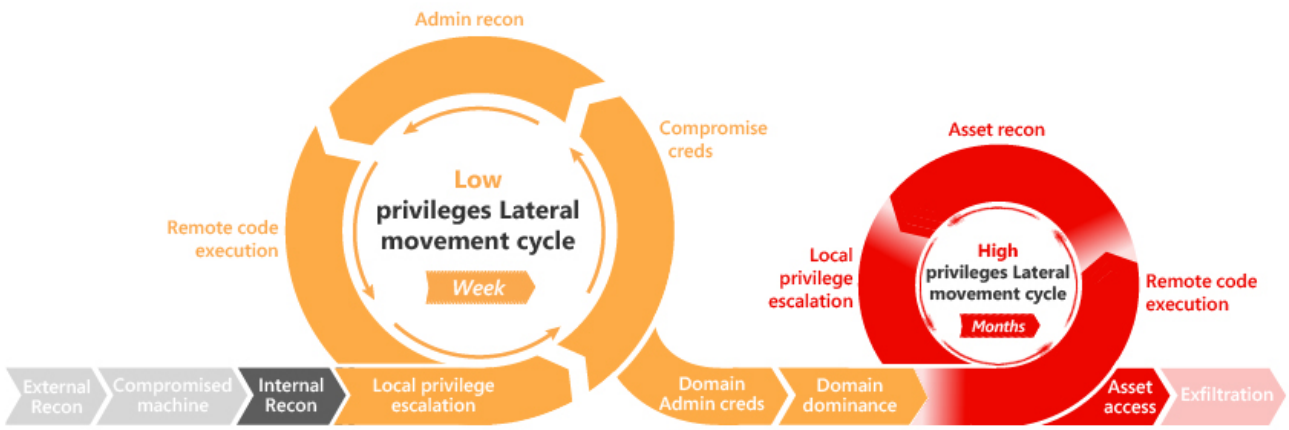
README.md

Active Directory Kill Chain Attack & Defense



Summary

This document was designed to be a useful, informational asset for those looking to understand the specific tactics, techniques, and procedures (TTPs) attackers are leveraging to compromise active directory and guidance to mitigation, detection, and prevention. And understand Active Directory Kill Chain Attack and Modern Post Exploitation Adversary Tradecraft Activity.

Table of Contents

Discovery

SPN Scanning

- SPN Scanning – Service Discovery without Network Port Scanning
- Active Directory: PowerShell script to list all SPNs used
- Discovering Service Accounts Without Using Privileges

Data Mining

- A Data Hunting Overview
- Push it, Push it Real Good
- Finding Sensitive Data on Domain SQL Servers using PowerUpSQL
- Sensitive Data Discovery in Email with MailSniper
- Remotely Searching for Sensitive Files
- I Hunt Sysadmins - harmj0y

User Hunting

- Hidden Administrative Accounts: BloodHound to the Rescue
- Active Directory Recon Without Admin Rights
- Gathering AD Data with the Active Directory PowerShell Module
- Using ActiveDirectory module for Domain Enumeration from PowerShell Constrained Language Mode
- PowerUpSQL Active Directory Recon Functions
- Derivative Local Admin
- Automated Derivative Administrator Search
- Dumping Active Directory Domain Info – with PowerUpSQL!

- Local Group Enumeration
- Attack Mapping With Bloodhound
- Situational Awareness
- Commands for Domain Network Compromise
- A Pentester's Guide to Group Scoping

LAPS

- Microsoft LAPS Security & Active Directory LAPS Configuration Recon
- Running LAPS with PowerView
- RastaMouse LAPS Part 1 & 2

AppLocker

- Enumerating AppLocker Config

Active Directory Federation Services

- 118 Attacking ADFS Endpoints with PowerShell Karl Fosaaen
- Using PowerShell to Identify Federated Domains
- LyncSniper: A tool for penetration testing Skype for Business and Lync deployments
- Troopers 19 - I am AD FS and So Can You

Privilege Escalation

sAMAccountName Spoofing

- sAMAccountName spoofing
- CVE-2021-42287/CVE-2021-42278 Weaponisation

Abusing Active Directory Certificate Services

- Certified Pre-Owned

PetitPotam

- PetitPotam
- From Stranger to DA // Using PetitPotam to NTLM relay to Domain Administrator

