Penetration Test Report

Sample Pentest

Friday, October 28th 2022

NOTE: This document may contain information that is potentially sensitive in-nature, including personally identifiable information. Use discretion when sharing this document with any other parties. The information contained herein is protected and is considered proprietary information.

Airiam

Email: info@airiam.com
Website: www.airiam.com

Table of contents

1. Executive Summary

On **Tuesday, November 2, 2021**, **Airiam** conducted an autonomous penetration test ("pentest")**.**

Airiam AI's Autonomous Penetration Testing as a Service (APTaaS) uses a mix of industry-standard and proprietary attack techniques to discover and validate exploitable vulnerabilities within the target network. Continuous pentesting helps network administrators address key security questions about their environment:

- Are my “crown jewels” systems and data secure?
- What urgent issues must I remediate immediately?
- How should I prioritize my vulnerabilities and other defensive efforts?
- Are detection & remediation times improving?
- Are my security tools and procedures effective?
- Am I lowering the impact risk of a cyber attack?

1.1. Overview

The pentest was launched on November 2, 2021 04:31 PM**.** It completed on November 2, 2021 06:16 PM, for a total duration of **1 hour, 44 minutes and 34 seconds**.

Installed and launched on host **10.0.220.50**. From there it scanned **22 hosts** in the following subnets:

- **Included subnets:**
  10.0.220.0/24, 10.0.225.0/24, 10.0.229.0/24, 10.0.100.96/28, 10.0.50.2, 10.0.40.99, 10.0.40.56, 10.0.40.103
- **Excluded subnets:**
  10.0.225.101, 10.0.220.53, 10.0.220.56

It discovered an additional **22 hosts** that were out of scope. No action was taken on these hosts.

1.2. Impact Summary

The pentest identified critical impacts that require immediate attention. These impacts represent critical vulnerabilities that can be leveraged by an attacker to compromise your network.

Domain Compromise (1)

Compromised 1 domain via 4 separate attack vectors

- Domain SMOKE.NET

Domain User Compromise (7)

Compromised 7 domain users

The top 5 are listed below.

- Domain Admin administrator on domain SMOKE.NET
- Domain Admin a-jsmith on domain SMOKE.NET
- Domain User nsunkavally on domain SMOKE.NET
- Domain User ns$ on domain SMOKE.NET
- Domain User svc_TESTGMSA2$ on domain SMOKE.NET

Host Compromise (14)

Compromised 14 hosts via 40 separate attack vectors

The top 5 are listed below.

- Host 10.0.220.55 (win2k3)
- Domain Controller 10.0.229.1 (dc.smoke.net)
- Host 10.0.220.54 (winxp)
- Host 10.0.40.99 (vcsa.smoke.net)
- Host 10.0.225.100

Ransomware Exposure (8)

Ransomware exposure on 8 stores via 24 separate attack vectors

The top 5 are listed below.

- Domain Controller 10.0.229.1 (dc.smoke.net)
- Host 10.0.40.99 (vcsa.smoke.net)
- Host 10.0.229.11 (fs.smoke.net)
- Host 10.0.225.2 (ns.smoke.net)

- Host 10.0.220.55 (win2k3)

Sensitive Data Exposure (13)

Compromised sensitive data on 13 stores via 21 separate attack vectors

The top 5 are listed below.

- Domain Controller 10.0.229.1 (dc.smoke.net)
- Host 10.0.229.11 (fs.smoke.net)
- Host 10.0.225.2 (ns.smoke.net)
- Host 10.0.220.55 (win2k3)
- Host 10.0.220.52 (win10.smoke.net)

Critical Infrastructure Compromise (5)

Compromised 5 critical applications or devices via 6 separate attack vectors

- Jenkins application at 10.0.225.100:8080
- LDAP service at 10.0.40.99:389
- Smart Install service at 10.0.220.254:4786
- Smart Install service at 10.0.229.254:4786
- Web service at 10.0.40.99:443

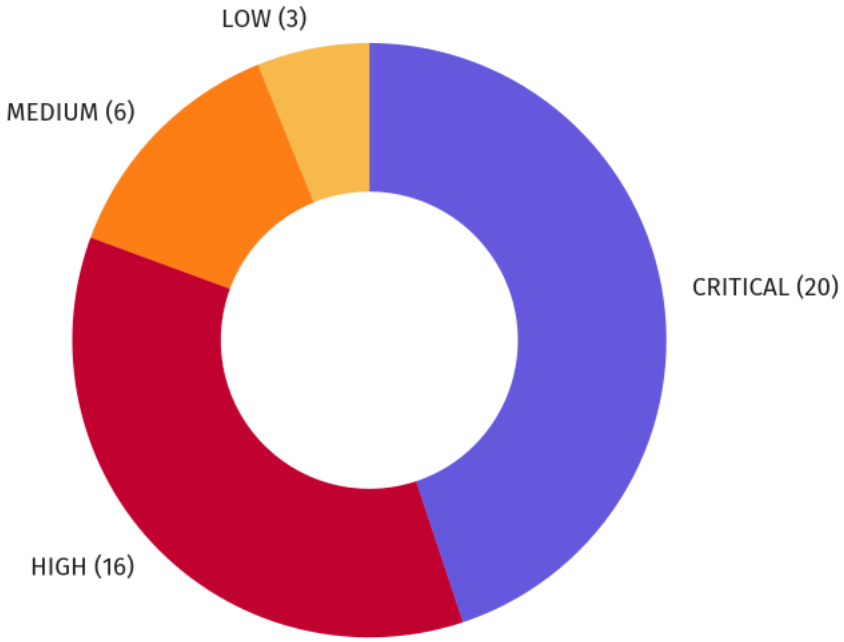
Brand Compromise (1)

Compromised 1 subdomain

- Subdomain doodle.h3ai.io

1.3. Weaknesses & Mitigations

The pentest identified CRITICAL degrees of risk within the target network, including **39 confirmed weaknesses** and **6 potential weaknesses.** These risks allow an attacker to steal data, disrupt operations, and cause financial or reputational loss.



Weaknesses by Severity

The following weaknesses were identified as having the highest degree of risk. Each weakness includes recommended mitigations and remediations.

The top 5 are listed below.

1. CRITICAL Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144, affecting 5 hosts)

   Apply the updates referenced in Microsoft Security Bulletin MS17-010.

   Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet. If at all possible disable SMBv1

2. CRITICAL Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472, affecting 1 host)

   Apply the updates referenced in Microsoft Security Bulletin CVE-2020-1472 and configure the registry key that will enable Enforcement Mode.

   On February 9, 2021 a Windows Update will automatically enable Enforcement Mode on all Domain Controllers regardless of the registry key value.

3. CRITICAL SMB Signing Not Required (H3-2021-0030, affecting 7 hosts)

   Enable and require SMB signing via Group Policy or Local Security Policy.

4. CRITICAL Credential Reuse (H3-2021-0032, affecting 5 hosts)

   Update the password to be unique and ensure it follows current password guidelines.

5. CRITICAL Server Service Vulnerability (CVE-2008-4250, affecting 2 hosts)

   Apply the updates referenced in Microsoft Security Bulletin MS08-067.

Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet.

2. Findings

2.1. Impact Details

2.1.1. Domain Compromise (1)

Compromised 1 domain via 4 separate attack vectors

Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.

Severity: CRITICAL

Domain SMOKE.NET	• Domain Admin a-jsmith on domain SMOKE.NET • Domain Admin administrator on domain SMOKE.NET • Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) found on Domain Controller 10.0.229.1 (dc.smoke.net) • Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) found on Domain Controller 10.0.229.1 (dc.smoke.net)

2.1.2. Domain User Compromise (7)

Compromised 7 domain users

Once a domain user is compromised, anything that user account has access to should be considered compromised.

Severity: CRITICAL

Domain Admin administrator	• Domain Admin administrator on domain SMOKE.NET
Domain Admin a-jsmith	• Domain Admin a-jsmith on domain SMOKE.NET
Domain User fs$	• Domain User fs$ on domain SMOKE.NET
Domain User jsmith	• Domain User jsmith on domain SMOKE.NET
Domain User ns$	• Domain User ns$ on domain SMOKE.NET

Domain User nsunkavally	• Domain User nsunkavally on domain SMOKE.NET
Domain User svc_TESTGMSA2$	• Domain User svc_TESTGMSA2$ on domain SMOKE.NET

2.1.3. Host Compromise (14)

Compromised 14 hosts via 40 separate attack vectors

Host compromise can lead to attackers gaining access to sensitive information, maintaining persistence within your network, and obtaining lateral movement within your networks.

Severity: CRITICAL

Host 10.0.220.55 (win2k3)	• Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.220.55:445 • Server Service Vulnerability (CVE-2008-4250) affecting SMB service at 10.0.220.55:445 • SMB service at 10.0.220.55:445 accessed by credential iwam_win2k3 • SMB service at 10.0.220.55:445 accessed by credential aspnet • SMB service at 10.0.220.55:445 accessed by credential iusr_win2k3 • SMB service at 10.0.220.55:445 accessed by credential administrator
Domain Controller 10.0.229.1 (dc.smoke.net)	• Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472) affecting SMB service at 10.0.229.1:445 • Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.229.1:445 • SMB service at 10.0.229.1:445 accessed by Domain Admin credential a-jsmith • SMB service at 10.0.229.1:445 accessed by Domain Admin credential administrator
Host 10.0.220.54 (winxp)	• Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.220.54:445 • Server Service Vulnerability (CVE-2008-4250) affecting SMB service at 10.0.220.54:445
Host 10.0.40.99 (vcsa.smoke.net)	• VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985) affecting Web service at 10.0.40.99:443 • VMware vCenter Server Access Control Vulnerability (CVE-2020-3952) affecting LDAP service at 10.0.40.99:389 • VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972) affecting Web service at 10.0.40.99:443

