CYBERSECURITY
ADVISORY

Authored by:

TLP:CLEAR

Product ID: AA23-349A

December 15, 2023

Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment

SUMMARY

In January 2023, the Cybersecurity and Infrastructure Security Agency (CISA) conducted a Risk and Vulnerability Assessment (RVA) at the request of a Healthcare and Public Health (HPH) sector organization to identify vulnerabilities and areas for improvement. An RVA is a two-week penetration test of an entire organization, with one week spent on external testing and one week spent assessing the internal network. As part of the RVA, the CISA assessment team conducted web application, phishing, penetration, database, and wireless assessments. The assessed organization was a large organization deploying on-premises software.

Actions to take today to harden your internal environment to mitigate follow-on activity after initial access.

- Use phishing-resistant multi-factor authentication (MFA) for all administrative access.
- Verify the implementation of appropriate hardening measures, and change, remove, or deactivate all default credentials.
- Implement network segregation controls.

During the one-week external assessment, the assessment team did not identify any significant or exploitable conditions in externally available systems that may allow a malicious actor to easily obtain initial access to the organization's network. Furthermore, the assessment team was unable to gain initial access to the assessed organization through phishing. However, during internal penetration testing, the team exploited misconfigurations, weak passwords, and other issues through multiple attack paths to compromise the organization's domain.

In coordination with the assessed organization, CISA is releasing this Cybersecurity Advisory (CSA) detailing the RVA team's activities and key findings to provide network defenders and software manufacturers recommendations for improving their organizations' and customers' cyber posture,

All organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

which reduces the impact of follow-on activity after initial access. CISA encourages the HPH sector and other critical infrastructure organizations deploying on-premises software, as well as software manufacturers, to apply the recommendations in the Mitigations section of this CSA to harden networks against malicious activity and to reduce the likelihood of domain compromise.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See the MITRE ATT&CK Tactics and Techniques section for tables of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques with corresponding mitigation and/or detection recommendations. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Introduction

CISA has authority to, upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and provide operational and timely technical assistance to federal and non-federal entities with respect to cybersecurity risks. *See generally* 6 U.S.C. §§ 652(c)(5), 659(c)(6). After receiving a request for an RVA from the organization and coordinating high-level details of the engagement with certain personnel at the organization, CISA conducted the RVA in January 2023.

During RVAs, CISA tests the security posture of an organization's network over a two-week period to determine the risk, vulnerability, and exploitability of systems and networks. During the first week (the external phase), the team tests public facing systems to identify exploitable vulnerabilities. During the second week (the internal phase), the team determines the susceptibility of the environment to an actor with internal access (e.g., malicious cyber actor or insider threat). The assessment team offers five services:

- **Web Application Assessment:** The assessment team uses commercial and open source tools to identify vulnerabilities in public-facing and internal web applications, demonstrating how they could be exploited.
- **Phishing Assessment:** The assessment team tests the susceptibility of staff and infrastructure to phishing attacks and determines what impact a phished user workstation could have on the internal network. The RVA team crafts compelling email pretexts and generates payloads, similar to ones used by threat actors, in order to provide a realistic threat perspective to the organization.
- **Penetration Testing:** The assessment team tests the security of an environment by simulating scenarios an advanced cyber actor may attempt. The team's goals are to establish a foothold, escalate privileges, and compromise the domain. The RVA team leverages both open source and commercial tools for host discovery, port and service mapping, vulnerability discovery and analysis, and vulnerability exploitation.
- **Database Assessment:** The assessment team uses commercial database tools to review databases for misconfigurations and missing patches.
- **Wireless Assessment:** The assessment team uses specialized wireless hardware to assess wireless access points, connected endpoints, and user awareness for vulnerabilities.

The assessed organization was in the HPH sector. See Table 1 for services in-scope for this RVA.

Table 1: In-Scope RVA Services

Phase	Scope	Services
External Assessment	Publicly available HPH-organization endpoints discovered during scanning	Penetration Testing Phishing Assessment Web Application Assessment
Internal Assessment	Internally available HPH-organization endpoints discovered during scanning	Database Assessment Penetration Testing Web Application Assessment Wireless Assessment

Phase I: External Assessment

Penetration and Web Application Testing

The CISA team did not identify any significant or exploitable conditions from penetration or web application testing that may allow a malicious actor to easily obtain initial access to the organization's network.

Phishing Assessment

The CISA team conducted phishing assessments that included both user and systems testing.

The team's phishing assessment was unsuccessful because the organization's defensive tools blocked the execution of the team's payloads. The payload testing resulted in most of the team's payloads being blocked by host-based protections through a combination of browser, policy, and antivirus software. Some of the payloads were successfully downloaded to disk without being immediately removed, but upon execution, the antivirus software detected the malicious code and blocked it from running. Some payloads appeared to successfully evade host-based protections but did not create a connection to the command and control (C2) infrastructure, indicating they may have been incompatible with the system or blocked by border protections.

Since none of the payloads successfully connected to the assessment team's C2 server, the team conducted a credential harvesting phishing campaign. Users were prompted to follow a malicious link within a phishing email under the pretext of verifying tax information and were then taken to a fake login form.

While twelve unique users from the organization submitted credentials through the malicious form, the CISA team was unable to leverage the credentials because they had limited access to external-facing resources. Additionally, the organization had multi-factor authentication (MFA) implemented for cloud accounts. **Note:** At the time of the assessment, the CISA team's operating procedures did not include certain machine-in-the-middle attacks that could have circumvented the form of MFA in place. However, it is important to note that tools like Evilginx[1] can be leveraged to bypass non-phishing resistant forms of MFA. Furthermore, if a user executes a malicious file, opening a connection to a malicious actor's command and control server, MFA will not prevent the actor from executing commands and carrying out actions under the context of that user.

Phase II: Internal Assessment

Database, Web Application, and Wireless Testing

The CISA assessment team did not identify any significant or exploitable conditions from database or wireless testing that may allow a malicious actor to easily compromise the confidentiality, integrity, and availability of the tested environment.

The team did identify default credentials [T1078.001] for multiple web interfaces during web application testing and used default printer credentials while penetration testing. (See the Attack Path 2 section for more information.)

Penetration Testing

The assessment team starts internal penetration testing with a connection to the organization's network but without a valid domain account. The team's goal is to compromise the domain by gaining domain admin or enterprise administrator-level permissions. Generally, the team first attempts to gain domain user access and then escalate privileges until the domain is compromised. This process is called the "attack path"—acquiring initial access to an organization and escalating privileges until the domain is compromised and/or vital assets for the organization are accessed. The attack path requires specialized expertise and is realistic to what adversaries may do in an environment.