Zerologon

- Cobalt Strike ZeroLogon-BOF
- CVE-2020-1472 POC
- Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472)

Passwords in SYSVOL & Group Policy Preferences

- Finding Passwords in SYSVOL & Exploiting Group Policy Preferences
- Pentesting in the Real World: Group Policy Pwnage

MS14-068 Kerberos Vulnerability

- MS14-068: Vulnerability in (Active Directory) Kerberos Could Allow Elevation of Privilege
- Digging into MS14-068, Exploitation and Defence
- From MS14-068 to Full Compromise – Step by Step

DNSAdmins

- Abusing DNSAdmins privilege for escalation in Active Directory
- From DNSAdmins to Domain Admin, When DNSAdmins is More than Just DNS Administration

Kerberos Delegation

- Constructing Kerberos Attacks with Delegation Primitives
- No Shells Required - a Walkthrough on Using Impacket and Kerberos to Delegate Your Way to DA
- CVE-2020-17049: Kerberos Bronze Bit Attack – Overview

Unconstrained Delegation

- Domain Controller Print Server + Unconstrained Kerberos Delegation = Pwned Active Directory Forest
- Active Directory Security Risk #101: Kerberos Unconstrained Delegation (or How Compromise of a Single Server Can Compromise the Domain)
- Unconstrained Delegation Permissions
- Trust? Years to earn, seconds to break
- Hunting in Active Directory: Unconstrained Delegation & Forests Trusts
- Exploiting Unconstrained Delegation

Constrained Delegation

- Another Word on Delegation
- From Kekeo to Rubeus
- S4U2Pwnage
- Kerberos Delegation, Spns And More...

Resource-Based Constrained Delegation

- Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory
- Kerberos Resource-based Constrained Delegation: Computer Object Take Over
- Resource Based Constrained Delegation
- A Case Study in Wagging the Dog: Computer Takeover
- BloodHound 2.1's New Computer Takeover Attack

Insecure Group Policy Object Permission Rights

- Abusing GPO Permissions
- A Red Teamer’s Guide to GPOs and OUs
- File templates for GPO Abuse
- GPO Abuse - Part 1
- GPO Abuse - Part 2
- SharpGPOAbuse

Insecure ACLs Permission Rights

- Exploiting Weak Active Directory Permissions With Powersploit
- Escalating privileges with ACLs in Active Directory
- Abusing Active Directory Permissions with PowerView
- BloodHound 1.3 – The ACL Attack Path Update
- Scanning for Active Directory Privileges & Privileged Accounts
- Active Directory Access Control List – Attacks and Defense
- aclpwn - Active Directory ACL exploitation with BloodHound

Domain Trusts

- A Guide to Attacking Domain Trusts
- It's All About Trust – Forging Kerberos Trust Tickets to Spoof Access across Active Directory Trusts
- Active Directory forest trusts part 1 - How does SID filtering work?
- The Forest Is Under Control. Taking over the entire Active Directory forest
- Not A Security Boundary: Breaking Forest Trusts

- The Trustpocalypse
- Pentesting Active Directory Forests
- Security Considerations for Active Directory (AD) Trusts
- Kerberos Golden Tickets are Now More Golden

DCShadow

- Privilege Escalation With DCShadow
- DCShadow
- DCShadow explained: A technical deep dive into the latest AD attack technique
- DCShadow - Silently turn off Active Directory Auditing
- DCShadow - Minimal permissions, Active Directory Deception, Shadowception and more

RID

- Rid Hijacking: When Guests Become Admins

Microsoft SQL Server

- How to get SQL Server Sysadmin Privileges as a Local Admin with PowerUpSQL
- Compromise With Powerupsql – Sql Attacks

Red Forest

- Attack and defend Microsoft Enhanced Security Administrative

Exchange

- Exchange-AD-Privesc
- Abusing Exchange: One API call away from Domain Admin
- NtlmRelayToEWS

NTLM Relay & LLMNR/NBNS

- Pwning with Responder – A Pentester's Guide
- Practical guide to NTLM Relaying in 2017 (A.K.A getting a foothold in under 5 minutes)
- Relaying credentials everywhere with ntlmrelayx
- Beyond LLMNR/NBNS Spoofing – Exploiting Active Directory-Integrated DNS
- Combining NTLM Relaying and Kerberos delegation
- mitm6 – compromising IPv4 networks via IPv6
- The worst of both worlds: Combining NTLM Relaying and Kerberos delegation