Host 10.0.225.100	• Unauthenticated Access to the Jenkins Script Console (H3-2020-0021) affecting Web service at 10.0.225.100:8080 • Apache ActiveMQ Remote Code Execution Vulnerability (CVE-2016-3088) affecting Web service at 10.0.225.100:8161 • Insecure Java JMX Configuration (H3-2020-0022) affecting Java service at 10.0.225.100:11099 • Apache HTTP Server Path Traversal and Remote Code Execution Vulnerability (CVE-2021-42013) affecting Web service at 10.0.225.100:8000 • SSH service at 10.0.225.100:22 accessed by credential admin
Host 10.0.220.52 (win10.smoke.net)	• Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.220.52:445 • SMB service at 10.0.220.52:445 accessed by credential xadmin • SMB service at 10.0.220.52:445 accessed by credential a-jsmith via man-in-the-middle relay attack • SMB service at 10.0.220.52:445 accessed by credential user
Host 10.0.225.2 (ns.smoke.net)	• Windows SMB Remote Code Execution Vulnerability (CVE-2017-0144) affecting SMB service at 10.0.225.2:445 • SMB service at 10.0.225.2:445 accessed by credential xadmin • SMB service at 10.0.225.2:445 accessed by credential administrator • SMB service at 10.0.225.2:445 accessed by credential a-jsmith via man-in-the-middle relay attack
Host 10.0.100.101	• IPMI service at 10.0.100.101:623 accessed by credential root • IPMI Cipher Zero Vulnerability (H3-2020-0017) affecting IPMI service at 10.0.100.101:623
Host 10.0.100.100	• IPMI service at 10.0.100.100:623 accessed by credential ADMIN
Host 10.0.40.56	• SSH service at 10.0.40.56:22 accessed by credential user
Host 10.0.229.11 (fs.smoke.net)	• SMB service at 10.0.229.11:445 accessed by credential a-jsmith via man-in-the-middle relay attack • SMB service at 10.0.229.11:445 accessed by credential xadmin • SMB service at 10.0.229.11:445 accessed by credential administrator • SMB service at 10.0.229.11:445 accessed by Local Admin credential jsmith
Host 10.0.40.103	• Weak or Default Credentials - Web Applications (H3-2021-0021) affecting Web service at 10.0.40.103:80
Host 10.0.220.51 (win7.smoke.net)	• SMB service at 10.0.220.51:445 accessed by credential user • SMB service at 10.0.220.51:445 accessed by credential xadmin

Host 10.0.100.102	• IPMI Cipher Zero Vulnerability (H3-2020-0017) affecting IPMI service at 10.0.100.102:623

2.1.4. Ransomware Exposure (8)

Ransomware exposure on 8 stores via 24 separate attack vectors

Ransomware exposures can be used by attackers to obtain access to business-critical data stores, encrypt them with a secret key, and demand a ransom payment from your company before releasing the decryption key. Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and affected services restored.

Severity: CRITICAL

Domain Controller 10.0.229.1 (dc.smoke.net)	• Read/Write access to SMB share C$ at 10.0.229.1:445 using Domain Admin credential administrator • Read/Write access to SMB share ADMIN$ at 10.0.229.1:445 using Domain Admin credential administrator
Host 10.0.40.99 (vcsa.smoke.net)	• VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985) affecting Web service at 10.0.40.99:443 exposes a ransomware target • VMware vCenter Server Access Control Vulnerability (CVE-2020-3952) affecting LDAP service at 10.0.40.99:389 exposes a ransomware target • VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972) affecting Web service at 10.0.40.99:443 exposes a ransomware target
Host 10.0.229.11 (fs.smoke.net)	• Read/Write access to SMB share C$ at 10.0.229.11:445 using credential administrator • Read/Write access to SMB share ADMIN$ at 10.0.229.11:445 using credential administrator • Read/Write access to SMB share FTP at 10.0.229.11:445 using credential administrator • Read/Write access to FTP service at 10.0.229.11:21 using credential anonymous
Host 10.0.225.2 (ns.smoke.net)	• Read/Write access to SMB share C$ at 10.0.225.2:445 using credential administrator • Read/Write access to SMB share ADMIN$ at 10.0.225.2:445 using credential administrator • Read/Write access to NFS share /Logs at 10.0.225.2:2049
Host 10.0.220.55 (win2k3)	• Read/Write access to SMB share C$ at 10.0.220.55:445 using credential administrator • Read/Write access to SMB share ADMIN$ at 10.0.220.55:445 using credential administrator

Host 10.0.225.100	• Read/Write access to Microsoft SQL Server database Northwind at 10.0.225.100:1433 using credential sa • Read/Write access to Microsoft SQL Server database AdventureWorks2017 at 10.0.225.100:1433 using credential sa • Read/Write access to Microsoft SQL Server database msdb at 10.0.225.100:1433 using credential sa • Read/Write access to Microsoft SQL Server database Pubs at 10.0.225.100:1433 using credential sa • Read/Write access to MySQL database employees at 10.0.225.100:3306 using credential root • Read/Write access to PostgreSQL database postgres at 10.0.225.100:5433 using credential postgres • Read/Write access to MySQL database performance_schema at 10.0.225.100:3306 using credential root • Read/Write access to MySQL database mysql at 10.0.225.100:3306 using credential root
Host 10.0.220.52 (win10.smoke.net)	• Read/Write access to SMB share Bitnami at 10.0.220.52:445 using credential jsmith
Host 10.0.220.51 (win7.smoke.net)	• Read/Write access to SMB share Guests at 10.0.220.51:445 using credential Guest

2.1.5. Sensitive Data Exposure (13)

Compromised sensitive data on 13 stores via 21 separate attack vectors

Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally identifiable information), financial account data, and other business-critical information to further exploit or gain profit.

Severity: CRITICAL

Domain Controller 10.0.229.1 (dc.smoke.net)	• SMB share C$ at 10.0.229.1:445 accessed by Domain Admin credential administrator • SMB share ADMIN$ at 10.0.229.1:445 accessed by Domain Admin credential administrator
Host 10.0.229.11 (fs.smoke.net)	• SMB share C$ at 10.0.229.11:445 accessed by credential administrator • SMB share ADMIN$ at 10.0.229.11:445 accessed by credential administrator
Host 10.0.225.2 (ns.smoke.net)	• SMB share C$ at 10.0.225.2:445 accessed by credential administrator • SMB share ADMIN$ at 10.0.225.2:445 accessed by credential administrator
Host 10.0.220.55 (win2k3)	• SMB share C$ at 10.0.220.55:445 accessed by credential administrator • SMB share ADMIN$ at 10.0.220.55:445 accessed by credential administrator

Host 10.0.220.52 (win10.smoke.net)	• SMB share Bitnami at 10.0.220.52:445 accessed by credential jsmith • SMB share Visitors at 10.0.220.52:445 accessed by credential xadmin
Host 10.0.225.100	• Microsoft SQL Server database at 10.0.225.100:1433 accessed by credential sa • PostgreSQL database at 10.0.225.100:5433 accessed by credential postgres • Docker Registry at 10.0.225.100:5001 accessed anonymously • MySQL database at 10.0.225.100:3306 accessed by credential root
Host 10.0.220.51 (win7.smoke.net)	• SMB share Guests at 10.0.220.51:445 accessed by credential Guest
GitLab repo fakegit2 in account kbuch	• Sensitive findings discovered in GitLab repo fakegit2
Bitbucket repo webdl in account kbuch07	• Sensitive findings discovered in Bitbucket repo webdl
GitLab repo secret_test in account kbuch	• Sensitive findings discovered in GitLab repo secret_test
Bitbucket repo fakegit in account kbuch07	• Sensitive findings discovered in Bitbucket repo fakegit
GitLab repo Test_truffle in account kbuch	• Sensitive findings discovered in GitLab repo Test_truffle
Bitbucket repo fakegit2 in account kbuch07	• Sensitive findings discovered in Bitbucket repo fakegit2

2.1.6. Critical Infrastructure Compromise (5)

Compromised 5 critical applications or devices via 6 separate attack vectors

Critical infrastructure consists of key devices and applications that provide attackers a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.

Severity: CRITICAL

Jenkins application at 10.0.225.100:8080	• Unauthenticated Access to the Jenkins Script Console (H3-2020-0021)
LDAP service at 10.0.40.99:389	• VMware vCenter Server Access Control Vulnerability (CVE-2020-3952)
Smart Install service at 10.0.220.254:4786	• Vulnerable Cisco Smart Install (CVE-2018-0171)

Smart Install service at 10.0.229.254:4786	• Vulnerable Cisco Smart Install (CVE-2018-0171)
Web service at 10.0.40.99:443	• VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability (CVE-2021-21985) • VMware vCenter vROPS Plugin Remote Code Execution Vulnerability (CVE-2021-21972)

2.1.7. Brand Compromise (1)

Compromised 1 subdomain

Brand compromise covers ways in which an attacker can harm your company's reputation by, for instance, defacing the company's website, hosting malware off the company's domain, or carrying out phishing attacks that appear to originate from the company.

Severity: HIGH

Subdomain doodle.h3ai.io	• Subdomain Takeover (H3-2021-0002) of doodle.h3ai.io

2.2. Weakness Summary

The pentest identified CRITICAL degrees of risk within the target network, including **39 confirmed weaknesses** (with proof-of-exploit provided) and **6 potential weaknesses**.

2.2.1. Confirmed Weaknesses

Count	First Seen	Name	Weakness Id	Type	Severity
5	04:34PM	Windows SMB Remote Code Execution Vulnerability	CVE-2017-0144		CRITICAL
7	04:33PM	SMB Signing Not Required	H3-2021-0030	SECURITY_MISCONFIGURATION	CRITICAL
5	04:39PM	Credential Reuse	H3-2021-0032	SECURITY_MISCONFIGURATION	CRITICAL
2	04:35PM	Server Service Vulnerability	CVE-2008-4250		CRITICAL
1	05:03PM	Apache ActiveMQ Remote Code Execution Vulnerability	CVE-2016-3088		CRITICAL
2	04:40PM	Vulnerable Cisco Smart Install	CVE-2018-0171		CRITICAL
1	04:33PM	VMware vCenter Server Access Control Vulnerability	CVE-2020-3952		CRITICAL
1	04:33PM	VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability	CVE-2021-21985		CRITICAL
1	04:34PM	Unauthenticated Access to the Jenkins Script Console	H3-2020-0021	SECURITY_MISCONFIGURATION	CRITICAL

