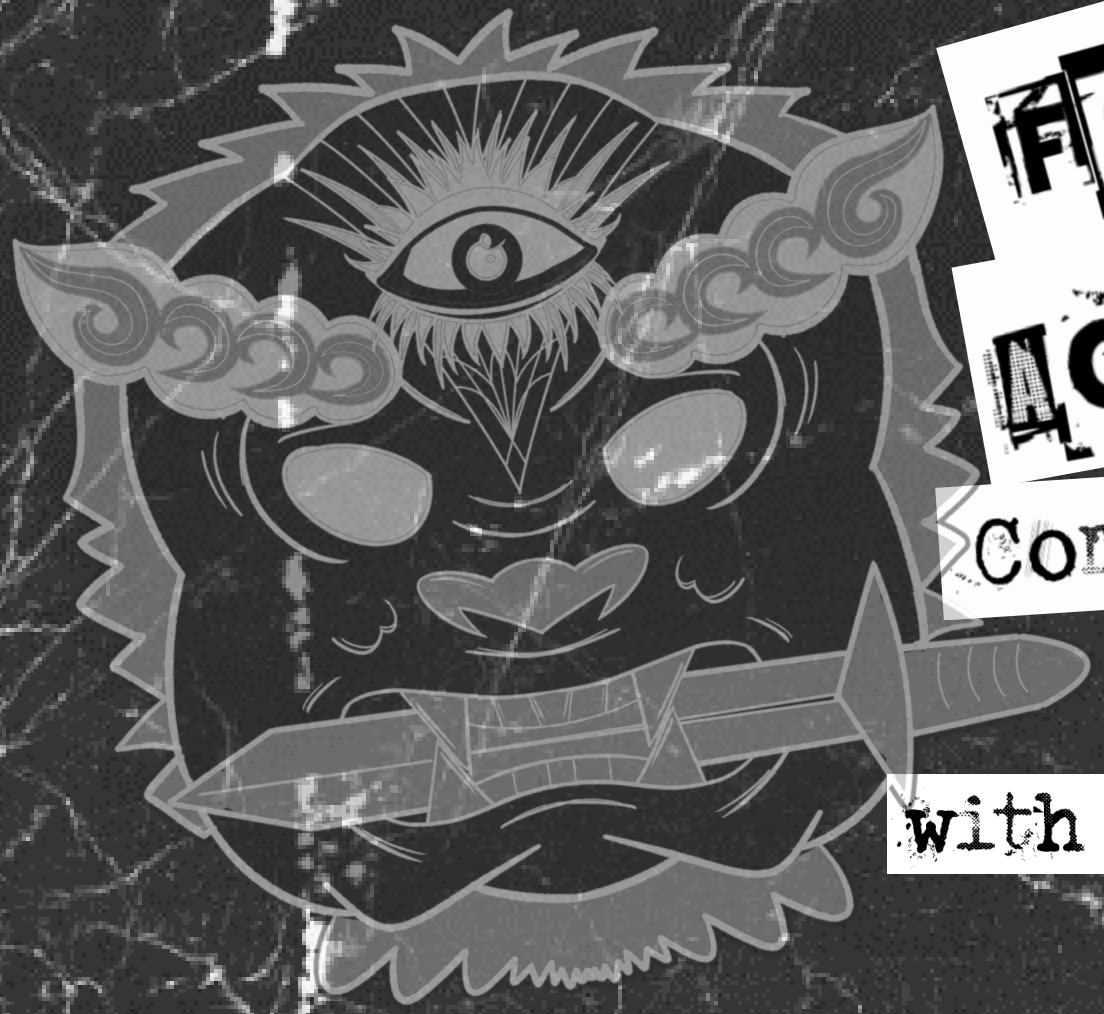


Fortifying Active Directory

Combatting Misconfigurations

with Jeff Tomkiewicz

The_Gh0stFace_Killer

Introduction

Joint advisory by the NSA and CISA

1.Default Configurations of Software and Applications

2. Improper Separation of User/Administrator Privileges

3.Insufficient Internal Network Monitoring

4. Lack of Network Segmentation

AGENDA

Continued

5. Poor Patch Management

6. Bypass of System Access Controls

7. Weak or Misconfigured MFA

8. Insufficient Access Control Lists (ACLs) on Network Shares and Services

9. Poor Credential Hygiene

10. Unrestricted Code Execution

Conclusion and Q&A

INTRODUCTION

whoami

Offensive Security Engineer for a Healthcare Fortune 40 org

Specializing in…

- Network Penetration Testing
- Social Engineering
- Physical / Covert Entry

JOINT ADVISORY BY THE NSA AND CISA

In October 2023, NSA and CISA Red and Blue Teams released an advisory on large organizations' top 10 most common network misconfigurations.