Lateral Movement

Microsoft SQL Server Database links

- SQL Server – Link... Link... Link... and Shell: How to Hack Database Links in SQL Server!
- SQL Server Link Crawling with PowerUpSQL

Pass The Hash

- Performing Pass-the-hash Attacks With Mimikatz
- How to Pass-the-Hash with Mimikatz
- Pass-the-Hash Is Dead: Long Live LocalAccountTokenFilterPolicy

System Center Configuration Manager (SCCM)

- Targeted Workstation Compromise With Sccm
- PowerSCCM - PowerShell module to interact with SCCM deployments

WSUS

- Remote Weaponization of WSUS MITM
- WSUSpendu
- Leveraging WSUS – Part One

Password Spraying

- Password Spraying Windows Active Directory Accounts - Tradecraft Security Weekly #5
- Attacking Exchange with MailSniper
- A Password Spraying tool for Active Directory Credentials by Jacob Wilkin
- SprayingToolkit

Automated Lateral Movement

- GoFetch is a tool to automatically exercise an attack plan generated by the BloodHound application
- DeathStar - Automate getting Domain Admin using Empire
- ANGRYPUPPY - Bloodhound Attack Path Automation in CobaltStrike

Defense Evasion

In-Memory Evasion

- Bypassing Memory Scanners with Cobalt Strike and Gargoyle
- In-Memory Evasions Course
- Bring Your Own Land (BYOL) – A Novel Red Teaming Technique

Endpoint Detection and Response (EDR) Evasion

- Red Teaming in the EDR age
- Sharp-Suite - Process Argument Spoofing
- Red Team Tactics: Combining Direct System Calls and sRDI to bypass AV/EDR
- Dechaining Macros and Evading EDR
- Bypass EDR's memory protection, introduction to hooking
- Bypassing Cylance and other AVs/EDRs by Unhooking Windows APIs
- Silencing Cylance: A Case Study in Modern EDRs

OPSEC

- Modern Defenses and YOU!
- OPSEC Considerations for Beacon Commands
- Red Team Tradecraft and TTP Guidance
- Fighting the Toolset

Microsoft ATA & ATP Evasion

- Red Team Techniques for Evading, Bypassing, and Disabling MS Advanced Threat Protection and Advanced Threat Analytics
- Red Team Revenge - Attacking Microsoft ATA
- Evading Microsoft ATA for Active Directory Domination

PowerShell ScriptBlock Logging Bypass

- PowerShell ScriptBlock Logging Bypass

PowerShell Anti-Malware Scan Interface (AMSI) Bypass

- How to bypass AMSI and execute ANY malicious Powershell code
- AMSI: How Windows 10 Plans to Stop Script-Based Attacks
- AMSI Bypass: Patching Technique
- Invisi-Shell - Hide your Powershell script in plain sight. Bypass all Powershell security features
- Dynamic Microsoft Office 365 AMSI In Memory Bypass Using VBA

- AmsiScanBuffer Bypass - Part 1
- AMSI Bypass

Loading .NET Assemblies Anti-Malware Scan Interface (AMSI) Bypass

- A PoC function to corrupt the g_amsiContext global variable in clr.dll in .NET Framework Early Access build 3694

AppLocker & Device Guard Bypass

- Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

Sysmon Evasion

- Subverting Sysmon: Application of a Formalized Security Product Evasion Methodology
- sysmon-config-bypass-finder
- Shhmon — Silencing Sysmon via Driver Unload

HoneyTokens Evasion

- Forging Trusts for Deception in Active Directory
- Honeypot Buster: A Unique Red-Team Tool

Disabling Security Tools

- Invoke-Phant0m - Windows Event Log Killer

Credential Dumping

NTDS.DIT Password Extraction

- How Attackers Pull the Active Directory Database (NTDS.dit) from a Domain Controller
- Extracting Password Hashes From The Ntds.dit File

SAM (Security Accounts Manager)

- Internal Monologue Attack: Retrieving NTLM Hashes without Touching LSASS

Kerberoasting

- Kerberoasting Without Mimikatz
- Cracking Kerberos TGS Tickets Using Kerberoast – Exploiting Kerberos to Compromise the Active Directory Domain