Count	First Seen	Name	Weakness Id	Type	Severity
1	04:33PM	Weak or Default Credentials - MySQL	H3-2021-0017	SECURITY_MISCONFIGURATION	CRITICAL
1	04:33PM	Weak or Default Credentials - Microsoft SQL Server	H3-2021-0016	SECURITY_MISCONFIGURATION	CRITICAL
1	05:00PM	Weak or Default Credentials - Postgres	H3-2021-0018	SECURITY_MISCONFIGURATION	CRITICAL
1	05:01PM	Insecure Java JMX Configuration	H3-2020-0022	SECURITY_MISCONFIGURATION	CRITICAL
14	04:40PM	Group Policy Preferences Password Elevation of Privilege Vulnerability	CVE-2014-1812		CRITICAL
2	05:45PM	Apache HTTP Server Path Traversal and Remote Code Execution Vulnerability	CVE-2021-42013		CRITICAL
2	04:44PM	IPMI Cipher Zero Vulnerability	H3-2020-0017	VULNERABILITY	CRITICAL
2	04:36PM	Weak or Default Credentials - SSH	H3-2021-0014	SECURITY_MISCONFIGURATION	CRITICAL
4	04:39PM	Weak or Default Credentials - Web Applications	H3-2021-0021	SECURITY_MISCONFIGURATION	CRITICAL
3	04:33PM	Guest Account Enabled	H3-2020-0008	SECURITY_MISCONFIGURATION	HIGH
3	04:43PM	Insecure IPMI Implementation	H3-2020-0016	VULNERABILITY	HIGH
1	04:33PM	Weak NFS Export Permissions	H3-2020-0009	SECURITY_MISCONFIGURATION	HIGH
14	04:42PM	Weak or Default Credentials - Cracked Credentials	H3-2021-0020	SECURITY_MISCONFIGURATION	HIGH
1	04:33PM	Unauthenticated Docker Registry API Access	H3-2021-0009	SECURITY_MISCONFIGURATION	HIGH
2	04:46PM	Anonymous FTP Enabled	H3-2020-0005	SECURITY_MISCONFIGURATION	HIGH
1	04:32PM	Subdomain Takeover	H3-2021-0002	SECURITY_MISCONFIGURATION	HIGH
1	04:41PM	NBT-NS Poisoning Possible	H3-2021-0035	SECURITY_MISCONFIGURATION	HIGH
1	04:44PM	OpenSSL Heartbleed Vulnerability	CVE-2014-0160		HIGH
1	04:33PM	Apache JServ Protocol (AJP) Vulnerability	CVE-2020-1938		HIGH
1	04:57PM	Kerberos Pre-Authentication Disabled	H3-2021-0011	SECURITY_MISCONFIGURATION	HIGH
1	04:57PM	Kerberoasting	H3-2021-0038	SECURITY_MISCONFIGURATION	HIGH
1	05:01PM	LLMNR Poisoning Possible	H3-2021-0034	SECURITY_MISCONFIGURATION	HIGH
6	04:31PM	Public Access to Git Repository	H3-2021-0031	SECURITY_MISCONFIGURATION	HIGH
2	04:46PM	Weak or Default Credentials - SNMP	H3-2021-0015	SECURITY_MISCONFIGURATION	MEDIUM
1	04:38PM	Unauthenticated Access to Elasticsearch	H3-2021-0036	SECURITY_MISCONFIGURATION	MEDIUM
1	04:56PM	Anonymous Access to ZooKeeper API	H3-2020-0002	SECURITY_MISCONFIGURATION	MEDIUM
1	04:33PM	Anonymous Access to Printer using PJL or PS	H3-2020-0003	SECURITY_MISCONFIGURATION	MEDIUM

Count	First Seen	Name	Weakness Id	Type	Severity
1	04:33PM	Zone Transfer Allowed to Any Server	H3-2020-0004	SECURITY_MISCONFIGURATION	MEDIUM
2	04:43PM	Public Access to Amazon S3 Bucket	H3-2021-0001	SECURITY_MISCONFIGURATION	MEDIUM
7	04:32PM	SMB Null Session Allowed	H3-2020-0007	SECURITY_MISCONFIGURATION	LOW

2.2.2. Potential Weaknesses

Count	First Seen	Name	Weakness Id	Type	Severity
1	04:56PM	Netlogon Elevation of Privilege Vulnerability	CVE-2020-1472		CRITICAL
1	04:33PM	VMware vCenter vROPS Plugin Remote Code Execution Vulnerability	CVE-2021-21972		CRITICAL
1	04:33PM	Remote Desktop Services Remote Code Execution Vulnerability	CVE-2019-0708		HIGH
1	04:33PM	Weak or Default Credentials - Telnet	H3-2021-0013	SECURITY_MISCONFIGURATION	HIGH
1	04:32PM	Dangling DNS Record	H3-2021-0024	SECURITY_MISCONFIGURATION	LOW
2	04:36PM	Expired SSL/TLS Certificate	H3-2021-0025	SECURITY_MISCONFIGURATION	LOW

2.3. Weakness Details

2.3.1. CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability

EternalBlue EternalChampion EternalSynergy EternalRomance MS17-010

Severity: CRITICAL

Description:

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-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

This vulnerability enables an attacker to gain complete control of the target system. This provides a point of presence in the network to conduct further reconnaissance, gather sensitive information, and launch advanced attacks to move laterally throughout the environment. NOTE: This single weakness is used to span all EternalBlue-related vulnerabilities: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148.

Mitigations:

- Apply the updates referenced in Microsoft Security Bulletin MS17-010.
- Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet. If at all possible disable SMBv1

References:

- MS17-010 @ https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- CVE-2017-0144 @ https://nvd.nist.gov/vuln/detail/CVE-2017-0144

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.220.55	tcp/445	microsoft-ds	Microsoft Windows 2003 Or 2008 Microsoft-ds	CRITICAL
10.0.229.1	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL
10.0.220.52	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL
10.0.220.54	tcp/445	microsoft-ds	Microsoft Windows XP Microsoft-ds	CRITICAL
10.0.225.2	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:40PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.220.55	tcp/445	SMB	C$	read,write	14,657
04:40PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.220.55	tcp/445	SMB	ADMIN$	read,write	14,101
04:40PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.220.55	tcp/445	SMB			0
04:40PM	Yes	iwam_win2k3	LOCAL_USER	Plaintext/Hash Dump	10.0.220.55	tcp/445	SMB			0
04:41PM	Yes	aspnet	LOCAL_USER	Plaintext/Hash Dump	10.0.220.55	tcp/445	SMB			0
04:40PM	Yes	iusr_win2k3	LOCAL_USER	Plaintext/Hash Dump	10.0.220.55	tcp/445	SMB			0

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:38PM	admin	ntlm_hash		88**********6c	Plaintext/Hash Dump		
04:38PM	administrator	ntlm_hash		88**********6c	Plaintext/Hash Dump		
04:38PM	administrator	ntlm_hash		88**********6c	Plaintext/Hash Dump		
05:00PM	administrator	ntlm_hash		7e**********16	Plaintext/Hash Dump		
04:38PM	aspnet	ntlm_hash		bd**********a5	Plaintext/Hash Dump		
04:38PM	guest	cleartext			Plaintext/Hash Dump		

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:38PM	guest	cleartext			Plaintext/Hash Dump		
05:00PM	guest	cleartext			Plaintext/Hash Dump		
04:38PM	helpassistant	ntlm_hash		97**********ac	Plaintext/Hash Dump		
04:38PM	iusr_win2k3	ntlm_hash		d2**********38	Plaintext/Hash Dump		
04:38PM	iwam_win2k3	ntlm_hash		0a**********3f	Plaintext/Hash Dump		
04:38PM	support_388945a0	ntlm_hash		44**********d3	Plaintext/Hash Dump		
04:38PM	support_388945a0	ntlm_hash		b0**********61	Plaintext/Hash Dump		

2.3.2. H3-2021-0030: SMB Signing Not Required

Severity: CRITICAL

Description:

The SMB server does not require signing

Impact: IMPERSONATION UNAUTHORIZED ACCESS

SMB signing is a security feature in the SMB protocol that enables SMB clients and servers to validate the authenticity and integrity of communication. When SMB signing is not required, it is possible for attackers to conduct man-in-the-middle attacks that intercept, modify, and relay communication. This can lead to attackers gaining domain account privileges and host access.

Mitigations:

- Enable and require SMB signing via Group Policy or Local Security Policy.

References:

- Microsoft network server: Digitally sign communications (always) @ https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852239(v=ws.11)
- Microsoft network client: Digitally sign communications (always) @ https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always
- Overview of Server Message Block Signing @ https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing
- Samba Configuration @ https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
- The Basics of SMB Signing (Covering Both SMB1 and SMB2) @ https://docs.microsoft.com/en-us/archive/blogs/josebda/the-basics-of-smb-signing-covering-both-smb1-and-smb2

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.2	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL

IP	Port	IANA Service Name	Product	Severity
10.0.220.52	tcp/445	microsoft-ds	Microsoft Windows 7 - 10 Microsoft-ds	CRITICAL
10.0.229.11	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL
10.0.50.2	tcp/445	netbios-ssn	Samba Smbd 4.6.2	LOW
10.0.220.51	tcp/445	microsoft-ds		LOW
10.0.220.54	tcp/445	microsoft-ds	Microsoft Windows XP Microsoft-ds	LOW
10.0.220.55	tcp/445	microsoft-ds	Microsoft Windows 2003 Or 2008 Microsoft-ds	LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:58PM	Yes	administrator	DOMAIN_ADMIN	Plaintext/Hash Dump	10.0.229.1	tcp/445	SMB	C$	read,write	101,819
04:58PM	Yes	administrator	DOMAIN_ADMIN	Plaintext/Hash Dump	10.0.229.1	tcp/445	SMB	ADMIN$	read,write	93,422
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	C$	read,write	113,316
04:58PM	Yes	administrator	DOMAIN_ADMIN	Plaintext/Hash Dump	10.0.229.1	tcp/445	SMB			0
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	ADMIN$	read,write	102,036
04:38PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.225.2	tcp/445	SMB	C$	read,write	61,543
04:38PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.225.2	tcp/445	SMB	ADMIN$	read,write	59,824
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	FTP	read,write	169
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	Users	read,write	2
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	Public	read,write	1
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	CertEnroll	read,write	1
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB	Visitors	read,write	2
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB			0
04:37PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.225.2	tcp/445	SMB			0
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB	Users	read	2,025
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB			0
04:42PM	Yes	user	LOCAL_USER	Man In The Middle	10.0.220.51	tcp/445	SMB			0
04:38PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.225.2	tcp/445	SMB			0
04:57PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB			0
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.51	tcp/445	SMB			0

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:57PM	administrator	ntlm_hash		2a**********1d	Plaintext/Hash Dump		
04:41PM	administrator	ntlm_hash		2a**********1d	Man In The Middle		smb_user
04:41PM	defaultaccount	ntlm_hash		31**********c0	Man In The Middle		smb_user
04:57PM	defaultaccount	cleartext			Plaintext/Hash Dump		
04:41PM	guest	ntlm_hash		31**********c0	Man In The Middle		smb_user
04:36PM	guest	ntlm_hash		31**********c0	Plaintext/Hash Dump		smb_user
04:57PM	guest	cleartext			Plaintext/Hash Dump		
04:41PM	visitor	ntlm_hash		31**********c0	Man In The Middle		smb_user
04:57PM	xadmin	ntlm_hash		5b**********63	Plaintext/Hash Dump		
04:41PM	xadmin	ntlm_hash		5b**********63	Man In The Middle		smb_user

2.3.3. H3-2021-0032: Credential Reuse

Severity: CRITICAL

Description:

A credential was found to be reused in the environment.

Impact: UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Attackers take advantage of credential reuse by exploiting a single flaw to gain access to a system, obtain valid credentials, and then attempt to laterally move with those credentials if they are reused.