For this assessment, the team compromised the organization's domain through four unique attack paths, and in a fifth attack path the team obtained access to sensitive information.

See the sections below for a description of the team's attack paths mapped to the MITRE ATT&CK for Enterprise framework. See the Findings section for information on issues that enabled the team to compromise the domain.

Attack Path 1

The assessment team initiated LLMNR/NBT-NS/mDNS/DHCP poisoning [T1557.001] with Responder[2], which works in two steps:

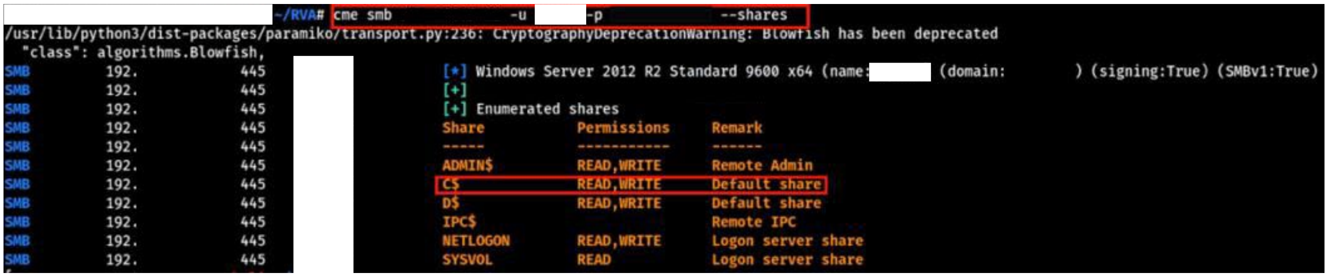
1. Responder listens to multicast name resolution queries (e.g., `LLMNR UDP/5355`, `NBTNS UDP/137`) [T1040] and under the right conditions spoofs a response to direct the victim host to a CISA-controlled machine on which Responder is running.
2. Once a victim connects to the machine, Responder exploits the connection to perform malicious functions such as stealing credentials or opening a session on a targeted host [T1021].

With this tool, the CISA team captured fifty-five New Technology Local Area Network Manager version 2 (NTLMv2) hashes, including the NTLMv2 hash for a service account. **Note:** NTLMv2 and other variations of the hash protocol are used for clients to join a domain, authenticate between Active Directory forests, authenticate between earlier versions of Windows operating systems (OSs), and authenticate computers that are not normally a part of the domain.[3] Cracking these passwords may enable malicious actors to establish a foothold in the domain and move laterally or elevate their privileges if the hash belongs to a privileged account.

The service account had a weak password, allowing the team to quickly crack it [T1110.002] and obtain access to the organization's domain. With domain access, the CISA assessment team enumerated accounts with a Service Principal Name (SPN) set [T1087.002]. SPN is the unique service identifier used by Kerberos authentication[4], and accounts with SPN are susceptible to Kerberoasting.

The CISA team used Impacket's[5] GetUserSPNs tool to request Ticket-Granting Service (TGS) tickets for all accounts with SPN set and obtained their Kerberos hashes [T1558.003]. Three of these accounts had domain administrator privileges—offline, the team cracked ACCOUNT 1 (which had a weak password).

Using CrackMapExec[6], the assessment team used ACCOUNT 1 [T1078.002] to successfully connect to a domain controller (DC). The team confirmed they compromised the domain because ACCOUNT 1 had `READ,WRITE` permissions over the `C$` administrative share [T1021.002] (see Figure 1).



```
[redacted]~/RVA# cme smb              -u [redacted] -p              --shares
/usr/lib/python3/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
SMB         192.            445    [redacted]       [*] Windows Server 2012 R2 Standard 9600 x64 (name:[redacted] (domain:        ) (signing:True) (SMBv1:True)
SMB         192.            445                     [+]
SMB         192.            445                     [+] Enumerated shares
SMB         192.            445                     Share           Permissions     Remark
SMB         192.            445                     -----           -----------     ------
SMB         192.            445                     ADMIN$          READ,WRITE      Remote Admin
SMB         192.            445                     C$              READ,WRITE      Default share
SMB         192.            445                     D$              READ,WRITE      Default share
SMB         192.            445                     IPC$                            Remote IPC
SMB         192.            445                     NETLOGON        READ,WRITE      Logon server share
SMB         192.            445                     SYSVOL          READ            Logon server share
```

Figure 1: ACCOUNT 1 Domain Admin Privileges

To further demonstrate the impact of compromising ACCOUNT 1, the assessment team used it to access a virtual machine interface. If a malicious actor compromised ACCOUNT 1, they could use it to modify, power off [T1529], and/or delete critical virtual machines, including domain controllers and file servers.

Attack Path 2

The team first mapped the network to identify open web ports [T1595.001], and then attempted to access various web interfaces [T1133] with default administrator credentials. The CISA team was able to log into a printer interface with a default password and found the device was configured with domain credentials to allow employees to save scanned documents to a network share [T1080].