- Extracting Service Account Passwords With Kerberoasting
- Cracking Service Account Passwords with Kerberoasting
- Kerberoast PW list for cracking passwords with complexity requirements
- DerbyCon 2019 - Kerberoasting Revisited

Kerberos AP-REP Roasting

- Roasting AS-REPs

Windows Credential Manager/Vault

- Operational Guidance for Offensive User DPAPI Abuse
- Jumping Network Segregation with RDP

DCSync

- Mimikatz and DCSync and ExtraSids, Oh My
- Mimikatz DCSync Usage, Exploitation, and Detection
- Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync

LLMNR/NBT-NS Poisoning

- LLMNR/NBT-NS Poisoning Using Responder

Others

- Compromising Plain Text Passwords In Active Directory
- Kerberos Tickets on Linux Red Teams

Persistence

Diamond Ticket

- A Diamond (Ticket) in the Ruff

Golden Ticket

- Golden Ticket
- Kerberos Golden Tickets are Now More Golden

SID History

- Sneaky Active Directory Persistence #14: SID History

Silver Ticket

- How Attackers Use Kerberos Silver Tickets to Exploit Systems
- Sneaky Active Directory Persistence #16: Computer Accounts & Domain Controller Silver Tickets

DCShadow

- Creating Persistence With Dcshadow

AdminSDHolder

- Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights
- Persistence Using Adminsdholder And Sdprop

Group Policy Object

- Sneaky Active Directory Persistence #17: Group Policy

Skeleton Keys

- Unlocking All The Doors To Active Directory With The Skeleton Key Attack
- Skeleton Key
- Attackers Can Now Use Mimikatz to Implant Skeleton Key on Domain Controllers & BackDoor Your Active Directory Forest

SeEnableDelegationPrivilege

- The Most Dangerous User Right You (Probably) Have Never Heard Of
- SeEnableDelegationPrivilege Active Directory Backdoor

Security Support Provider

- Sneaky Active Directory Persistence #12: Malicious Security Support Provider (SSP)

Directory Services Restore Mode

- Sneaky Active Directory Persistence #11: Directory Service Restore Mode (DSRM)
- Sneaky Active Directory Persistence #13: DSRM Persistence v2

ACLs & Security Descriptors

- An ACE Up the Sleeve: Designing Active Directory DACL Backdoors
- Shadow Admins – The Stealthy Accounts That You Should Fear The Most
- The Unintended Risks of Trusting Active Directory

Tools & Scripts

- Certify - Certify is a C# tool to enumerate and abuse misconfigurations in Active Directory Certificate Services (AD CS).
- PSPKIAudit - PowerShell toolkit for auditing Active Directory Certificate Services (AD CS).
- PowerView - Situational Awareness PowerShell framework
- BloodHound - Six Degrees of Domain Admin
- Impacket - Impacket is a collection of Python classes for working with network protocols
- aclpwn.py - Active Directory ACL exploitation with BloodHound
- CrackMapExec - A swiss army knife for pentesting networks
- ADACLScanner - A tool with GUI or command linte used to create reports of access control lists (DACLs) and system access control lists (SACLs) in Active Directory
- zBang - zBang is a risk assessment tool that detects potential privileged account threats
- SafetyKatz - SafetyKatz is a combination of slightly modified version of @gentilkiwi's Mimikatz project and @subTee's .NET PE Loader.
- SharpDump - SharpDump is a C# port of PowerSploit's Out-Minidump.ps1 functionality.
- PowerUpSQL - A PowerShell Toolkit for Attacking SQL Server
- Rubeus - Rubeus is a C# toolset for raw Kerberos interaction and abuses
- ADRecon - A tool which gathers information about the Active Directory and generates a report which can provide a holistic picture of the current state of the target AD environment
- Mimikatz - Utility to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory but also perform pass-the-hash, pass-the-ticket or build Golden tickets
- Grouper - A PowerShell script for helping to find vulnerable settings in AD Group Policy.
- Powermad - PowerShell MachineAccountQuota and DNS exploit tools
- RACE - RACE is a PowerShell module for executing ACL attacks against Windows targets.
- DomainPasswordSpray - DomainPasswordSpray is a tool written in PowerShell to perform a password spray attack against users of a domain.
- MailSniper - MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.)