Mitigations:

- Update the password to be unique and ensure it follows current password guidelines.

References:

- NIST Password Guidelines @ https://pages.nist.gov/800-63-3/sp800-63b.html

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
administrator	LOCAL_ADMIN	Plaintext/Hash Dump	SMB	10.0.229.11	tcp/445	CRITICAL
xadmin	LOCAL_USER	Plaintext/Hash Dump	SMB	10.0.220.52	tcp/445	CRITICAL
user	LOCAL_USER	Man In The Middle	SMB	10.0.220.51	tcp/445	HIGH
xadmin	LOCAL_USER	Plaintext/Hash Dump	SMB	10.0.220.51	tcp/445	HIGH
xadmin	LOCAL_USER	Plaintext/Hash Dump	SMB	10.0.229.11	tcp/445	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	C$	read,write	113,316
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	ADMIN$	read,write	102,036
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	FTP	read,write	169
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	Users	read,write	2
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	Public	read,write	1
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB	CertEnroll	read,write	1
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB	Visitors	read,write	2
04:57PM	Yes	administrator	LOCAL_ADMIN	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB			0
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB	Users	read	2,025
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB			0
04:42PM	Yes	user	LOCAL_USER	Man In The Middle	10.0.220.51	tcp/445	SMB			0
04:57PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB			0
04:39PM	Yes	xadmin	LOCAL_USER	Plaintext/Hash Dump	10.0.220.51	tcp/445	SMB			0

2.3.4. CVE-2008-4250: Server Service Vulnerability MS08-067

Severity: CRITICAL

Description:

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request, as exploited in the wild in October 2008, aka "Server Service Vulnerability.

Mitigations:

- Apply the updates referenced in Microsoft Security Bulletin MS08-067.
- Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet.

References:

- CVE-2008-4250 @ https://nvd.nist.gov/vuln/detail/CVE-2008-4250

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.220.54	tcp/445	microsoft-ds	Microsoft Windows XP Microsoft-ds	CRITICAL
10.0.220.55	tcp/445	microsoft-ds	Microsoft Windows 2003 Or 2008 Microsoft-ds	CRITICAL

2.3.5. CVE-2016-3088: Apache ActiveMQ Remote Code Execution Vulnerability

Severity: CRITICAL

Description:

The Fileserver web application in Apache ActiveMQ 5.x before 5.14.0 allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS PRIVILEGE ESCALATION INFORMATION DISCLOSURE

This vulnerability enables attackers to upload a webshell to the vulnerable ActiveMQ server. Through the uploaded webshell, attackers can execute arbitrary commands on the vulnerable host in the context of the user running the ActiveMQ server process.

Mitigations:

- Upgrade Apache ActiveMQ to the latest version. This vulnerability is fixed in version 5.14.0 and later.
- Update the Apache ActiveMQ configuration to disable the Fileserver feature. Refer to the Apache ActiveMQ Advisory reference.

References:

- Apache ActiveMQ Advisory @ https://activemq.apache.org/security-advisories.data/CVE-2016-3088-announcement.txt
- Red Hat Guidance @ https://access.redhat.com/security/cve/cve-2016-3088
- CVE-2016-3088 @ https://nvd.nist.gov/vuln/detail/CVE-2016-3088

Affected Applications:

Name	VHost	IP	Port	Severity
apache activemq		10.0.225.100	tcp/8161	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
05:02PM	Yes	admin	APPLICATION_USER	Default Login	10.0.225.100	tcp/8161	Web			12
05:01PM	Yes	user	APPLICATION_USER	Default Login	10.0.225.100	tcp/8161	Web			12
05:00PM	No			Anonymous	10.0.225.100	tcp/8161	Web			2

2.3.6. CVE-2018-0171: Vulnerable Cisco Smart Install

Severity: CRITICAL

Description:

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device. The vulnerability is due to improper validation of packet data. An attacker could exploit this vulnerability by sending a crafted Smart Install message to an affected device on TCP port 4786. A successful exploit could allow the attacker to cause a buffer overflow on the affected device, which could have the following impacts: Triggering a reload of the device, Allowing the attacker to execute arbitrary code on the device, Causing an indefinite loop on the affected device that triggers a watchdog crash. Cisco Bug IDs: CSCvg76186.

Impact: PRIVILEGE ESCALATION INFORMATION DISCLOSURE

A vulnerability in the Smart Install feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition, or to execute arbitrary code on an affected device.

Mitigations:

- If an upgrade to a non-vulnerable version cannot be made the smart install service should be disabled.
- Cisco has released free software updates that address the vulnerability described in this advisory. Customers may only install and expect support for software versions and feature sets for which they have purchased a license.

References:

- CVE-2018-0171 @ https://nvd.nist.gov/vuln/detail/CVE-2018-0171

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.220.254	tcp/4786	smart-install		CRITICAL
10.0.229.254	tcp/4786	smart-install		CRITICAL

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
05:06PM	root	ios9_hash		$9**********SU	Plaintext/Hash Dump		cisco_user
04:41PM	root	ios9_hash		$9**********SU	Plaintext/Hash Dump		cisco_user
05:06PM		ios9_hash		$9**********aU	Plaintext/Hash Dump		cisco_enable
04:41PM		ios9_hash		$9**********aU	Plaintext/Hash Dump		cisco_enable

2.3.7. CVE-2020-3952: VMware vCenter Server Access Control Vulnerability

Severity: CRITICAL

Description:

Under certain conditions, vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Services Controller (PSC), does not correctly implement access controls.

Impact: FILE UPLOAD UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Vulnerable vCenter Servers may disclose administrative account credentials and allow creation of an attacker-controlled administrative account allowing full control of the vCenter Server resources.

Mitigations:

- Apply all updates and patch to the latest version of vCenter Server.

References:

- CVE-2020-3952 @ https://nvd.nist.gov/vuln/detail/CVE-2020-3952
- VMware Security Advisories @ https://www.vmware.com/security/advisories/VMSA-2020-0006.html

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.40.99	tcp/389	ldap		CRITICAL

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:33PM	Administrator	vcenter_hash		e2**********55	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	DNS/vcsa.smoke.net	vcenter_hash		0b**********14	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	host/vcsa.smoke.net	vcenter_hash		bb**********37	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	K/M	vcenter_hash		57**********04	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	krbtgt/VSPHERE.LOCAL	vcenter_hash		ea**********28	Plaintext/ Hash Dump	vsphere.local	vcenter_user

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:33PM	ldap/vcsa.smoke.net	vcenter_hash		07**********69	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	vcsa.smoke.net	vcenter_hash		53**********60	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	vmca/vcsa.smoke.net	vcenter_hash		ee**********16	Plaintext/ Hash Dump	vsphere.local	vcenter_user
04:33PM	waiter f512597f-6934-47d8-9642-ee3177bf83f0	vcenter_hash		0f**********64	Plaintext/ Hash Dump	vsphere.local	vcenter_user

2.3.8. CVE-2021-21985: VMware vCenter vSAN Health Check Plugin Remote Code Execution Vulnerability

Severity: CRITICAL

Description:

The vSphere Client (HTML5) contains a remote code execution vulnerability due to lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS

A malicious actor with network access to port 443 on vCenter Server may perform actions allowed by the impacted plug-ins without authentication.

Mitigations:

- Apply all updates and patch to the latest vendor-supported version.
- Apply workarounds described in VMware KB83829.

References:

- CVE-2021-21985 @ https://nvd.nist.gov/vuln/detail/CVE-2021-21985
- Proof of Concept for CVE-2021-21985 @ https://github.com/r0ckysec/CVE-2021-21985/blob/main/CVE-2021-21985_exp.py
- VMware Advisory VMSA-2021-0010 @ https://www.vmware.com/security/advisories/VMSA-2021-0010.html
- VMware KB83829 @ https://kb.vmware.com/s/article/83829

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.40.99	tcp/443	https	VMware vSphere Http Config	CRITICAL

2.3.9. H3-2020-0021: Unauthenticated Access to the Jenkins Script Console

Severity: CRITICAL

Description:

The Jenkins server exposes the script console to unauthenticated users.

Impact: REMOTE CODE EXECUTION INFORMATION DISCLOSURE UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Attackers can use the Jenkins script console to execute arbitrary commands on the Jenkins host and to gain shell access. Attackers can gain access to credentials stored in Jenkins or other confidential data.

Mitigations:

- Restrict access to the script console to administrative users. Disable unauthenticated script console access in the Global Security Configuration section of the admin interface.

References:

- Securing Jenkins @ https://www.jenkins.io/doc/book/system-administration/security/
- Jenkins - Script-Console Java Execution (Metasploit) @ https://www.exploit-db.com/exploits/24272

Affected Applications:

Name	VHost	IP	Port	Severity
jenkins		10.0.225.100	tcp/8080	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:58PM	Yes	jsmith	DOMAIN_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB	Bitnami	read,write	20,060
04:57PM	Yes	jsmith	DOMAIN_USER	Plaintext/Hash Dump	10.0.229.1	tcp/445	SMB		read_password_policy	0
04:57PM	Yes	jsmith	DOMAIN_USER	Plaintext/Hash Dump	10.0.220.51	tcp/445	SMB			0
04:57PM	Yes	jsmith	DOMAIN_USER	Plaintext/Hash Dump	10.0.220.52	tcp/445	SMB			0
04:57PM	Yes	jsmith	DOMAIN_USER	Plaintext/Hash Dump	10.0.229.11	tcp/445	SMB		local_admin	0

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:57PM	Yes	jsmith	DOMAIN_USER	Plaintext/Hash Dump	10.0.225.2	tcp/445	SMB			0
04:33PM	No			Anonymous	10.0.225.100	tcp/8080	Web			15

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:34PM	baduser	cleartext	b*********d		Plaintext/Hash Dump		
04:34PM	jsmith	cleartext	S*********!		Plaintext/Hash Dump		
04:34PM	user	cleartext	p*******		Plaintext/Hash Dump		

2.3.10. H3-2021-0017: Weak or Default Credentials - MySQL

Severity: CRITICAL

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION FILE UPLOAD

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
root	SERVICE_USER	Default Login	Database	10.0.225.100	tcp/3306	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:34PM	Yes	root	SERVICE_USER	Default Login	10.0.225.100	tcp/3306	Database	employees	list,read,write	3,919,015
04:34PM	Yes	root	SERVICE_USER	Default Login	10.0.225.100	tcp/3306	Database	performance_schema	list,read,write	358,456
04:34PM	Yes	root	SERVICE_USER	Default Login	10.0.225.100	tcp/3306	Database	mysql	list,read,write	141,445
04:34PM	Yes	root	SERVICE_USER	Default Login	10.0.225.100	tcp/3306	Database	sys	list,read,write	6
04:33PM	Yes	root	SERVICE_USER	Default Login	10.0.225.100	tcp/3306	Database			0

2.3.11. H3-2021-0016: Weak or Default Credentials - Microsoft SQL Server

Severity: CRITICAL

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION FILE UPLOAD

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
sa	ADMIN	Default Login	Database	10.0.225.100	tcp/1433	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:34PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database	Northwind	list,read,write	3,308
04:34PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database	AdventureWorks2017	list,read,write	1,597
04:34PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database	msdb	list,read,write	1,619
04:34PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database	Pubs	list,read,write	255
04:34PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database	master	list,read,write	4
04:34PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database	tempdb	list	0
04:33PM	Yes	sa	ADMIN	Default Login	10.0.225.100	tcp/1433	Database			0

2.3.12. H3-2021-0018: Weak or Default Credentials - Postgres

Severity: CRITICAL

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION FILE UPLOAD

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
postgres	SERVICE_USER	Default Login	Database	10.0.225.100	tcp/5433	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
05:00PM	Yes	postgres	SERVICE_USER	Default Login	10.0.225.100	tcp/5433	Database	postgres	list,read,write	2,141,275
05:00PM	Yes	postgres	SERVICE_USER	Default Login	10.0.225.100	tcp/5433	Database			0

2.3.13. H3-2020-0022: Insecure Java JMX Configuration

Severity: CRITICAL

Description:

The JMX endpoint is unauthenticated and provides users arbitrary access to the JMX-monitored application, as well as the ability to execute arbitrary code at the target.