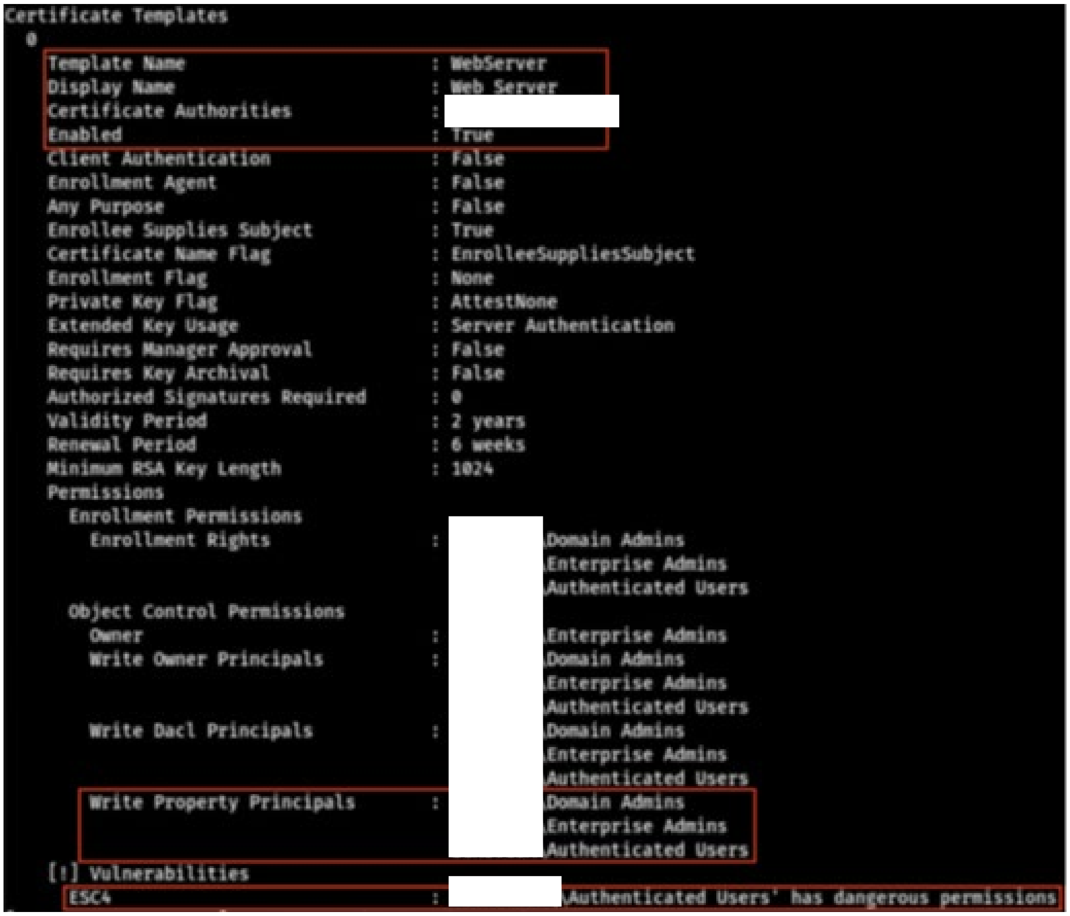
While logged into the printer interface as an administrator, the team 1) modified the "Save as file" configuration to use File Transfer Protocol (FTP) instead of Server Message Block (SMB) and 2) changed the Server Name and Network Path to point to a CISA-controlled machine running Responder [T1557]. Then, the team executed a "Connection Test" that sent the username and password over FTP [T1187] to the CISA machine running Responder, which captured cleartext credentials for a non-privileged domain account (ACCOUNT 2).

Using ACCOUNT 2 and Certipy[7], the team enumerated potential certificate template vulnerabilities found in Active Directory Certificate Services (ADCS). **Note:** ADCS templates are used to build certificates for different types of servers and other entities on an organization's network. Malicious actors can exploit template misconfigurations [T1649] to manipulate the certificate infrastructure into issuing fraudulent certificates and/or escalate user privileges to a domain administrator.

The `WebServer` template was misconfigured to allow all authenticated users permission to:

- Change the properties of the template (via `Object Control Permissions` with `Write Property Principals` set to `Authenticated Users`).
- Enroll for the certificate (via `Enrollment Permissions` including the `Authenticated Users` group).
- Request a certificate for a different user (via `EnrolleeSuppliesSubject` set as `True`).

See Figure 2 for the displayed certificate template misconfigurations.



```
Certificate Templates
  0
    Template Name                       : WebServer
    Display Name                        : Web Server
    Certificate Authorities             : [redacted]
    Enabled                             : True
    Client Authentication               : False
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : None
    Private Key Flag                    : AttestNone
    Extended Key Usage                  : Server Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 2 years
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 1024
    Permissions
      Enrollment Permissions
        Enrollment Rights               : [redacted]Domain Admins
                                                 Enterprise Admins
                                                 Authenticated Users

      Object Control Permissions
        Owner                           :        Enterprise Admins
        Write Owner Principals          :        Domain Admins
                                                 Enterprise Admins
                                                 Authenticated Users

        Write Dacl Principals           :        Domain Admins
                                                 Enterprise Admins
                                                 Authenticated Users

        Write Property Principals       :        Domain Admins
                                                 Enterprise Admins
                                                 Authenticated Users
    [!] Vulnerabilities
      ESC4                              : [redacted]Authenticated Users' has dangerous permissions
```

Figure 2: Misconfigured Certificate Template Enumerated via Certipy

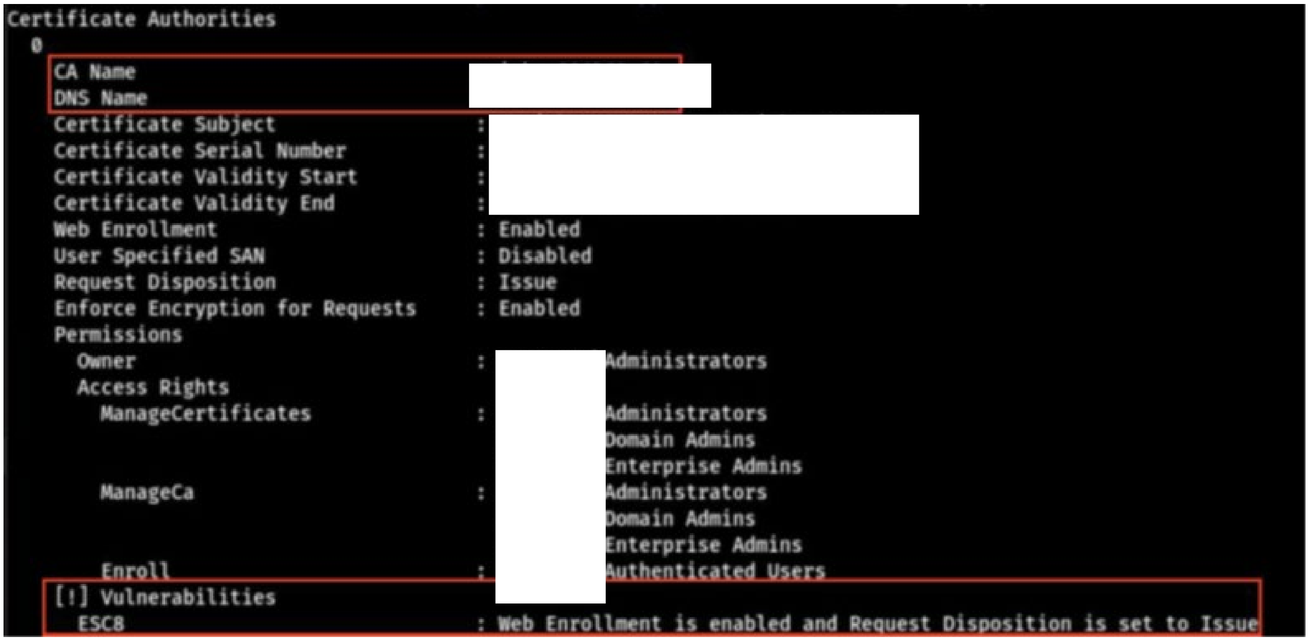
The template's `Client Authentication` was set to `False`, preventing the CISA assessment team from requesting a certificate that could be used to authenticate to a server in the domain. To demonstrate how this misconfiguration could lead to privilege escalation, the assessment team, leveraging its status as a mere authenticated user, briefly changed the `WebServer` template properties to set `Client Authentication` to `True` so that a certificate could be obtained for server authentication, ensuring the property was set back to its original setting of `False` immediately thereafter.