- LAPSToolkit - Tool to audit and attack LAPS environments.
- CredDefense - Credential and Red Teaming Defense for Windows Environments
- ldapdomaindump - Active Directory information dumper via LDAP
- SpoolSample - PoC tool to coerce Windows hosts authenticate to other machines via the MS-RPRN RPC interface
- adconnectdump - Azure AD Connect password extraction
- o365recon - Script to retrieve information via O365 with a valid cred
- ROADtools - ROADtools is a framework to interact with Azure AD. I
- Stormspotter - Stormspotter creates an “attack graph” of the resources in an Azure subscription.
- AADInternals - AADInternals is PowerShell module for administering Azure AD and Office 365
- MicroBurst: A PowerShell Toolkit for Attacking Azure - MicroBurst includes functions and scripts that support Azure Services discovery, weak configuration auditing, and post exploitation actions such as credential dumping.
- sam-the-admin - Exploiting CVE-2021-42278 and CVE-2021-42287 to impersonate DA from standard domain user
- CVE-2021-42287/CVE-2021-42278 Scanner & Exploiter. - CVE-2021-42287/CVE-2021-42278 Scanner & Exploiter. Yet another low effort domain user to domain admin exploit.
- ADModule - Microsoft signed ActiveDirectory PowerShell module
- ImproHound - Identify the attack paths in BloodHound breaking your AD tiering
- ADExplorerSnapshot.py - ADExplorerSnapshot.py is an AD Explorer snapshot ingestor for BloodHound.

Ebooks

- The Dog Whisperer’s Handbook – A Hacker’s Guide to the BloodHound Galaxy
- Varonis eBook: Pen Testing Active Directory Environments

Cheat Sheets

- Tools Cheat Sheets - Tools (PowerView, PowerUp, Empire, and PowerSploit)
- DogWhisperer - BloodHound Cypher Cheat Sheet (v2)
- PowerView-3.0 tips and tricks
- PowerView-2.0 tips and tricks
- BloodhoundAD-Queries
- Kerberos Attacks Cheat Sheet
- Bloodhound Cypher Cheatsheet

- Kerberos cheatsheet
- Active Directory Exploitation Cheat Sheet

Other Resources

- Tactics, Techniques and Procedures for Attacking Active Directory BlackHat Asia 2019
- Bloodhound walkthrough. A Tool for Many Tradecrafts
- Attack Methods for Gaining Domain Admin Rights in Active Directory
- PowerShell Is Dead Epic Learnings
- Finding Our Path: How We're Trying to Improve Active Directory Security
- SteelCon 2019: Getting Splunky With Kerberos - Ross Bingham and Tom MacDonald
- AD-security-workshop

Azure Active Directory

- AZURE AD INTRODUCTION FOR RED TEAMERS
- I'm in your cloud... reading everyone's email. Hacking Azure AD via Active Directory
- Utilizing Azure Services for Red Team Engagements
- Blue Cloud of Death: Red Teaming Azure
- Azure AD Connect for Red Teamers
- Red Teaming Microsoft: Part 1 – Active Directory Leaks via Azure
- Attacking & Defending the Microsoft Cloud
- How to create a backdoor to Azure AD
- Azurehound Cypher Cheatsheet
- Keys of the kingdom: Playing God as Global Admin

Defense & Detection

Tools & Scripts

- Invoke-TrimarcADChecks - The Invoke-TrimarcADChecks.ps1 PowerShell script is designed to gather data from a single domain AD forest to performed Active Directory Security Assessment (ADSA).
- Create-Tiers in AD - Project Title Active Directory Auto Deployment of Tiers in any environment
- SAMRi10 - Hardening SAM Remote Access in Windows 10/Server 2016
- Net Cease - Hardening Net Session Enumeration