Impact: REMOTE CODE EXECUTION INFORMATION DISCLOSURE UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Attackers can coerce the target to download malicious payloads from an attacker-controlled server. The attacker can then execute arbitrary commands on the target host and gain shell access.

Mitigations:

- Configure user authentication and SSL on the JMX endpoint.

References:

- Attacking RMI based JMX Services @ https://mogwailabs.de/en/blog/2019/04/attacking-rmi-based-jmx-services/
- Java JMX Server Insecure Configuration Java Code Execution (Metasploit) @ https://www.rapid7.com/db/modules/exploit/multi/misc/java_jmx_server

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.100	tcp/11099	java-rmi	Java RMI	CRITICAL

2.3.14. CVE-2014-1812: Group Policy Preferences Password Elevation of Privilege Vulnerability

Severity: CRITICAL

Description:

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."

Impact: PRIVILEGE ESCALATION

The Group Policy implementation in Microsoft Windows allows an attacker who has gained access to a regular domain user to obtain cleartext credentials from the SYSVOL share on a Domain Controller. These credentials may lead to an elevation of privilege to Domain Administrator rights depending on the credentials obtained.

Mitigations:

- Apply the updates referenced in Microsoft Security Bulletin MS14-025 below.
- Those that had existing group policies that used the Group Policy preferences before this patch was applied will need to take additional action to remove those policies. Follow the steps outlined in the "Removing CPassword preferences" at the very bottom of the Knowledge Base article linked below.

References:

- CVE-2014-1812 @ https://nvd.nist.gov/vuln/detail/CVE-2014-1812
- Microsoft Security Bulletin MS14-025 @ https://technet.microsoft.com/security/bulletin/MS14-025
- Knowledge Base Article 2962486 @ https://support.microsoft.com/kb/2962486

Affected Resources:

Resource	Repo	Severity
/Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml	10.0.229.1:445: C$	CRITICAL
/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml	10.0.229.1:445: SYSVOL	CRITICAL
/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml	10.0.229.1:445: ADMIN$	CRITICAL
/ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml	10.0.229.1:445: C$	CRITICAL
/ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml	10.0.229.11:445: C$	CRITICAL
/SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml	10.0.229.1:445: ADMIN$	CRITICAL
/Windows/SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml	10.0.229.1:445: C$	CRITICAL
/Windows/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml	10.0.229.1:445: C$	CRITICAL
/Windows/SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml	10.0.229.1:445: C$	CRITICAL
/SYSVOL/domain/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml	10.0.229.1:445: ADMIN$	CRITICAL
/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/ScheduledTasks/ScheduledTasks.xml	10.0.229.1:445: SYSVOL	CRITICAL
/SYSVOL/sysvol/smoke.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml	10.0.229.1:445: ADMIN$	CRITICAL
/ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/Groups/Groups.xml	10.0.225.2:445: C$	HIGH

Resource	Repo	Severity
/ProgramData/Microsoft/Group Policy/History/{31B2F340-016D-11D2-945F-00C04FB984F9}/Machine/Preferences/ScheduledTasks/ScheduledTasks.xml	10.0.225.2:445: C$	HIGH

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
05:02PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:01PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:01PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:01PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
04:40PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:02PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:03PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:01PM	administrator	cleartext	U*********$		Plaintext/Hash Dump		
05:02PM	xadmin	cleartext	L********n		Plaintext/Hash Dump		
05:02PM	xadmin	cleartext	L********n		Plaintext/Hash Dump		
05:01PM	xadmin	cleartext	L********n		Plaintext/Hash Dump		
05:00PM	xadmin	cleartext	L********n		Plaintext/Hash Dump		
05:03PM	xadmin	cleartext	L********n		Plaintext/Hash Dump		
05:02PM	xadmin	cleartext	L********n		Plaintext/Hash Dump		

2.3.15. CVE-2021-42013: Apache HTTP Server Path Traversal and Remote Code Execution Vulnerability

Severity: CRITICAL

Description:

It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION

This vulnerability allows unauthenticated attackers to retrieve sensitive data on the server, such as configuration files containing passwords. In certain server configurations, if CGI scripts are enabled, attackers can execute arbitrary commands on the vulnerable host.

Mitigations:

- This vulnerability affects Apache HTTP Server 2.4.49 and 2.4.50. Upgrade to version 2.4.51.

References:

- Apache 2.4 Vulnerabilities @ https://httpd.apache.org/security/vulnerabilities_24.html
- CVE-2021-42013 @ https://nvd.nist.gov/vuln/detail/CVE-2021-42013

Affected Applications:

Name	VHost	IP	Port	Severity
apache http_server		10.0.225.100	tcp/8000	CRITICAL
apache http_server		10.0.225.100	tcp/8888	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:34PM	No			Anonymous	10.0.225.100	tcp/8000	Web			1
04:40PM	No			Anonymous	10.0.225.100	tcp/8888	Web			1

2.3.16. H3-2020-0017: IPMI Cipher Zero Vulnerability

Severity: CRITICAL

Description:

Various vendor IPMI implementations allow remote attackers to bypass authentication and execute arbitrary IPMI commands by using cipher suite 0 (aka cipher zero) and an arbitrary password.

Impact: INFORMATION DISCLOSURE REMOTE CODE EXECUTION PRIVILEGE ESCALATION

An attacker exploiting the Cipher Zero vulnerability may gain control of the management interface of a system. This level of access potentially allows an attacker to control hardware or software at the system level.

Mitigations:

- Disable the IPMI service if not needed.
- Disable cipher suite zero authentication method.
- If IPMI service is required and unable to disable cipher suite zero authentication, implement access controls to limit access via whitelisted addresses.

References:

- CWE-287: Improper Authentication @ http://cwe.mitre.org/data/definitions/287.html
- CVE-2013-4782 @ https://nvd.nist.gov/vuln/detail/CVE-2013-4782
- CVE-2013-4783 @ https://nvd.nist.gov/vuln/detail/CVE-2013-4783
- CVE-2013-4784 @ https://nvd.nist.gov/vuln/detail/CVE-2013-4784
- CVE-2013-4785 @ https://nvd.nist.gov/vuln/detail/CVE-2013-4785

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.100.101	udp/623	asf-rmcp		CRITICAL
10.0.100.102	udp/623	asf-rmcp		CRITICAL

2.3.17. H3-2021-0014: Weak or Default Credentials - SSH

Severity: CRITICAL

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: REMOTE CODE EXECUTION INFORMATION DISCLOSURE UNAUTHORIZED ACCESS FILE UPLOAD

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
user	LOCAL_USER	Default Login	SSH	10.0.40.56	tcp/22	CRITICAL
admin	LOCAL_USER	Default Login	SSH	10.0.225.100	tcp/22	CRITICAL

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:37PM	Yes	user	LOCAL_USER	Default Login	10.0.40.56	tcp/22	SSH			0
04:36PM	Yes	admin	LOCAL_USER	Default Login	10.0.225.100	tcp/22	SSH			0

2.3.18. H3-2021-0021: Weak or Default Credentials - Web Applications

Severity: CRITICAL

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
tomcat	APPLICATION_USER	Default Login	Web	10.0.40.103	tcp/80	CRITICAL
user	APPLICATION_USER	Default Login	Web	10.0.225.100	tcp/8161	MEDIUM
admin	APPLICATION_USER	Default Login	Web	10.0.225.100	tcp/8161	MEDIUM

Username	Role	Source	Service Type	IP	Port	Severity
ADMIN	APPLICATION_USER	Default Login	Web	10.0.100.100	tcp/80	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
05:02PM	Yes	admin	APPLICATION_USER	Default Login	10.0.225.100	tcp/8161	Web			12
05:01PM	Yes	user	APPLICATION_USER	Default Login	10.0.225.100	tcp/8161	Web			12
04:40PM	Yes	tomcat	APPLICATION_USER	Default Login	10.0.40.103	tcp/80	Web			5
05:01PM	Yes	admin	APPLICATION_USER	Default Login	10.0.225.100	tcp/8161	Web			0
04:39PM	Yes	ADMIN	APPLICATION_USER	Default Login	10.0.100.100	tcp/80	Web			0
04:39PM	Yes	ADMIN	APPLICATION_USER	Default Login	10.0.100.100	tcp/80	Web			1
04:39PM	Yes	tomcat	APPLICATION_USER	Default Login	10.0.40.103	tcp/80	Web			0
05:01PM	Yes	user	APPLICATION_USER	Default Login	10.0.225.100	tcp/8161	Web			0
04:34PM	No			Anonymous	10.0.40.103	tcp/80	Web			67
05:00PM	No			Anonymous	10.0.225.100	tcp/8161	Web			2
04:34PM	No			Anonymous	10.0.100.100	tcp/80	Web			1

2.3.19. H3-2020-0008: Guest Account Enabled

Severity: HIGH

Description:

The default Guest account allows unauthenticated network users to log on as a Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS

Enabled Guest accounts can allow attackers access to shared resources without supplying credentials or a password. Sensitive information may be gathered and used to launch additional attacks

Mitigations:

- Disable the Guest account if not needed.
- If needed, ensure Guest account does not have access to sensitive information.