The team used Certipy with the ACCOUNT 2 credentials to request a certificate for a Domain Administrator account (ACCOUNT 3). The team then authenticated to the domain controller as ACCOUNT 3 with the generated certificate [T1550] and retrieved the NTLM hash for ACCOUNT 3 [T1003]. The team used the hash to authenticate to the domain controller [T1550.002] and validated Domain Administrator privileges, demonstrating compromise of the domain via the `WebServer` template misconfiguration.

Attack Path 3

The CISA team used a tool called CrackMapExec to spray easily guessable passwords [T1110.003] across all domain accounts and obtained two sets of valid credentials for standard domain user accounts.

The assessment team leveraged one of the domain user accounts (ACCOUNT 4) to enumerate ADCS via Certipy and found that web enrollment was enabled (see Figure 3). If web enrollment is enabled, malicious actors can abuse certain services and/or misconfigurations in the environment to coerce a server to authenticate to an actor-controlled computer, which can relay the authentication to the ADCS web enrollment service and obtain a certificate for the server's account (known as a relay attack).



```
Certificate Authorities
  0
    CA Name                             [redacted]
    DNS Name
    Certificate Subject               : [redacted]
    Certificate Serial Number         :
    Certificate Validity Start        :
    Certificate Validity End          :
    Web Enrollment                    : Enabled
    User Specified SAN                : Disabled
    Request Disposition               : Issue
    Enforce Encryption for Requests   : Enabled
    Permissions
      Owner                           : [redacted]Administrators
      Access Rights
        ManageCertificates            :           Administrators
                                                  Domain Admins
                                                  Enterprise Admins
        ManageCa                      :           Administrators
                                                  Domain Admins
                                                  Enterprise Admins
        Enroll                        :           Authenticated Users
    [!] Vulnerabilities
      ESC8                            : Web Enrollment is enabled and Request Disposition is set to Issue
```

Figure 3: Misconfigured ADCS Enumerated via Certipy

The team used PetitPotam [8] with ACCOUNT 4 credentials to force the organization's domain controller to authenticate to the CISA-operated machine and then used Certipy to relay the coerced authentication attempt to the ADCS web enrollment service to receive a valid certificate for

ACCOUNT 5, the domain controller machine account. They used this certificate to acquire a TGT [T1558] for ACCOUNT 5.

With the TGT for ACCOUNT 5, the CISA team used `DCSync` to dump the NTLM hash [T1003.006] for ACCOUNT 3 (a Domain Administrator account [see Attack Path 2 section]), effectively leading to domain compromise.

Attack Path 4

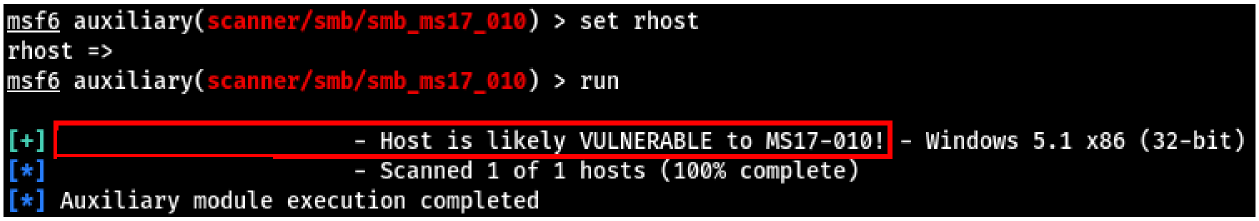
The CISA team identified several systems on the organization’s network that do not enforce SMB signing. The team exploited this misconfiguration to obtain cleartext credentials for two domain administrator accounts.

First, the team used Responder to capture the NTLMv2 hash for a domain administrator account. Next, they used Impacket’s NTLMrelayx tool[9] to relay the authentication for the domain administrator, opening a SOCKS connection on a host that did not enforce SMB signing. The team then used DonPAPI[10] to dump cleartext credentials through the SOCKS connection and obtained credentials for two additional domain administrator accounts.

The CISA team validated the privileges of these accounts by checking for `READ,WRITE` access on a domain controller `C$` share [T1039], demonstrating Domain Administrator access and therefore domain compromise.

Attack Path 5

The team did vulnerability scanning [T1046] and identified a server vulnerable to CVE-2017-0144 (an Improper Input Validation [CWE-20] vulnerability known as “EternalBlue” that affects SMB version 1 [SMBv1] and enables remote code execution [see Figure 4]).



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost
rhost =>
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+]                          - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*]                          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 4: Checking for EternalBlue Vulnerability

The CISA assessment team then executed a well-known EternalBlue exploit [T1210] and established a shell on the server. This shell allowed them to execute commands [T1059.003] under the context of the local `SYSTEM` account.

With this local `SYSTEM` account, CISA dumped password hashes from a Security Account Manager (SAM) database [T1003.002]. The team parsed the hashes and identified one for a local administrator account. Upon parsing the contents of the SAM database dump, the CISA team identified an NTLM hash for the local administrator account, which can be used to authenticate to various services.

The team sprayed the acquired NTLM hash across a network segment and identified multiple instances of password reuse allowing the team to access various resources including sensitive information with the hash.

Findings

Key Issues

The CISA assessments team identified several findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Each finding, listed below, includes a description with supporting details. See the Mitigations section for recommendations on how to mitigate these issues.

The CISA team rated their findings on a severity scale from critical to informational (see Table 2).