- PingCastle - A tool designed to assess quickly the Active Directory security level with a methodology based on risk assessment and a maturity framework
- Aorato Skeleton Key Malware Remote DC Scanner - Remotely scans for the existence of the Skeleton Key Malware
- Reset the krbtgt account password/keys - This script will enable you to reset the krbtgt account password and related keys while minimizing the likelihood of Kerberos authentication issues being caused by the operation
- Reset The KrbTgt Account Password/Keys For RWDCs/RODCs
- RiskySPN - RiskySPNs is a collection of PowerShell scripts focused on detecting and abusing accounts associated with SPNs (Service Principal Name).
- Deploy-Deception - A PowerShell module to deploy active directory decoy objects
- SpoolerScanner - Check if MS-RPRN is remotely available with powershell/c#
- dcept - A tool for deploying and detecting use of Active Directory honeytokens
- LogonTracer - Investigate malicious Windows logon by visualizing and analyzing Windows event log
- DCSYNCMonitor - Monitors for DCSYNC and DCSHADOW attacks and create custom Windows Events for these events
- Sigma - Generic Signature Format for SIEM Systems
- Sysmon - System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.
- SysmonSearch - Investigate suspicious activity by visualizing Sysmon's event log
- ClrGuard - ClrGuard is a proof of concept project to explore instrumenting the Common Language Runtime (CLR) for security purposes.
- Get-ClrReflection - Detects memory-only CLR (.NET) modules.
- Get-InjectedThread - Get-InjectedThread looks at each running thread to determine if it is the result of memory injection.
- SilkETW - SilkETW & SilkService are flexible C# wrappers for ETW, they are meant to abstract away the complexities of ETW and give people a simple interface to perform research and introspection.
- WatchAD - AD Security Intrusion Detection System
- Sparrow - Sparrow.ps1 was created by CISA's Cloud Forensics team to help detect possible compromised accounts and applications in the Azure/m365 environment.
- DFIR-O365RC - The DFIR-O365RC PowerShell module is a set of functions that allow the DFIR analyst to collect logs relevant for Office 365 Business Email Compromise investigations.
- AzureADIncidentResponse - Tooling to assist in Azure AD incident response
- ADTimeline - The ADTimeline script generates a timeline based on Active Directory replication metadata for objects considered of interest.

Sysmon Configuration

- sysmon-modular - A Sysmon configuration repository for everybody to customise
- sysmon-dfir - Sources, configuration and how to detect evil things utilizing Microsoft Sysmon.
- sysmon-config - Sysmon configuration file template with default high-quality event tracing

Active Directory Security Checks (by Sean Metcalf - @Pyrotek3)

General Recommendations

- Manage local Administrator passwords (LAPS).
- Implement RDP Restricted Admin mode (as needed).
- Remove unsupported OSs from the network.
- Monitor scheduled tasks on sensitive systems (DCs, etc.).
- Ensure that OOB management passwords (DSRM) are changed regularly & securely stored.
- Use SMB v2/v3+
- Default domain Administrator & KRBTGT password should be changed every year & when an AD admin leaves.
- Remove trusts that are no longer necessary & enable SID filtering as appropriate.
- All domain authentications should be set (when possible) to: "Send NTLMv2 response onlyrefuse LM & NTLM."
- Block internet access for DCs, servers, & all administration systems.

Protect Admin Credentials

- No "user" or computer accounts in admin groups.
- Ensure all admin accounts are "sensitive & cannot be delegated".
- Add admin accounts to "Protected Users" group (requires Windows Server 2012 R2 Domain Controllers, 2012R2 DFL for domain protection).
- Disable all inactive admin accounts and remove from privileged groups.

Protect AD Admin Credentials

- Limit AD admin membership (DA, EA, Schema Admins, etc.) & only use custom delegation groups.
- ‘Tiered’ Administration mitigating credential theft impact.
- Ensure admins only logon to approved admin workstations & servers.
- Leverage time-based, temporary group membership for all admin accounts

Protect Service Account Credentials

- Limit to systems of the same security level.
- Leverage “(Group) Managed Service Accounts” (or PW >20 characters) to mitigate credential theft (kerberoast).
- Implement FGPP (DFL =>2008) to increase PW requirements for SAs and administrators.
- Logon restrictions – prevent interactive logon & limit logon capability to specific computers.
- Disable inactive SAs & remove from privileged groups.

Protect Resources

- Segment network to protect admin & critical systems.
- Deploy IDS to monitor the internal corporate network.
- Network device & OOB management on separate network.

Protect Domain Controllers

- Only run software & services to support AD.
- Minimal groups (& users) with DC admin/logon rights.
- Ensure patches are applied before running DCPromo (especially MS14-068 and other critical patches).
- Validate scheduled tasks & scripts.