One thing interesting of note both teams swapped roles and learn each others' jobs 3 months prior to the engagement… Purple Teaming to the EXTREME!!!

Highlighted two(2) trends:

1. Systemic weaknesses in large organizations with "mature" cyber postures
2. Software manufacturers need to embrace secure-by-design principles to reduce the burden on defenders

Default Configurations of Software and Applications

Definition

Software and application default configurations in Active Directory (AD) environments often include settings that prioritize ease of use and ignore security.

- Default Credentials
- Legacy Protocols/Services
- Insecure SMB Services
- Misconfigured Active Directory Certificate Services (AD CS)

Default Configurations of Software and Applications

Risk Findings

Assessment teams regularly found the following:

Insecure Active Directory Certificate Services (ADCS)

- Risk of unauthorized certificate issuance
- Weak cryptographic algorithms
- Improper certificate revocation settings

Insecure Legacy Protocols and Services

- NTLM / LM Hashes
- SMBv1 / Open SMB Shares

Default Configurations of Software and Applications

Best Practices

ADCS Configuration

- Configure Strong Algorithms
- Restrict Certificate Templates
- Enforce Certificate Revocation
  - Online Certificate Status Protocol(OCSP) / Certificate Revocation Lists (CRLs)
- Isolate CA Servers

Disable Legacy Protocols and Services

- Disable NTLM via Group Policy
- Remove LM Hashes
  - Configure the NoLMHash policy in Group Policy
- Secure SMB Versions and Configurations

Improper Separation of User/Administrator Privileges

Definition

Principle of Least Privilege in Active Directory

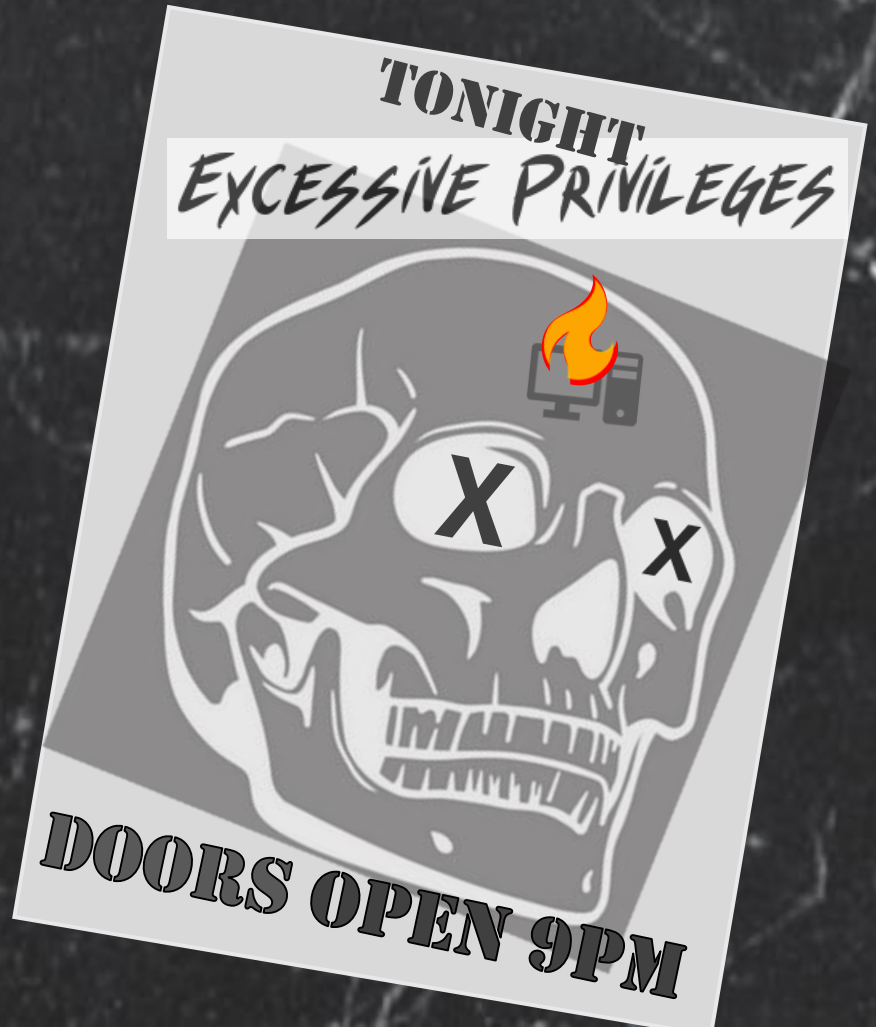
The principle of least privilege (PoLP) dictates that users and systems should be granted the minimum levels of access—or permissions—necessary to perform their job functions.