Table 2: Severity Rating Criteria

Severity	Description
Critical	Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploitation and potential impact. Critical items are reported to the customer immediately.
High	Malicious actors may be able to exercise full control on the targeted device.
Medium	Malicious actors may be able to exercise some control of the targeted device.
Low	The vulnerabilities discovered are reported as items of interest but are not normally exploitable. Many low items reported by security tools are not included in this report because they are often informational, unverified, or of minor risk.
Informational	These vulnerabilities are potential weaknesses within the system that cannot be readily exploited. These findings represent areas that the customer should be cognizant of, but do not require any immediate action.

The CISA assessment team identified four High severity vulnerabilities and one Medium severity vulnerability during penetration testing that contributed to the team's ability to compromise the domain. See Table 3 for a list and description of these findings.

Table 3: Key Issues Contributing to Domain Compromise

Issue	Severity	Service	Description
Poor Credential Hygiene: Easily Crackable Passwords	High	Penetration Testing	As part of their assessment, the team reviewed the organization's domain password policy and found it was weak because the minimum password length was

Issue	Severity	Service	Description
			set to 8 characters. Passwords less than 15 characters without randomness are easily crackable, and malicious actors with minimal technical knowledge can use these credentials to access the related services. The assessment team was able to easily crack many passwords throughout the assessment to move laterally and increase access within the domain. Specifically, the team: • Cracked the NTLMv2 hash for a domain account, and subsequently accessed the domain. (See the Attack Path 1 section.) Cracked the password hash (obtained via Kerberoasting) of a domain administrator account and subsequently compromised the domain. (See the Attack Path 1 section.)
Poor Credential Hygiene: Guessable Credentials	High	Penetration Testing	As part of the penetration test, the assessment team tested to see if one or more services is accessible using a list of enumerated usernames alongside an easily guessed password. The objective is to see if a malicious actor with minimal technical knowledge can use these credentials to access the related services, enabling them to move laterally or escalate privileges. Easily guessable passwords are often comprised of common words, seasons, months and/or years, and are sometimes combined with special characters. Additionally, phrases or names that are popular locally (such as the organization being tested or a local sports teams) may also be considered easily guessable. The team sprayed common passwords against domain user accounts and obtained valid credentials for standard domain users.

Issue	Severity	Service	Description
			(See the Attack Path 3 section.) (Cracking was not necessary for this attack.)
Misconfigured ADCS Certificate Templates	High	Penetration Testing	The team identified a `WebServer` template configured to allow all authenticated users permission to change the properties of the template and obtain certificates for different users. The team exploited the template to acquire a certificate for a Domain Administrator account (see the Attack Path 2 section).
Unnecessary Network Services Enabled	High	Penetration Testing	Malicious actors can exploit security vulnerabilities and misconfigurations in network services, especially legacy services. The assessment team identified legacy name resolution protocols (e.g., NetBIOS, LLMNR, mDNS) enabled in the network, and abused LLMNR to capture NTLMv2 hashes, which they then cracked and used for domain access. (See the Attack Path 1 section.) The team also identified an ADCS server with web enrollment enabled and leveraged it to compromise the domain through coercion and relaying. (See Attack Path 3 section.) Additionally, the team identified hosts with `WebClient` and Spooler services, which are often abused by malicious actors to coerce authentication.
Elevated Service Account Privileges	High	Penetration Testing	Applications often require user accounts to operate. These user accounts, which are known as service accounts, often require elevated privileges. If an application or service running with a service account is compromised, an actor may have the same privileges and access as the service account.

Issue	Severity	Service	Description
			The CISA team identified a service account with Domain Administrator privileges and used it to access the domain after cracking its password (See the Attack Path 1 section).
SMB Signing Not Enabled	High	Penetration Testing	The CISA team identified several systems on the organization's network that do not enforce SMB signing and exploited this for relayed authentication to obtain cleartext credentials for two domain administrator accounts.
Insecure Default Configuration: Default Credentials	Medium	Web Application Assessment	Many off-the-shelf applications are released with built-in administrative accounts using predefined credentials that can often be found with a simple web search. Malicious actors with minimal technical knowledge can use these credentials to access the related services. During testing, the CISA team identified multiple web interfaces with default administrator credentials and used default credentials for a printer interface to capture domain credentials of a non-privileged domain account. (See the Attack Path 2 section.)

In addition to the issues listed above, the team identified three High and seven Medium severity findings. These vulnerabilities and misconfigurations may allow a malicious actor to compromise the confidentiality, integrity, and availability of the tested environment. See Table 4 for a list and description of these findings.

Table 4: Additional Key Issues

Issue	Severity	Service	Description
Poor Credential Hygiene: Password Reuse for Administrator and User Accounts	High	Penetration Testing	Elevated password reuse is when an administrator uses the same password for their user and administrator accounts. If the user account password is compromised, it can be used to gain access to the administrative account.

Issue	Severity	Service	Description
			The assessment team identified an instance where the same password was set for an admin user's administrative account as well as their standard user account.
Poor Credential Hygiene: Password Reuse for Administrator Accounts	Medium	Penetration Testing	If administrator passwords are the same for various administrator accounts, malicious actors can use the password to access all systems that share this credential after compromising one account. The assessment team found multiple instances of local administrator accounts across various systems using the same password.
Poor Patch Management: Out-of-Date Software	High	Penetration Testing	Patches and updates are released to address existing and emerging security vulnerabilities, and failure to apply the latest leaves systems open to attack with publicly available exploits. (The risk presented by missing patches and updates depends on the severity of the vulnerability). The assessment team identified several unpatched systems including instances of CVE-2019-0708 (known as "BlueKeep") and EternalBlue. The team was unable to successfully compromise the systems with BlueKeep, but they did exploit EternalBlue on a server to implant a shell on a server with local `SYSTEM` privileges (see the Attack Path 5 section).
Poor Patch Management: Unsupported OS or Application	High	Penetration Testing	Using software or hardware that is no longer supported by the vendor poses a significant security risk because new and existing vulnerabilities are no longer patched). There is no way to address security vulnerabilities on these devices to ensure that they are secure. The overall security posture of the entire network is at risk because an attacker can target these

Issue	Severity	Service	Description
			devices to establish an initial foothold into the network. The assessment team identified end-of-life (EOL) Windows Server 2008 R2 and Windows Server 2008 and Windows 5.1.
Use of Weak Authentication Measures	Medium	Penetration Testing	Applications may have weak or broken mechanisms to verify user identity before granting user access to protected functionalities. Malicious actors can exploit these to bypass authentication and gain access to use application resources and functionality. The assessment team abused the Cisco Smart Install protocol to obtain configuration files for several Cisco devices on the organization's network. These files contained encrypted Cisco passwords. (The CISA team was unable to crack these passwords within the assessment timeframe.)
PII Disclosure	Medium	Penetration Testing	The assessment team identified an unencrypted Excel file containing PII on a file share.
Hosts with `Unconstrained Delegation` Enabled Unnecessarily	Medium	Penetration Testing	The CISA team identified two systems that appeared to be configured with `Unconstrained Delegation` enabled. Hosts with `Unconstrained Delegation` enabled store the Kerberos TGTs of all users that authenticate to that host, enabling actors to steal service tickets or compromise krbtgt accounts and perform golden ticket or silver ticket attacks. Although the assessment team was unable to fully exploit this configuration because they lost access to one of the vulnerable hosts, it could have led to domain compromise under the right circumstances.