References:

- Accounts: Guest account status - security policy setting @ https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.220.51	tcp/445	microsoft-ds		HIGH
10.0.50.2	tcp/445	netbios-ssn	Samba Smbd 4.6.2	LOW
10.0.220.51	tcp/3389	tcpwrapped		LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:35PM	Yes	Guest	LOCAL_USER	Anonymous	10.0.220.51	tcp/445	SMB	Guests	read,write	250,006

2.3.20. H3-2020-0016: Insecure IPMI Implementation

Severity: HIGH

Description:

The IPMI 2.0 specification supports RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication, which allows remote attackers to obtain password hashes and conduct offline password guessing attacks by obtaining the HMAC from a RAKP message 2 response from a BMC.

Impact: INFORMATION DISCLOSURE REMOTE CODE EXECUTION PRIVILEGE ESCALATION

Use of RAKP authentication allows an attacker to capture password hashes that may be used to gain control of the management interface of a system. This level of access potentially allows an attacker to control hardware or software at the system level.

Mitigations:

- Disable the IPMI service if not needed. If required, implement access controls to limit access via whitelisted addresses.

References:

- CWE-287: Improper Authentication @ http://cwe.mitre.org/data/definitions/287.html
- CVE-2013-4786 @ https://nvd.nist.gov/vuln/detail/CVE-2013-4786

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.100.100	udp/623	asf-rmcp		HIGH
10.0.100.101	udp/623	asf-rmcp		HIGH
10.0.100.102	udp/623	asf-rmcp		HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:47PM	Yes	root	LOCAL_USER	Plaintext/Hash Dump	10.0.100.101	udp/623	IPMI			0

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:45PM	Yes	ADMIN	LOCAL_USER	Plaintext/Hash Dump	10.0.100.100	udp/623	IPMI			0

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:44PM	ADMIN	cleartext	A****		Plaintext/Hash Dump		ipmi_user
04:46PM	root	cleartext	c*****		Plaintext/Hash Dump		ipmi_user
04:43PM	root	ipmi_hash		82**********09	Plaintext/Hash Dump		ipmi_user

2.3.21. H3-2020-0009: Weak NFS Export Permissions

Severity: HIGH

Description:

The NFS server allows any remote system to mount or access exported shares.

Impact: INFORMATION DISCLOSURE FILE UPLOAD UNAUTHORIZED ACCESS

World readable NFS shares allow any remote system to connect to the server. This provides an attacker access to any files made available by the NFS server.

Mitigations:

- Implement appropriate controls to restrict access to authorized systems only.
- Review the permissions of the exported NFS share to confirm secure best practices are being used.

References:

- CWE-284: Improper Access Control @ https://cwe.mitre.org/data/definitions/284.html
- Security and NFS @ http://nfs.sourceforge.net/nfs-howto/ar01s06.html

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.2	tcp/2049	nfs		HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:33PM	No			Anonymous	10.0.225.2	tcp/2049	NFS	/Logs	read,write	152

2.3.22. H3-2021-0020: Weak or Default Credentials - Cracked Credentials

Severity: HIGH

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS REMOTE CODE EXECUTION FILE UPLOAD

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Potential Credentials:

Username	Source	Service Type	Domain	Severity
administrator	Cracked			HIGH
nsunkavally	Cracked		SMOKE.NET	HIGH
xadmin	Cracked			HIGH
xadmin	Cracked			HIGH
user	Cracked			HIGH
administrator	Cracked			HIGH
xadmin	Cracked			HIGH
a-jsmith	Cracked		SMOKE	HIGH
xadmin	Cracked			HIGH
a-jsmith	Cracked		SMOKE	HIGH
a-jsmith	Cracked		SMOKE	HIGH
a-jsmith	Cracked			HIGH

Username	Source	Service Type	Domain	Severity
administrator	Cracked			HIGH
admin	Cracked			HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:59PM	Yes	a-jsmith	DOMAIN_ADMIN	Cracked	10.0.229.1	tcp/445	SMB			0
05:09PM	Yes	nsunkavally	DOMAIN_USER	Cracked	10.0.229.1	tcp/445	SMB			0
05:09PM	Yes	nsunkavally	DOMAIN_USER	Cracked	10.0.220.51	tcp/445	SMB			0
05:09PM	Yes	nsunkavally	DOMAIN_USER	Cracked	10.0.220.52	tcp/445	SMB			0
05:09PM	Yes	nsunkavally	DOMAIN_USER	Cracked	10.0.229.11	tcp/445	SMB			0
05:09PM	Yes	nsunkavally	DOMAIN_USER	Cracked	10.0.225.2	tcp/445	SMB			0

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:46PM	admin	cleartext	p*******		Cracked		
04:56PM	administrator	cleartext	p*******		Cracked		
05:20PM	administrator	cleartext	p*******		Cracked		
05:57PM	administrator	cleartext	P*******		Cracked		
05:41PM	a-jsmith	cleartext	1*******		Cracked	SMOKE	smb_user
05:49PM	a-jsmith	cleartext	1*******		Cracked	SMOKE	smb_user
04:50PM	a-jsmith	cleartext	1*******		Cracked		
04:45PM	a-jsmith	cleartext	1*******		Cracked	SMOKE	smb_user
05:08PM	nsunkavally	cleartext	H*******!		Cracked	SMOKE.NET	
04:47PM	user	cleartext	p*******		Cracked		smb_user
05:07PM	xadmin	cleartext	L********n		Cracked		
04:42PM	xadmin	cleartext	L********n		Cracked		smb_user
04:47PM	xadmin	cleartext	L********n		Cracked		smb_user
04:44PM	xadmin	cleartext	L********n		Cracked		smb_user

2.3.23. H3-2021-0009: Unauthenticated Docker Registry API Access

Severity: HIGH

Description:

The Docker Registry API is accessible without authentication.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS FILE UPLOAD

An attacker could access sensitive information stored in the registry such as manifests and configurations of each image stored in the catalog.

Mitigations:

- Ensure the Docker Registry API implements TLS certificates from a trusted CA.
- Enable authentication to the Docker Registry API by configuring basic authentication or token based authentication.

References:

- Docker Registry @ https://docs.docker.com/registry/
- Configuring a registry @ https://docs.docker.com/registry/configuration/#auth

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.100	tcp/5001	http	Redhat Docker Registry	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:33PM	No			Anonymous	10.0.225.100	tcp/5001	Docker Registry	test/test	list,read,write	1
04:33PM	No			Anonymous	10.0.225.100	tcp/5001	Docker Registry	busybox	list,read,write	1
04:33PM	No			Anonymous	10.0.225.100	tcp/5001	Docker Registry	python	list,read,write	1
04:33PM	No			Anonymous	10.0.225.100	tcp/5001	Docker Registry	ubuntu	list,read,write	1

2.3.24. H3-2020-0005: Anonymous FTP Enabled

Severity: HIGH

Description:

Anonymous login is allowed on the remote FTP server.

Impact: INFORMATION DISCLOSURE FILE UPLOAD UNAUTHORIZED ACCESS

Anonymous login allows any remote user to connect to the FTP server without providing a password or unique credentials. This allows access to files made available by the FTP server.

Mitigations:

- Disable anonymous login or disable the FTP service if not needed.

References:

- CWE-284: Improper Access Control @ https://cwe.mitre.org/data/definitions/284.html

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.229.11	tcp/21	ftp	Microsoft Ftpd, Microsoft IIS	HIGH
10.0.225.100	tcp/9090	ftp	vsFTPd Project vsFTPd 3.0.3	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:56PM	Yes	anonymous	SERVICE_USER	Anonymous	10.0.229.11	tcp/21	FTP		read,write	169
04:46PM	Yes	anonymous	SERVICE_USER	Anonymous	10.0.225.100	tcp/9090	FTP		read	149

2.3.25. H3-2021-0002: Subdomain Takeover

Severity: HIGH

Description:

The DNS record for a subdomain has a CNAME record that points to another subdomain that is not in use. Attackers may be able to claim the subdomain that is the CNAME for this subdomain.

Impact: DEFACEMENT IMPERSONATION

By taking over a legitimate looking company domain, attackers can trick users through phishing campaigns, attempt to steal user cookies and passwords, deface the company web site and damage the company brand.

Mitigations:

- If the subdomain is not in use, remove the stale DNS record for it.
- If the subdomain is in use, reclaim the subdomain that is the CNAME, or set a new valid CNAME for this subdomain.

References:

- Subdomain Takeovers: Thoughts on Risk @ https://0xpatrik.com/subdomain-takeover/
- Prevent Dangling DNS Entries and Avoid Subdomain Takeover @ https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Affected External Domains:

Domain	CNAME	IP Addresses	Severity
doodle.h3ai.io	11285521401250.s3-website.us-east-2.amazonaws.com	52.219.102.44	HIGH

2.3.26. H3-2021-0035: NBT-NS Poisoning Possible

Severity: HIGH

Description:

Netbios Name Service (NBT-NS) is one of two components of Microsoft Windows machines that server as alternate methods of host identification. An attacker can spoof a reply as an authoritative source to a victim request and capture the credential information passed over the network. Credential information can be captured in hashed or plaintext format.

Impact: REMOTE CODE EXECUTION PRIVILEGE ESCALATION

A captured hash credential can be cracked offline to discover the plaintext password and also be relayed for reuse on other systems. Likewise, a captured plaintext credential can be immediately used to access other systems.

Mitigations:

- Disable NBT-NS in the network adapter settings by selecting 'Disable NetBIOS over TCP/IP. Alternatively, disable by using a registry key.

References:

- T1171 - LLMNR/NBT-NS Poisoning and Relay @ https://attack.mitre.org/techniques/T1171/
- Local Network Vulnerabilities - LLMNR and NTB-NS Poisoning @ https://www.surecloud.com/services/news/local-network-vulnerabilities-llmnr-nbt-ns-poisoning
- LLMNR and NBT-NS Mitigation @ https://cccsecuritycenter.org/remediation/llmnr-nbt-ns

Affected Hosts:

IP	Host Name	Operating System	Severity
10.0.220.51	win7.smoke.net	Linux, Microsoft Windows	HIGH

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:36PM	a-jsmith	ntlmv2_hash		a-**********00	Man In The Middle	SMOKE	smb_user
04:41PM	a-jsmith	ntlmv2_hash		a-**********00	Man In The Middle	SMOKE	smb_user

2.3.27. CVE-2014-0160: OpenSSL Heartbleed Vulnerability Heartbleed

Severity: HIGH

Description:

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Impact: INFORMATION DISCLOSURE

Attackers can use this vulnerability to dump sensitive information from the memory of vulnerable servers. Sensitive information can include private keys, passwords, and other confidential data.

Mitigations:

- The vulnerability is patched in OpenSSL version 1.0.1g and later. Refer to your vendor's documentation to upgrade to the latest version.