- Privilege Assignment Pitfalls:
  - Excessive Privileges
  - Shared Accounts
  - Misuse of Built In Groups
  - Lack of Monitoring and Auditing

IMPROPER SEPARATION OF USER/ADMINISTRATOR PRIVILEGES

Risk Findings

After obtaining initial access via an account with administrative permissions, an assessment team compromised a domain in under a business day.



Improper Separation of User/Administrator Privileges

Best Practices

- Regular Privilege Audits
- Training and Awareness
- Implement Segmentation and Isolation
- Use Secure Administrative Practices
  - Role-Based Access Control (RBAC)
  - Administrative Tier Model
  - Just Enough Administration (JEA)
  - Privileged Access Workstations (PAWs)

```
# Identify users in privileged AD groups

Get-ADGroupMember -Identity "Domain Admins"

Get-ADGroupMember -Identity "Enterprise Admins"
```

INSUFFICIENT INTERNAL NETWORK MONITORING

Definition

Insufficient internal network monitoring can out right incapacitate organisations. The importance of tracking in Active Directory (AD) environments serves two folds:

- Security and Compliance
  - Detecting Threats
  - Compliance
- Operational Insight
  - Performance Management
  - Incident Response

INSUFFICIENT INTERNAL NETWORK MONITORING

Risk Findings

Assessment teams exploited insufficient monitoring to gain access to assessed networks.

- Observations by assessment teams revealed a concerning gap in the cybersecurity measures of some organizations, with host-based monitoring in place but a notable absence of network monitoring.
- An assessment team gained persistent deep access to a large organization with a mature cyber posture. There was no detection of lateral movement, persistence, or command and control (C2), including attempted noisy activities to trigger a security response.

Insufficient Internal Network Monitoring

Best Practices

Tools and Techniques

- Security Information and Event Management (SIEM) Systems
- AD Specific Monitoring Tools
- Network Traffic Analysis
- Endpoint Detection and Response (EDR)
- Event Log Monitoring

Indicators of Compromise (IoC) with Monitoring

- Unusual Logon Activity
- Changes to Critical AD Groups
- Suspicious Process Activity
- Changes in Security Settings and Policies

Lack of Network Segmentation

Definition

Network segmentation involves dividing a network into smaller, distinct segments or subnetworks. Each segment is isolated. This is typically using firewalls, VLANs, or other network security devices. Isolation helps control and restrict traffic flow between segments.

- Importance
  - Isolation of Critical Systems
  - Containment of Breaches
  - Access Control

Lack of Network Segmentation

Risk Findings

- Assessment teams often gained access to OT networks—despite prior assurance that the networks were air gapped, with no possible connection to the IT network. Special purpose, forgotten, or even accidental network connections were discovered.