Issue	Severity	Service	Description
Cleartext Password Disclosure	Medium	Penetration Testing	Storing passwords in cleartext is a security risk because malicious actors with access to these files can use them. The assessment team identified several unencrypted files on a file share containing passwords for various personal and organizational accounts.
Insecure File Shares	Medium	Penetration Testing	Access to sensitive data (e.g., data related to business functions, IT functions, and/or personnel) should be restricted to only certain authenticated and authorized users. The assessment team found an unsecured directory on a file share with sensitive IT information. The directory was accessible to all users in the domain group. Malicious actors with user privileges could access and/or exfiltrate this data.

Additional Issues

The CISA team identified one Informational severity within the organization's networks and systems. These issues may allow a malicious actor to compromise the confidentiality, integrity, and availability of the tested environment, but are not readily exploitable. The information provided is to encourage the stakeholder to investigate these issues further to adjust their environments or eliminate certain aspects as needed, but the urgency is low.

Table 5: Informational Issues That CISA Team Noted

Issue	Severity	Service	Description
Overly Permissive Accounts	Informational	Penetration Testing	Account privileges are intended to control user access to host or application resources to limit access to sensitive information in support of a least-privilege security model. When user (or other) accounts have high privileges, users can see and/or do things they normally should not, and malicious actors can exploit this to access host and application resources. The assessment team identified Active Directory objects where the `Human Resources` group appeared to be part of the

Issue	Severity	Service	Description
			privileged `Account Operators` group. This may have provided elevated privileges to accounts in the `Human Resources` group. (The CISA team was unable to validate and demonstrate the potential impact of this relationship within the assessment period).

Noted Strengths

The CISA team noted the following business, technical, and administrative components that enhanced the network security posture of the tested environment:

- The organization’s network was found to have several strong, security-oriented characteristics such as:
  - Effective antivirus software;
  - Endpoint detection and response capabilities;
  - Good policies and best practices for protecting users from malicious files including not allowing users to mount ISO files;
  - Minimal external attack surface, limiting an adversary’s ability to leverage external vulnerabilities to gain initial access to the organization’s networks and systems;
  - Strong wireless protocols;
  - And network segmentation.
- The organization’s security also demonstrated their ability to detect some of the CISA team's actions throughout testing and overall situational awareness through the use of logs and alerts.
- The organization used MFA for cloud accounts. The assessment team obtained cloud credentials via a phishing campaign but was unable to use them because of MFA prompts.

MITIGATIONS

Network Defenders

CISA recommends HPH Sector and other critical infrastructure organizations implement the mitigations in Table 6 to mitigate the issues listed in the Findings section of this advisory. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA’s Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

Table 6: Recommendations to Mitigate Identified Issues

Issue	Recommendation
Poor Credential Hygiene: Easily Crackable Passwords	• **Follow National Institute of Standards and Technologies (NIST) guidelines when creating password policies** to enforce use of "strong" passwords that cannot be cracked [CPG 2.B].[11] Consider using password managers to generate and store passwords. • **Use "strong" passphrases for private keys** to make cracking resource intensive [CPG 2.B]. Do not store credentials within the registry in Windows systems. Establish an organizational policy that prohibits password storage in files. • **Ensure adequate password length (ideally 15+ characters) and complexity requirements for Windows service accounts** and implement passwords with periodic expiration on these accounts [CPG 2.B]. Use Managed Service Accounts, when possible, to manage service account passwords automatically.
Poor Credential Hygiene: Guessable Credentials	• **Do not reuse local administrator account passwords across systems**. Ensure that passwords are "strong" and unique [CPG 2.C]. • **Use phishing-resistant multi-factor authentication (MFA) for all administrative access**, including domain administrative access [CPG 2.H]. If an organization that uses mobile push-notification-based MFA is unable to implement phishing-resistant MFA, use number matching to mitigate MFA fatigue. For more information, see CISA fact sheets on Implementing Phishing-Resistant MFA and Implementing Number Matching in MFA Applications.
Misconfigured ADCS Certificate Templates	• **Restrict enrollment rights in templates to only those users or groups that require it**. Remove the `Enrollee Supplies Subject` flag from templates if it is not necessary or enforce manager approval if required. Consider removing `Write Owner`, `Write DACL` and `Write Property` permissions from low-privilege groups, such as `Authenticated Users` where those permissions are not needed.
Unnecessary Network Services Enabled	• **Ensure that only ports, protocols, and services with validated business needs are running on each system**. Disable deprecated protocols (including NetBIOS, LLMNR, and mDNS) on the network that are not strictly necessary for business functions, or limit the systems and services that use the protocol, where possible [CPG 2.W].

Issue	Recommendation
	• **Disable the `WebClient` and Spooler services** where possible to minimize risk of coerced authentication. • **Disable ADCS web-enrollment services**. If this service cannot be disabled, disable NTLM authentication to prevent malicious actors from performing NTLM relay attacks or abusing the Spooler and `WebClient` services to coerce and relay authentication to the web-enrollment service.
Elevated Service Account Privileges	• **Run daemon applications using a non-Administrator account** when appropriate. • **Configure Service accounts with only the permissions necessary for the services they operate**. • To mitigate Kerberoasting attacks, **use AES or stronger encryption** instead of RC4 for Kerberos hashes [CPG 2.K]. RC4 is considered weak encryption.
SMB Signing Not Enabled	• **Require SMB signing for both SMB client and server on all systems** to prevent certain adversary-in-the-middle and pass-the-hash attacks. See Microsoft's Overview of Server Message Block signing for more information.
Insecure Default Configuration: Default Credentials	• **Verify the implementation of appropriate hardening measures, and change, remove, or deactivate all default credentials** [CPG 2.A]. • Before deploying any new devices in a networked environment, **change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems** to have values consistent with administration-level accounts [CPG 2.A].
Poor Credential Hygiene: Password Reuse for Administrator and User Accounts	• **Discontinue reuse or sharing of administrative credentials** among user/administrative accounts [CPG 2.C]. • **Use unique credentials across workstations**, when possible, in accordance with applicable federal standards, industry best practices, and/or agency-defined requirements. • **Train users, especially privileged users, against password reuse** [CPG 2.I].
Poor Credential Hygiene: Password Reuse for Administrator Accounts	• **Discontinue reuse or sharing of administrative credentials among systems** [CPG 2.C]. When possible, use unique credentials across all workstations in accordance with applicable federal standards, industry best practices, and/or agency-defined requirements.