References:

- CVE-2014-0160 @ https://nvd.nist.gov/vuln/detail/CVE-2014-0160
- Heartbleed @ https://heartbleed.com/
- FOX-IT Blog Writeup @ http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.100	tcp/8443	https	Apache HTTPD 2.2.22	HIGH

2.3.28. CVE-2020-1938: Apache JServ Protocol (AJP) Vulnerability GhostCat

Severity: HIGH

Description:

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS

Attackers can read files contained within the web application's base folder. These files may contain sensitive information. In certain cases, attackers can achieve remote code execution if the web application permits uploading files to its base folder.

Mitigations:

- Update to the latest version of Apache Tomcat. Apache Tomcat has released versions 9.0.31, 8.5.51, and 7.0.100 to fix this vulnerability.

- Red Hat recommends disabling the Apache JServ Protocol (AJP) connector in Tomcat if not used, or binding it to localhost port, since most of AJP's use is in cluster environments, and the 8009 port should never be exposed on the internet without strict access-control lists. The AJP connector is enabled by default on all Tomcat servers.
- If the AJP service does not need to be publicly accessible, ensure that access is filtered.

References:

- CVE-2020-1938 @ https://nvd.nist.gov/vuln/detail/CVE-2020-1938

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.40.103	tcp/8009	ajp13	Apache Jserv	HIGH

2.3.29. H3-2021-0011: Kerberos Pre-Authentication Disabled AS-REP Roast

Severity: HIGH

Description:

Kerberos pre-authentication is security control that prevents unauthenticated attackers from obtaining sensitive information about other users in a domain. This security measure is enabled by default and should never be disabled for a user.

Impact: INFORMATION DISCLOSURE

An attacker can obtain the password hash of a user when Kerberos pre-authentication is disabled.

Mitigations:

- Re-enable Kerberos pre-authentication for the user. Find the User within Active Directory, and under the Account tab within the Account options uncheck 'Do not require Kerberos preauthentication'.

References:

- Kerberos Pre-Authentication: Why It Should Not Be Disabled @ https://social.technet.microsoft.com/wiki/contents/articles/23559.kerberos-pre-authentication-why-it-should-not-be-disabled.aspx
- AS-REP Toasting Attack Example @ https://stealthbits.com/blog/cracking-active-directory-passwords-with-as-rep-roasting/

Affected Potential Credentials:

Username	Source	Service Type	Domain	Severity
nsunkavally	Plaintext/Hash Dump		SMOKE.NET	HIGH

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:57PM	nsunkavally	kerb_asrep_hash		$k**********d8	Plaintext/Hash Dump	SMOKE.NET	

2.3.30. H3-2021-0038: Kerberoasting

Severity: HIGH

Description:

Kerberoasting is an attacker technique that exploits weaknesses inherent to the Kerberos protocol. This technique enables an attacker with a low-privilege domain user account to retrieve password hashes for higher-privilege service accounts.

Impact: INFORMATION DISCLOSURE PRIVILEGE ESCALATION

An attacker who's able to crack the password hash of a Kerberoastable service account will be able to escalate his or her privileges to those of the service account.

Mitigations:

- Group Managed Service Accounts (gMSA) and standalone Managed Service Accounts (sMSA) are the recommended Microsoft alternative to using user Service Principal Names (SPNs).
- If a user Service Principal (SPN) Name is required, ensure the user account is set up with a long, complex, and random password to prevent attackers from cracking the password hash obtained from Kerberoasting.

References:

- MITRE ATT&CK Technique: Kerberoasting @ https://attack.mitre.org/techniques/T1558/003/
- Group Managed Service Accounts Overview @ https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

Affected Potential Credentials:

Username	Source	Service Type	Domain	Severity
svc_SOLARWINDS	Plaintext/Hash Dump			HIGH

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
04:57PM	svc_SOLARWINDS	kerb_tgs_hash		$k**********e5	Plaintext/Hash Dump		

2.3.31. H3-2021-0034: LLMNR Poisoning Possible

Severity: HIGH

Description:

Link-Local Multicast Name Resolution (LLMNR) is one of two components of Microsoft Windows machines that server as alternate methods of host identification. An attacker can spoof a reply as an authoritative source to a victim request and capture the credential information passed over the network. Credential information can be captured in hashed or plaintext format.

Impact: REMOTE CODE EXECUTION PRIVILEGE ESCALATION

A captured hash credential can be cracked offline to discover the plaintext password for reuse on other systems or the hash can be relayed and used to access other systems as well. Likewise, a captured plaintext credential can be immediately used to access other systems.

Mitigations:

- Disable LLMNR using Group Policy to enable 'Turn OFF Multicast Name Resolution' setting under 'Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client'.

References:

- T1171 - LLMNR/NBT-NS Poisoning and Relay @ https://attack.mitre.org/techniques/T1171/
- Local Network Vulnerabilities - LLMNR and NTB-NS Poisoning @ https://www.surecloud.com/services/news/local-network-vulnerabilities-llmnr-nbt-ns-poisoning
- LLMNR and NBT-NS Mitigation @ https://cccsecuritycenter.org/remediation/llmnr-nbt-ns

Affected Hosts:

IP	Host Name	Operating System	Severity
10.0.220.51	win7.smoke.net	Linux, Microsoft Windows	HIGH

Related Potential Credentials:

First Seen	User	Key Type	Password	Hash	Source	Domain	Service Type
05:01PM	a-jsmith	ntlmv2_hash		a-**********00	Man In The Middle	SMOKE	smb_user

2.3.32. H3-2021-0031: Public Access to Git Repository

Severity: HIGH

Description:

A Git repository that your company may own is publicly accessible.

Impact: INFORMATION DISCLOSURE

Attackers may be able to identify sensitive data in the source code stored in the repository.

Mitigations:

- Confirm the repository should be publicly accessible, and if not remove public access and only allow authorized users to access the repository.

- Review and regularly audit the source code stored in the repository for sensitive data that should not be publicly exposed.

References:

- Security Best Practices for GitHub Enterprise Server @ https://github.blog/2019-12-05-security-best-practices-for-github-enterprise-server/
- Security Best Practices for Git Users @ https://resources.infosecinstitute.com/topic/security-best-practices-for-git-users/
- 10 GitHub Security Best Practices @ https://snyk.io/blog/ten-git-hub-security-best-practices/
- Removing sensitive data from a repository @ https://docs.github.com/en/github/authenticating-to-github/removing-sensitive-data-from-a-repository

Affected Repositories:

Name	Service Type	IP	Port	Severity
fakegit2	Bitbucket: kbuch07			HIGH
fakegit2	GitLab: kbuch			HIGH
webdl	Bitbucket: kbuch07			HIGH
Test_truffle	GitLab: kbuch			HIGH
secret_test	GitLab: kbuch			HIGH
fakegit	Bitbucket: kbuch07			HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:32PM	No			Anonymous	N/A			fakegit2	read	2
04:32PM	No			Anonymous	N/A			secret_test	read	2
04:32PM	No			Anonymous	N/A			Test_truffle	read	2
04:32PM	No			Anonymous	N/A			webdl	read	7
04:32PM	No			Anonymous	N/A			fakegit2	read	2
04:32PM	No			Anonymous	N/A			fakegit	read	2

2.3.33. H3-2021-0015: Weak or Default Credentials - SNMP

Severity: MEDIUM

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
		Brute Force	SNMP	10.0.225.100	udp/161	MEDIUM
		Brute Force	SNMP	10.0.225.100	udp/161	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:46PM	Yes			Brute Force	10.0.225.100	udp/161	SNMP		read,write	0
04:46PM	Yes			Brute Force	10.0.225.100	udp/161	SNMP		read	0

2.3.34. H3-2021-0036: Unauthenticated Access to Elasticsearch

Severity: MEDIUM

Description:

Elasticsearch is a distributed search engine, commonly used for log aggregation and analysis. Unauthenticated access to Elasticsearch allows attackers to retrieve and potentially alter data in the cluster.

Impact: UNAUTHORIZED ACCESS INFORMATION DISCLOSURE FILE UPLOAD

Attackers can access sensitive data stored in the Elasticsearch cluster, such as plain-text passwords, operational intelligence, and business-critical information. Attackers with write access can tamper with data and reconfigure the cluster.

Mitigations:

- Require authentication to access the Elasticsearch cluster. Enabling xpack.security.enabled=True in the configuration file will disable anonymous access.

References:

- Set up Minimal Security for Elasticsearch @ https://www.elastic.co/guide/en/elasticsearch/reference/current/security-minimal-setup.html

Affected Applications:

Name	VHost	IP	Port	Severity
elasticsearch		10.0.40.56	tcp/9200	MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:38PM	No			Anonymous	10.0.40.56	tcp/9200	Web			1

2.3.35. H3-2020-0002: Anonymous Access to ZooKeeper API

Severity: MEDIUM

Description:

The ZooKeeper API accepts anonymous connections.

Impact: FILE UPLOAD DENIAL OF SERVICE UNAUTHORIZED ACCESS

Attackers could perform denial-of-service (DoS) attacks by killing services or uploading large files to fill up the filesystem.

Mitigations:

- Configure authentication if possible or at least configure ACLs on the ZooKeeper API if authentication is not possible.

References:

- CWE-284: Improper Access Control @ https://cwe.mitre.org/data/definitions/284.html
- ZooKeeper Security @ https://docs.confluent.io/current/security/zk-security.html
- Configuring ZooKeeper @ https://access.redhat.com/documentation/en-us/red_hat_amq/7.2/html/using_amq_streams_on_red_hat_enterprise_linux_rhel/configuring_zookeeper

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.100	tcp/2181	eforward		MEDIUM

2.3.36. H3-2020-0003: Anonymous Access to Printer using PJL or PS

Severity: MEDIUM

Description:

The remote host is a printer that is open to anonymous HP Printer Job Language (PJL) or Postscript (PS) commands.

Impact: DEFACEMENT FILE UPLOAD REMOTE CODE EXECUTION INFORMATION DISCLOSURE DENIAL OF SERVICE UNAUTHORIZED ACCESS

Attackers can manipulate and capture print jobs, recover passwords stored on the printer file system, or perform physical damage against the printer.

Mitigations:

- Disable printing over port 9100, or disable anonymous access by configuring passwords for PJL and file system access.

References:

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor @ https://cwe.mitre.org/data/definitions/200.html
- Printer Exploitation Toolkit @ https://github.com/RUB-NDS/PRET

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.100	tcp/9100	jetdirect	HP JetDirect	MEDIUM

2.3.37. H3-2020-0004: Zone Transfer Allowed to Any Server

Severity: MEDIUM

Description:

The remote DNS server allows zone transfers to any server. Zone transfers are used to replicate DNS data across multiple DNS servers.