Protect Workstations (& Servers)

- Patch quickly, especially privilege escalation vulnerabilities.
- Deploy security back-port patch (KB2871997).
- Set Wdigest reg key to 0 (KB2871997/Windows 8.1/2012R2+): HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlSecurityProvidersWdigest
- Deploy workstation whitelisting (Microsoft AppLocker) to block code exec in user folders – home dir & profile path.
- Deploy workstation app sandboxing technology (EMET) to mitigate application memory exploits (0-days).

Logging

- Enable enhanced auditing
- “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings”
- Enable PowerShell module logging (“*”) & forward logs to central log server (WEF or other method).

- Enable CMD Process logging & enhancement (KB3004375) and forward logs to central log server.
- SIEM or equivalent to centralize as much log data as possible.
- User Behavioural Analysis system for enhanced knowledge of user activity (such as Microsoft ATA).

Security Pro's Checks

- Identify who has AD admin rights (domain/forest).
- Identify who can logon to Domain Controllers (& admin rights to virtual environment hosting virtual DCs).
- Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions.
- Ensure AD admins (aka Domain Admins) protect their credentials by not logging into untrusted systems (workstations).
- Limit service account rights that are currently DA (or equivalent).

Important Security Updates

CVE	Title	Description	Link
CVE-2020-1472	Netlogon Elevation of Privilege Vulnerability	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

CVE	Title	Description	Link
CVE-2019-1040	Windows NTLM Tampering Vulnerability	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1040
CVE-2019-0683	Active Directory Elevation of Privilege Vulnerability	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0683

CVE	Title	Description	Link
CVE-2019-0708	Remote Desktop Services Remote Code Execution Vulnerability	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
CVE-2018-8581	Microsoft Exchange Server Elevation of Privilege Vulnerability	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka "Microsoft Exchange Server Elevation of Privilege Vulnerability." This affects Microsoft Exchange Server.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8518

CVE	Title	Description	Link
CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143

CVE	Title	Description	Link
CVE-2016-0128	Windows SAM and LSAD Downgrade Vulnerability	The SAM and LSAD protocol implementations in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 do not properly establish an RPC channel, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "Windows SAM and LSAD Downgrade Vulnerability" or "BADLOCK."	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2016-0128

CVE	Title	Description	Link
CVE-2014-6324	Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)	The Kerberos Key Distribution Center (KDC) in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote authenticated domain users to obtain domain administrator privileges via a forged signature in a ticket, as exploited in the wild in November 2014, aka "Kerberos Checksum Vulnerability."	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-068

CVE	Title	Description	Link
CVE-2014-1812	Vulnerability in Group Policy Preferences could allow elevation of privilege	The Group Policy implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly handle distribution of passwords, which allows remote authenticated users to obtain sensitive credential information and consequently gain privileges by leveraging access to the SYSVOL share, as exploited in the wild in May 2014, aka "Group Policy Preferences Password Elevation of Privilege Vulnerability."	https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevati

Detection

Attack	Event ID
Account and Group Enumeration	4798: A user's local group membership was enumerated 4799: A security-enabled local group membership was enumerated

Attack	Event ID
AdminSDHolder	4780: The ACL was set on accounts which are members of administrators groups
Kekeo	4624: Account Logon 4672: Admin Logon 4768: Kerberos TGS Request
Silver Ticket	4624: Account Logon 4634: Account Logoff 4672: Admin Logon
Golden Ticket	4624: Account Logon 4672: Admin Logon
PowerShell	4103: Script Block Logging 400: Engine Lifecycle 403: Engine Lifecycle 4103: Module Logging 600: Provider Lifecycle
DCShadow	4742: A computer account was changed 5137: A directory service object was created 5141: A directory service object was deleted 4929: An Active Directory replica source naming context was removed
Skeleton Keys	4673: A privileged service was called 4611: A trusted logon process has been registered with the Local Security Authority 4688: A new process has been created 4689: A new process has exited
PYKEK MS14-068	4672: Admin Logon 4624: Account Logon 4768: Kerberos TGS Request
Kerberoasting	4769: A Kerberos ticket was requested
S4U2Proxy	4769: A Kerberos ticket was requested
Lateral Movement	4688: A new process has been created 4689: A process has exited 4624: An account was successfully logged on 4625: An account failed to log on