Lack of Network Segmentation

Best Practices

Strategies for Segmenting AD Controlled Networks

- Tiered Administration Model
- Use of VLANs and Subnets
- Firewalls and Access Control Lists (ACLs)
- Privileged Access Workstations (PAWs)
- Network Segmentation Tools

```
# Check Windows Firewall rules related to segmentation

Get-NetFirewallRule -PolicyStore ActiveStore
```

POOR PATCH MANAGEMENT

Impact of Outdated AD Systems and Software

- Security Vulnerabilities
  - Exploitation
  - Malware and Ransomware
- Operational Issues
  - System Instability
  - Compliance Risks
- Examples
  - EternalBlue (MS17-010) - exploited by the WannaCry ransomware
  - ZeroLogon (CVE-2020-1472) - critical vulnerability in the Netlogon protocol, allowing attackers to domain admin privileges

POOR PATCH MANAGEMENT

Risk Findings

- Assessment teams frequently observe organizations using unsupported Windows operating systems without updates MS17-010 and MS08-67
  - MS08-67 - Vulnerability in Server Service Could Allow Remote Code Execution

POOR PATCH MANAGEMENT

Best Practices

Automating Updates and Patch Management Processes

- Patch Management Tools
- Automated Patch Deployment
- Patch Testing and Validation
- Security Baselines and Configuration Management
- Monitoring and Reporting

```
# Check for missing patches

Get-WindowsUpdateLog | Select-String "Failed"
```

```
# Example: Generating a Compliance Report with PowerShell
Get-WindowsUpdateLog | Out-File -FilePath "C:\UpdateLogs\UpdateComplianceReport.txt"
```

Bypass of System Access Controls

- Attackers can bypass system access controls by compromising alternate authentication methods in an environment.

- Common Methods Used:
  - Pass-the-Hash (PtH) Attacks
  - Pass-the-Ticket (PtT) Attacks
  - Golden Ticket Attacks
  - Silver Ticket Attacks
  - DCShadow Attacks
  - Credential Dumping
  - Exploiting Misconfigurations

BYPASS OF SYSTEM ACCESS CONTROLS

Risk Findings

- By mimicking accounts, assessment teams expanded and fortify their access without detection.
- Kerberoasting was one of the most time-efficient ways to elevate privileges and allowed movement laterally throughout organizations networks.

BYPASS OF SYSTEM ACCESS CONTROLS

Best Practices

Security Measures to Reinforce Access Controls

- Implement Least Privilege
- Use Strong Authentication Methods
- Regularly Update and Patch Systems
- Monitor and Audit
- Restrict Credential Use
- Implement Network Segmentation
- Regular Audits and Penetration Testing
- Deploy Endpoint Protection

```
# Check ACLs for critical AD objects

Get-Acl "AD:\CN=AdminSDHolder,CN=System,DC=domain,DC=com"
```

WEAK OR MISCONFIGURED

MULTI-FACTOR AUTHENTICATION (MFA)

MFA Importance in AD Security

- Enhanced Security
  - Provides multiple forms of verification
- Mitigation of Common Attacks
  - Social Engineering
  - Credential Stuffing
  - Pass-the-Hash(PtH)
- Compliance and Standards
  - Regulatory Requirements
  - Security Standards

Weak or Misconfigured Multi-Factor Authentication (MFA)

Risk Findings

- An assessment team knew a user's main credentials, but their login attempts were blocked by MFA requirements.
- The team then masqueraded as IT staff and convinced the user to provide the MFA code over the phone, allowing the team to complete their login attempt and gain access to the user's email and other organizational resources.

Weak or Misconfigured Multi-Factor Authentication (MFA)

Best Practices

Security Measures to Reinforce Access Controls

- Train employees on social engineering tactics such as vishing and phishing.
- Select Appropriate MFA Methods
- Enforce MFA Across the Organization
- Regularly Review and Update MFA Configurations
- Integration with Existing Systems
- Monitor and Report

```
# Connect to Azure AD
Connect-AzureAD

# Get MFA status for all users
Get-AzureADUser | Select-Object UserPrincipalName, DisplayName, StrongAuthenticationMethods | Format-Table -AutoSize
```

INSUFFICIENT ACLS ON NETWORK SHARES AND SERVICES

Access Control Lists (ACLs) in Active Directory (AD)

- Definition and Role
  - Use Access Control Entries (ACEs)
- Function in AD
  - Security
  - Granularity

