

Introduction to common

Red Team Attacks & Blue Team Defenses

Brought to you by



Common Red Team Attack Vectors and Techniques

Common Attack Kill Chain

Common Blue Team Detective and Preventative Controls

Common Variations

Find Emails & Users		Verify Emails & Users			Create Phishing Payloads & Sites		
LinkedIn.com Data.com	Google.com Bing.com	SMTP Server Cmds	Send Test Emails	HTTP with NTLM	Office365 OWA MS APIs	Create Content-Filter Exceptions	Buy Expired Domains

Email Sources			Email Targets		Email Content		
Spoofed Internal Domain	Spoofed External Domain	Domain Similar to Company	Hacked Account	Mass Mailing	Targeted Mailing	Pretext Scenario	Malicious Links Malicious Files & Embedding

Malicious Links	Website Components				Files		
Port Scan Geo Locate	Phish Web Site	Credential Collection Form	Java Applet ClickOnce HTA	Brower Exploit	Brower Add-On Exploit	Common exec file formats	Office Docs + Macros

Common Payload Command Types

Commands	Binaries	Scripts	Standard Code	Assembly Code	Byte Code
cmd, wmi, wrm, ftp, net, etc	Executable, Installer, Library	PS, VB, VBS, JS, Bat	C, C++, C#	shellcode	Java, .Net

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
--	------------------	--	-----------------	----------------	-------------------	--------------------------	-------------

Egress Ports		Common Protocols				Common Types	
TCP UDP	IPv4 IPv6	HTTP HTTPS	DNS ICMP NTP	SSH Telnet Rlogin	FTP NFS SMB	Torrent IM SMTP	Beacon Bind Shell Reverse Shell Web Shell

Weak Configurations

Weak Password or Password Storage Method	Insecure Service	Insecure Schtask	Insecure GPO	Insecure Protocol	Excessive Privilege	OS	APP
--	------------------	------------------	--------------	-------------------	---------------------	----	-----

Steal Authentication Tokens	Common local Targets						
Password / Private Key	Password Hash (PTH)	Kerberos Ticket (PTT)	OS, Domain, & Network Information	Users & Groups	Cache & Logs	Services & Processes	Installed Apps Files & Registry

Passive Recon	Active Discovery					Locate Domain, Ent. & Forest Admins	
Sniffing	Trace Route	Ping & Port Scanning	DNS & ADS Queries	Share & Logon Scanning	DB, SP & Mail Svr Scanning	Domain GPOs & SPN	Remote Sessions & Processes

Stolen Authentication Tokens	Common Methods								
Password / Private Key	Password Hash (PTH)	Kerberos Ticket (PTT)	MGMT Services	Windows Service	Sched Task	File Share	DB, App & VM Servers	Remote Exploit, Physical	GPO, SCCM

Steal Admin Authentication Tokens	Attack DCs	Escalate to Root Domain					
Password / Private Key	Password Hash (PTH)	Kerberos Ticket (PTT)	Exploits, Kerberoast & GPP	Shared Password	Delegated Privs Nested Groups	Domain Trusts & SID History	Exploits Kerberoast GPO

Common Data Stores				Common Data Targets			
Mail Servers	File Servers	Database Servers	Code Repositories	PII PHI CHD	IP & Research	Financial Data	Insider Trading Info

Common Protocols TCP/UDP, v4/6				Data Handling			Physical Media
LAN & Wireless	Common & Uncommon Ports	Standard & Custom Protocols	C2 and Alternative Channels	Staged & not Staged	Large & Small Files	Compression Encoding Encryption	USB & SD CD DVD

Stolen Authentication Tokens	Two Factor	Common Internet Facing Interfaces				
Password / Private Key	Password Hash (PTH)	Kerberos Ticket (PTT)	Private Key Token Seed Skeleton Key	VPN	RDP SSH VDE	Web Shells Office365 Azure AWS Web Based Citrix & TS

Prepare Phishing Attacks

from public resources

Send Phishing Emails

to employee addresses

Deliver the Payloads

to employee systems

Run the Payload Commands

on employee systems

Maintain Local Persistence

on employee systems

Obtain Command & Control Channel

from employee systems

Escalate Local Privileges

on employee systems

Perform Local Recon / Discovery

on employee systems

Perform Network Recon / Discovery

on internal networks

Perform Lateral Movement

between systems/networks

Escalate Domain Privileges

via common vectors

Find and Access Sensitive Data

in common data stores

Exfiltrate Sensitive Data

using common channels

Maintain Remote Access Without a C2

using common interfaces

Endpoint

NA

NA

NA

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy
Mail client configurations
MS Office Security Settings
Web browser configurations
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Asset / config / patch mgmt.
Anti-virus / HIDs / HIPs
Secure group policy settings
Application white listing
Least privilege enforcement
Logs / SEIM / Alerts

Network

Deny / log VRY requests
Deny / log EXPN requests
Log RCPT commands executed sequentially
Large numbers of HTTP NTLM requests

Email filters, thresholds, and spam rules
Email source verification
Blacklist checks
SPF record checks
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

NA

NA

NA

NA

Firewall Rules / Segmentation
NIDs / NIPs
Fix Up Protocols
Web Filtering / White Listing
Authenticated HTTP Proxies
Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Logs / SEIM / Alerts

Process

User awareness training
Track company's point of presence and employee exposure.
Monitor domain expirations

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures

User awareness training
Incident response procedures