

Author: Scott Sutherland, NetSPI 2016

Version: 3.2