Attack	Event ID
DNSAdmin	770: DNS Server plugin DLL has been loaded 541: The setting serverlevelplugindll on scope . has been set to `<dll path>` 150: DNS Server could not load or initialize the plug-in DLL
DCSync	4662: An operation was performed on an object
Password Spraying	4625: An account failed to log on 4771: Kerberos pre-authentication failed 4648: A logon was attempted using explicit credentials

Resources

- How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472
- Securing Active Directory: Performing an Active Directory Security Review
- ACTIVE DIRECTORY SECURITY ASSESSMENT CHECKLIST
- ASD Strategies to Mitigate Cyber Security Incidents
- Reducing the Active Directory Attack Surface
- Changes to Ticket-Granting Ticket (TGT) Delegation Across Trusts in Windows Server (AskPFEPlat edition)
- ADV190006 | Guidance to mitigate unconstrained delegation vulnerabilities
- ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing
- Active Directory: Ultimate Reading Collection
- Security Hardening Tips and Recommendations
- Securing Domain Controllers to Improve Active Directory Security
- Securing Windows Workstations: Developing a Secure Baseline
- Implementing Secure Administrative Hosts
- Privileged Access Management for Active Directory Domain Services
- Awesome Windows Domain Hardening
- Best Practices for Securing Active Directory
- Introducing the Adversary Resilience Methodology—Part One
- Introducing the Adversary Resilience Methodology—Part Two
- Mitigating Pass-the-Hash and Other Credential Theft, version 2
- Configuration guidance for implementing the Windows 10 and Windows Server 2016 DoD Secure Host Baseline settings
- Monitoring Active Directory for Signs of Compromise
- Detecting Lateral Movement through Tracking Event Logs

- Kerberos Golden Ticket Protection Mitigating Pass-the-Ticket on Active Directory
- Overview of Microsoft's "Best Practices for Securing Active Directory"
- The Keys to the Kingdom: Limiting Active Directory Administrators
- Protect Privileged AD Accounts With Five Free Controls
- The Most Common Active Directory Security Issues and What You Can Do to Fix Them
- Event Forwarding Guidance
- Planting the Red Forest: Improving AD on the Road to ESAE
- Detecting Kerberoasting Activity
- Security Considerations for Trusts
- Advanced Threat Analytics suspicious activity guide
- Protection from Kerberos Golden Ticket
- Windows 10 Credential Theft Mitigation Guide
- Detecting Pass-The- Ticket and Pass-The- Hash Attack Using Simple WMI Commands
- Step by Step Deploy Microsoft Local Administrator Password Solution
- Active Directory Security Best Practices
- Finally Deploy and Audit LAPS with Project VAST, Part 1 of 2
- Windows Security Log Events
- Talk Transcript BSidesCharm Detecting the Elusive: Active Directory Threat Hunting
- Preventing Mimikatz Attacks
- Understanding "Red Forest" - The 3-Tier ESAE and Alternative Ways to Protect Privileged Credentials
- Securing Microsoft Active Directory Federation Server (ADFS)
- Azure AD and ADFS best practices: Defending against password spray attacks
- AD Reading: Active Directory Backup and Disaster Recovery
- Ten Process Injection Techniques: A Technical Survey Of Common And Trending Process Injection Techniques
- Hunting For In-Memory .NET Attacks
- Mimikatz Overview, Defenses and Detection
- Trimarc Research: Detecting Password Spraying with Security Event Auditing
- Hunting for Gargoyle Memory Scanning Evasion
- Planning and getting started on the Windows Defender Application Control deployment process
- Preventing Lateral Movement Using Network Access Groups
- How to Go from Responding to Hunting with Sysinternals Sysmon
- Windows Event Forwarding Guidance
- Threat Mitigation Strategies: Part 2 – Technical Recommendations and Information
- Modern Hardening: Lessons Learned on Hardening Applications and Services

- ITSP.70.012 Guidance for Hardening Microsoft Windows 10 Enterprise
- Blue Team Tips
- Active Directory Domain Security Technical Implementation Guide (STIG)
- Active Directory Security Testing Guide - v2.0
- Best practices for securing Active Directory Federation Services
- The most common on premises vulnerabilities & misconfigurations

License

Releases

No releases published

Packages

No packages published

Contributors 4


infosecn1nja Rahmat Nurfauzi


apanonimo José M. Aparicio


screetsec Edo Maland


h3xstream Philippe Arteau