Issue	Recommendation
	• **Implement a security awareness program** that focuses on the methods commonly used in intrusions that can be blocked through individual action [CPG 2.I]. • **Implement Local Administrator Password Solution (LAPS)** where possible if your OS is older than Windows Server 2019 and Windows 10 as these versions do not have LAPS built in. **Note:** The authoring organizations recommend organizations upgrade to Windows Server 2019 and Windows 10 or greater.
Poor Patch Management: Out-of-Date Software	• **Enforce consistent patch management** across all systems and hosts within the network environment [CPG 1.E]. • Where patching is not possible due to limitations, **implement network segregation controls** [CPG 2.F] to limit exposure of the vulnerable system or host. • **Consider deploying automated patch management tools and software update tools** for operating system and software/applications on all systems for which such tools are available and safe.
Poor Patch Management: Unsupported OS or Application	• **Evaluate the use of unsupported hardware and software and discontinue** where possible. If discontinuing the use of unsupported hardware and software is not possible, implement additional network protections to mitigate the risk.
Use of Weak Authentication Measures	• **Require phishing-resistant MFA for all user accounts that have access to sensitive data or systems**. If MFA is not possible, it is recommended to, at a minimum, configure a more secure password policy by aligning with guidelines put forth by trusted entities such as NIST [CPG 2.H].
PII Disclosure	• **Implement a process to review files and systems for insecure handling of PII** [CPG 2.L]. Properly secure or remove the information. Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in cleartext. • **Encrypt PII and other sensitive data**, and train users who handle sensitive data to utilize best practices for encrypting data and storing it securely. If sensitive data must be stored on shares or other locations, restrict access to these locations as much as possible through access controls and network segmentation [CPG 2.F, 2.K, 2.L].

Issue	Recommendation
Hosts with `Unconstrained Delegation` Enabled Unnecessarily	• **Remove `Unconstrained Delegation` from all servers**. If `Unconstrained Delegation` functionality is required, upgrade operating systems and applications to leverage other approaches (e.g., configure `Constrained Delegation`, enable the `Account is sensitive and cannot be delegated` option) or explore whether systems can be retired or further isolated from the enterprise. CISA recommends Windows Server 2019 or greater.
Cleartext Password Disclosure	• **Implement a review process for files and systems to look for cleartext account credentials**. When credentials are found, remove or change them to maintain security [CPG 2.L]. • **Conduct periodic scans of server machines using automated tools to determine whether sensitive data** (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in cleartext. Consider implementing a secure password manager solution in cases where passwords need to be stored [CPG 2.L].
Insecure File Shares	• **Restrict access to file shares containing sensitive data** to only certain authenticated and authorized users [CPG 2.L].

Additionally, CISA recommends that HPH sector organizations implement the following strategies to mitigate cyber threats:

- **Mitigation Strategy #1 Asset Management and Security:**
  - CISA recommends that HPH sector organizations implement and maintain an asset management policy to reduce the risk of exposing vulnerabilities, devices, or services that could be exploited by threat actors to gain unauthorized access, steal sensitive data, or disrupt critical services. The focus areas for this mitigation strategy include asset management and asset security, addressing asset inventory, procurement, decommissioning, and network segmentation as they relate to hardware, software, and data assets.
- **Mitigation Strategy #2 Identity Management and Device Security:**
  - CISA recommends entities secure their devices and digital accounts and manage their online access to protect sensitive data and PII/PHI from compromise. The focus areas for this mitigation strategy include email security, phising prevention, access management, password policies, data protection and loss prevention, and device logs and monitoring solutions.
- **Mitigation Strategy #3 Vulnerability, Patch, and Configuration Management:**
  - CISA recommends entities mitigate known vulnerabilities and establish secure configuration baselines to reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks. The focus areas for this mitigation

strategy include vulnerability and patch Management, and configuration and change management.

For more information on these mitigations strategies, see CISA's Healthcare and Public Health Sector webpage.

Software Manufacturers

The above mitigations apply to HPH sector and other critical infrastructure organizations with on-premises or hybrid environments. Recognizing that insecure software is the root cause of the majority of these flaws, and that the responsibility should not be on the end user, CISA urges software manufacturers to implement the following to reduce the prevalence of misconfigurations, weak passwords, and other weaknesses identified and exploited through the assessment team:

- **Embed security into product architecture throughout the entire** software development lifecycle (SDLC).
- **Eliminate default passwords**. Do not provide software with default passwords. To eliminate default passwords, require administrators set a "strong" password [CPG 2.B] during installation and configuration.
- **Create secure configuration templates**. Provide configuration templates with certain safe settings based on an organization's risk appetite (e.g., low, medium, and high security templates). Support these templates with hardening guides based on the risks the manufacturer has identified. The default configuration should be a secure one, and organizations should need to opt in if they desire a less secure configuration.
- **Design products so that the compromise of a single security control does not result in compromise of the entire system**. For example, narrowly provision user privileges by default and employ ACLs to reduce the impact of a compromised account. This will make it more difficult for a malicious cyber actor to escalate privileges and move laterally.
- **Mandate MFA, ideally phishing-resistant MFA, for privileged users** and make MFA a default, rather than opt-in, feature.

These mitigations align with tactics provided in the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. CISA urges software manufacturers to take ownership of improving the security outcomes of their customers by applying these and other secure by design tactics. By using secure by design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing security software and logs, monitoring, and making routine updates.

For more information on secure by design, see CISA's Secure by Design webpage. For more information on common misconfigurations and guidance on reducing their prevalence, see the joint advisory NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations.