INSUFFICIENT ACLS ON NETWORK SHARES AND SERVICES

Best Practices

Best Practices for Configuring ACLs

- Principle Least Privilege
- Inheritance Management
- Regular Audits and Reviews
- Use of Groups for Permissions
- Documentation and Change Control
- Segregation of Duties

```
# Get ACLs for shared folders

Get-SmbShare | ForEach-Object { Get-Acl $_.Path }
```

Insufficient ACLs on Network Shares and Services

Risk Findings

- Assessment teams regularly identified sensitive data and PII on shared drives (e.g., scanned documents, social security numbers, and tax returns) that could be used for extortion or social engineering of the organization or employees.

POOR CREDENTIAL HYGIENE

Common Credential Management Errors in AD

- Weak Password Policies
- Unchanged Default Credentials
- Password Sharing
- Storing Credentials Insecurely
- Lack of MFA
- Over-permissive Access Rights

POOR CREDENTIAL HYGIENE

Risk Findings

- Assessment teams cracked password hashes for NTLM users, Kerberos service account tickets, NetNTLMv2, and PFX stores allowing for privilege escalation and move laterally within networks.
- In 12 hours, one team cracked over 80% of all users passwords in an Active Directory, resulting in hundreds of valid credentials.

POOR CREDENTIAL HYGIENE

Best Practices

Security Measures to Reinforce Access Controls

- Enforce Strong Password Policies
- Implement MFA
- Regular Credential Audits
- Secure Storage of Credentials
- Integration with Existing Systems
- Educate Users on Credential Security
- Monitor and Respond to Credential Compromise.

```
# Search for weak passwords in AD

Get-ADUser -Filter * -Properties PasswordLastSet | Where-Object { $_.PasswordLastSet -lt (Get-Date).AddDays(-90) }
```

UNRESTRICTED CODE EXECUTION

Risks Associated with Unrestricted Code Execution

- Privilege Escalation
- Malware and Ransomware
- Lateral Movement
- Data Exfiltration
- Persistence Mechanisms

UNRESTRICTED CODE EXECUTION

Risk Findings

- Assessment teams frequently leveraged unrestricted code execution in the form of executables, dynamic link libraries (DLLs), HTML applications, and macros (scripts used in office automation documents)to establish initial access, persistence, and lateral movement.

UNRESTRICTED CODE EXECUTION

Best Practices

Security Measures to Reinforce Access Controls

- Group Policy Restrictions
- Application Whitelisting
- User Account Control (UAC)
- Restrict Administrative Access
- Integration with Existing Systems
- Security Hardening

UNRESTRICTED CODE EXECUTION

Best Practices

Security Measures to Reinforce Access Controls

- Group Policy Restrictions
- Application Whitelisting
- User Account Control (UAC)
- Restrict Administrative Access
- Security Hardening

```
# Create AppLocker rules to whitelist applications

New-AppLockerPolicy -Default -UserOrGroupSid "S-1-1-0" -XmlPolicy "C:\AppLockerPolicy.xml"

Import-AppLockerPolicy -XmlPolicy "C:\AppLockerPolicy.xml" -Merge
```

CONCLUSION

- In conclusion, addressing the top 10 cybersecurity misconfigurations outlined by the NSA and CISA in Active Directory (AD) environments is essential.
- Issues like poor credential hygiene, weak MFA, insufficient ACLs, and unrestricted code execution can expose networks to significant risks.
- By enforcing best practices such as regular audits, strong password policies, application whitelisting, and network segmentation, organizations can mitigate these vulnerabilities.
- Proactive management and continuous monitoring are key to strengthening AD security and preventing breaches.

- CISA and NSA (2023, October 5). Cybersecurity Advisory: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations_. Cisa.gov. Retrieved July 8, 2024, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278aApplication Whitelisting

- Microsoft (2008, October 23). Microsoft Security Bulletin MS08-067 - Critical Vulnerability in Server Service Could Allow Remote Code Execution (958644). Microsoft.com. Retrieved July 8, 2024, from https://learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067

- GitHub:
  - https://github.com/theGh0stfaceKiller/Fortifying-Active-Directory-Combatting-Misconfigurations