VALIDATE SECURITY CONTROLS

In addition to applying the listed mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for

Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 7 – 16).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- For consolidated findings from the RVAs by Fiscal Year mapped to MITRE ATT&CK, see CISA's Risk and Vulnerability Assessments page.
- See joint CSA NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations for information on the most common cybersecurity misconfigurations in large organizations and TTPs actors use to exploit these misconfigurations.
- See CISA's Healthcare and Public Health Sector webpage.
- See CISA's RedEye tool on CISA's GitHub page. RedEye is an interactive open-source analytic tool used to visualize and report red team command and control activities. See CISA's RedEye tool overview video for more information.

REFERENCES

[1] Github | kgretzky / evilginx

[2] Github | lgandx / Responder

[3] Network security LAN Manager authentication level - Windows Security | Microsoft Learn

[4] Service principal names - Win32 apps | Microsoft Learn

[5] Github | fortra / impacket

[6] Github | byt3bl33d3r / CrackMapExec

[7] Github | ly4k / Certipy

[8] Github | topotam / PetitPotam

[9] Github | fortra / impacket / examples

[10] Github | login-securite / DonPAPI

[11] SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management | CSRC (nist.gov)

APPENDIX: MITRE ATT&CK TACTICS AND TECHNIQUES

Table 7: CISA Team ATT&CK Techniques for Reconnaissance

Reconnaissance		
Technique Title	**ID**	**Use**
Active Scanning: Scanning IP Blocks	T1595.001	The CISA team first mapped the network to identify open web ports.

See Table 8 – 16 for all referenced threat actor tactics and techniques in this advisory.

Table 8: CISA Team ATT&CK Techniques for Initial Access

Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts: Default Accounts	T1078.001	The CISA team did identify default credentials for multiple web interfaces during web application testing and used default printer credentials while penetration testing.
External Remote Services	T1133	The CISA team attempted to access various web interfaces with default administrator credentials.

Table 9: CISA Team ATT&CK Techniques for Execution

Execution		
Technique Title	**ID**	**Use**
Command-Line Interface	T1059	The CISA team accessed a virtual machine interface enabling them to modify, power off, and/or delete critical virtual machines including domain controllers, file servers, and servers.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	The CISA team used a webshell that allowed them to execute commands under the context of the local `SYSTEM` account.

Table 10: CISA Team ATT&CK Techniques for Privilege Escalation

Privilege Escalation		
Technique Title	**ID**	**Use**
Valid Accounts: Domain Accounts	T1078.002	The CISA team used CrackMapExec to use ACCOUNT 1 to successfully connect to a domain controller (DC).

Table 11: CISA Team ATT&CK Techniques for Defense Evasion

Defense Evasion		
Technique Title	**ID**	**Use**
Use Alternate Authentication Material	T1550	The CISA team authenticated to the domain controller as ACCOUNT 3 with the generated certificate.

Table 12: CISA Team ATT&CK Techniques for Credential Access

Credential Access		
Technique Title	**ID**	**Use**
LLMNR/NBT-NS Poisoning and Relay	T1557.001	The CISA team initiated a LLMNR/NBT-NS/mDNS/DHCP poisoning tool to spoof a connection to the organization’s server for forced access.
Brute Force: Password Cracking	T1110.002	The CISA team cracked a service account with a weak password, giving them access to it.
Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	The CISA team gained access to domain accounts because any domain user can request a TGS ticket for domain accounts.
Adversary-in-the-Middle	T1557	The CISA team modified the “Save as file” configuration, to use File Transfer Protocol (FTP) instead of Server Message Block (SMB) and changed the Server Name and Network Path to point to a CISA-controlled machine running Responder.

Forced Authentication	T1187	The CISA team executed a “Connection Test” that sent the username and password over FTP.
Steal or Forge Authentication Certificates	T1649	The CISA team used `Certipy` to enumerate the ADCS certificate template vulnerabilities, allowing them to obtain certificates for different users.
OS Credential Dumping	T1003	The CISA team retrieved the NTLM hash for ACCOUNT 3.
Use Alternate Authentication Material: Pass the Hash	T1550.002	The CISA team used the hash to authenticate to the domain controller and validated Domain Administrator privileges, demonstrating compromise of the domain.
Brute Force: Password Spraying	T1110.003	The CISA team used a tool called `CrackMapExec` to spray easily guessable passwords across all domain accounts, giving them two sets of valid credentials.
Steal or Forge Kerberos Tickets	T1558	The CISA team used this certificate to acquire a TGT for ACCOUNT 5.
OS Credential Dumping: DCSync	T1003.006	The CISA team used `DCSync` to dump the NTLM hash for ACCOUNT 3 (a Domain Administrator account), effectively leading to domain compromise.
OS Credential Dumping: Security Account Manager	T1003.002	The CISA team dumped password hashes from a Security Account Manager (SAM) database.

Table 13: CISA Team ATT&CK Techniques for Discovery

Discovery		
Technique Title	**ID**	**Use**
Network Sniffing	T1040	The CISA team spoofed a response to direct the victim host to a CISA-controlled machine on which Responder is running.

Account Discovery: Domain Account	T1087.002	The CISA team enumerated accounts with a Service Principal Name (SPN) set with their domain access.
Network Service Scanning	T1046	The CISA team canned the organization’s network to identify open web ports to see where they could leverage the default credentials they had.

Table 14: CISA Team ATT&CK Techniques for Lateral Movement

Lateral Movement		
Technique Title	**ID**	**Use**
Remote Services	T1021	The CISA team exploited its Responder to perform malicious functions, such as stealing credentials or opening a session on a targeted host.
SMB/Windows Admin Shares	T1021.002	The CISA team confirmed they compromised the domain because ACCOUNT 1 had `READ,WRITE` permissions over the `C$` administrative share.
Taint Shared Content	T1080	The CISA team found the device was configured with domain credentials to allow employees to save scanned documents to a network share.
Exploitation of Remote Services	T1210	The CISA team then executed a well-known EternalBlue exploit and established a shell on the server.

Table 15: CISA Team ATT&CK Techniques for Collection

Collection		
Technique Title	**ID**	**Use**
Data from Network Shared Drive	T1039	The CISA team obtained credentials for cleartext, hashes, and from files.

Table 16: CISA Team ATT&CK Techniques for Impact

Collection		
Technique Title	**ID**	**Use**
System Shutdown/Reboot	T1529	The CISA team assessed that with ACCOUNT 1, they could use it to modify, power off, and/or delete critical virtual machines, including domain controllers and file servers.

VERSION HISTORY

December 14, 2023: Initial version.