Impact: INFORMATION DISCLOSURE DENIAL OF SERVICE

Allowing zone transfers to any server provides an attacker with information that can be used to identify target systems. This information may be used to carry out additional attacks.

Mitigations:

- Only allow zone transfers to servers that require the information.

References:

- CAPEC-291: DNS Zone Transfers @ https://capec.mitre.org/data/definitions/291.html
- AXFR Requests May Leak Domain Information @ https://www.us-cert.gov/ncas/alerts/TA15-103A

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.2	tcp/53	domain	Microsoft DNS 6.1.7601 (1DB1446A)	MEDIUM

2.3.38. H3-2021-0001: Public Access to Amazon S3 Bucket

Severity: MEDIUM

Description:

An Amazon S3 bucket that your company may own is publicly accessible, either to everyone or any authenticated (cross-account) AWS user.

Impact: INFORMATION DISCLOSURE UNAUTHORIZED ACCESS DEFACEMENT FILE UPLOAD

Attackers may be able to access sensitive data hosted in the bucket. Depending on bucket permissions, attackers may be able to delete objects in the bucket, upload new objects to the bucket, modify existing objects in the bucket, or modify bucket and object permissions

Mitigations:

- Verify that the bucket is in fact owned by your company. The bucket that was found has a name similar to one of your company's subdomains.
- Review the data contained in the bucket, and remove any data that should not be exposed.
- Review bucket and object permissions for anonymous and any authenticated (cross-account) AWS users. Apply least-privilege permissions as appropriate.

References:

- Security Best Practices for AWS S3 @ https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html
- How can I secure the files in my Amazon S3 bucket? @ https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/

Affected Repositories:

Name	Service Type	IP	Port	Severity
doodle.h3ai.io	AWS S3			MEDIUM
11285521401250	AWS S3			MEDIUM

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:43PM	No			Anonymous	N/A		AWS S3	doodle.h3ai.io	list,read	2
04:43PM	No			Cross-Account	N/A		AWS S3	doodle.h3ai.io	list,read,read_acl	2
04:44PM	No			Anonymous	N/A		AWS S3	11285521401250	list,read	1
04:44PM	No			Cross-Account	N/A		AWS S3	11285521401250	list,read	1

2.3.39. H3-2020-0007: SMB Null Session Allowed

Severity: LOW

Description:

A specific type of weak share permissions, SMB null sessions allow unauthenticated connections from remote systems.

Impact: INFORMATION DISCLOSURE REMOTE CODE EXECUTION FILE UPLOAD UNAUTHORIZED ACCESS

Null sessions do not require credentials and can expose information to be used in further attacks.

Mitigations:

- Disable SMB Null Sessions if not needed using Group Policy or other enterprise configuration management solution.
- If SMB Null Sessions are required, implement strong NTFS permissions for more granular access control to authorized resources.

References:

- CWE-284: Improper Access Control @ https://cwe.mitre.org/data/definitions/284.html
- Network security: Allow LocalSystem NULL session fallback @ https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-localsystem-null-session-fallback
- Share Permissions @ http://techgenix.com/share-permissions/

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.50.2	tcp/445	netbios-ssn	Samba Smbd 4.6.2	LOW
10.0.220.51	tcp/445	microsoft-ds		LOW
10.0.220.54	tcp/445	microsoft-ds	Microsoft Windows XP Microsoft-ds	LOW
10.0.220.55	tcp/445	microsoft-ds	Microsoft Windows 2003 Or 2008 Microsoft-ds	LOW
10.0.225.2	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW
10.0.229.1	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW
10.0.229.2	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	LOW

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:33PM	No			Anonymous	10.0.50.2	tcp/445	SMB	TV Shows	read	2,090

2.3.40. CVE-2020-1472: Netlogon Elevation of Privilege Vulnerability Zerologon

Severity: CRITICAL

Description:

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), aka 'Netlogon Elevation of Privilege Vulnerability'.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

A vulnerability exists in the Netlogon Remote Protocol that allows an unauthenticated, remote attacker to gain access to the Domain Controller's machine account. This account has Domain Administrator rights which can allow the attacker to fully compromise the domain and execute arbitray code on any domain joined systems.

Mitigations:

- Apply the updates referenced in Microsoft Security Bulletin CVE-2020-1472 and configure the registry key that will enable Enforcement Mode.
- On February 9, 2021 a Windows Update will automatically enable Enforcement Mode on all Domain Controllers regardless of the registry key value.

References:

- CVE-2020-1472 @ https://nvd.nist.gov/vuln/detail/CVE-2020-1472
- Microsoft Security Bulletin CVE-2020-1472 @ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
- Microsoft Registry Key for Enforcement Mode @ https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc#EnforcementMode

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.229.1	tcp/445	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	CRITICAL

2.3.41. CVE-2021-21972: VMware vCenter vROPS Plugin Remote Code Execution Vulnerability

Severity: CRITICAL

Description:

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).

Impact: FILE UPLOAD REMOTE CODE EXECUTION UNAUTHORIZED ACCESS

Unauthenticated attackers with network access to a vulnerable VMware vCenter Server can gain full control of the server by exploiting this vulnerability.

Mitigations:

- Apply all updates and patch to the latest vendor-supported version.
- Apply workarounds described in VMware KB82374.

References:

- CVE-2021-21972 @ https://nvd.nist.gov/vuln/detail/CVE-2021-21972
- Proof of Concept for CVE-2021-21972 @ https://github.com/horizon3ai/CVE-2021-21972/
- VMware Advisory VMSA-2021-0002 @ https://www.vmware.com/security/advisories/VMSA-2021-0002.html
- VMware KB82374 @ https://kb.vmware.com/s/article/82374

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.40.99	tcp/443	https	VMware vSphere Http Config	CRITICAL

2.3.42. CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability BlueKeep

Severity: HIGH

Description:

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'.

Impact: REMOTE CODE EXECUTION UNAUTHORIZED ACCESS PRIVILEGE ESCALATION

Vulnerable systems allow an attacker to gain complete control of the target system. This provides a point of presence in the network to conduct further reconnaissance, gather sensitive information, and launch advanced attacks to move laterally throughout the environment.

Mitigations:

- Apply the patches released on May 19, 2019 by Microsoft.
- Disable remote desktop services if not required. Enable Network Level Authentication (NLA).

References:

- CVE-2019-0708 @ https://nvd.nist.gov/vuln/detail/CVE-2019-0708
- Microsoft Updates: CVE-2019-0708 @ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- Customer guidance for CVE-2019-0708 @ https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.225.2	tcp/3389	ms-wbt-server		CRITICAL

2.3.43. H3-2021-0013: Weak or Default Credentials - Telnet

Severity: HIGH

Description:

Weak credentials include passwords that are easily obtained by password guessing, password spraying, or cracked using dictionary attacks. Default passwords are publicly known and obtainable by an attacker and provide immediate access to a system.

Impact: REMOTE CODE EXECUTION INFORMATION DISCLOSURE UNAUTHORIZED ACCESS FILE UPLOAD

An attacker can openly maneuver throughout an environment and access information if a password is compromised.

Mitigations:

- Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.
- Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.
- Implement multi-factor authentication where possible.

References:

- CWE-521: Weak Password Requirements @ https://cwe.mitre.org/data/definitions/521.html
- T1110: Brute Force @ https://attack.mitre.org/techniques/T1110/

Affected Credentials:

Username	Role	Source	Service Type	IP	Port	Severity
root	LOCAL_USER	Default Login	Telnet	10.0.225.100	tcp/23	HIGH

Related Credentials & Resources:

First Seen	Proof	Username	Role	Source	IP	Port	Service Type	Name	Permissions	Total Resources
04:33PM	No	root	LOCAL_USER	Default Login	10.0.225.100	tcp/23	Telnet			0

2.3.44. H3-2021-0024: Dangling DNS Record

Severity: LOW

Description:

The DNS record for a subdomain has a CNAME record that points to another subdomain that is not in use or does not resolve to an IP address.

Impact: DEFACEMENT IMPERSONATION

A dangling DNS record gives attackers an opportunity to attempt a subdomain takeover. By taking over a legitimate looking company domain, attackers can trick users through phishing campaigns, attempt to steal user cookies and passwords, deface the company web site and damage the company brand.

Mitigations:

- If the subdomain is not in use, remove the stale DNS record for it.
- If the subdomain is in use, set its CNAME record to a valid DNS hostname.

References:

- Subdomain Takeovers: Thoughts on Risk @ https://0xpatrik.com/subdomain-takeover/
- Prevent Dangling DNS Entries and Avoid Subdomain Takeover @ https://docs.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

Affected External Domains:

Domain	CNAME	IP Addresses	Severity
doodle.h3ai.io	11285521401250.s3-website.us-east-2.amazonaws.com	52.219.102.44	LOW

2.3.45. H3-2021-0025: Expired SSL/TLS Certificate

Severity: LOW

Description:

The SSL/TLS certificate has expired or is close to expiring.

Impact: IMPERSONATION

An expired certificate causes browser security warnings to appear when a user browses to the web site using the certificate. These warnings erode user trust in the web site and create alert fatigue. Attackers can take advantage of this by launching man-in-the-middle attacks using a fraudulent certificate and trick users into divulging confidential information. If the web site uses HTTP Strict Transport Security (HSTS) and has an expired certificate, users won't be able to browse to it at all.

Mitigations:

- Renew the certificate.
- If not in use, shut down the web site with the expired certificate.

References:

- Let's Encrypt @ https://letsencrypt.org/docs/
- Public Key Certificate @ https://en.wikipedia.org/wiki/Public_key_certificate

- HTTP Strict Transport Security @ https://https.cio.gov/hsts/

Affected Services:

IP	Port	IANA Service Name	Product	Severity
10.0.100.100	tcp/443	https	ATEN/Supermicro IPMI Web Interface, Supermicro Intelligent Platform Management Firmware	LOW
10.0.225.100	tcp/4443	https	Apache HTTPD 2.4.46	LOW

3. Appendices

3.1. Credentials

The pentest captured **36 confirmed credentials** (with proof-of-access) and **104 potential credentials**.

3.1.1. Confirmed Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
04:57PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.11:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:58PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:33PM	root	STANDARD	mysql	Default Login	10.0.225.100:3306	3306	MySQL 8.0.20
04:59PM	a-jsmith	STANDARD	microsoft-ds	Cracked	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:33PM	sa	STANDARD	ms-sql-s	Default Login	10.0.225.100:1433	1433	Microsoft SQL Server 2019 15.00.4033
05:00PM	postgres	STANDARD	postgresql	Default Login	10.0.225.100:5433	5433	PostgreSQL DB 11.3 - 11.7
04:37PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.225.2:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:39PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.52:445	445	Microsoft Windows 7 - 10 Microsoft-ds
04:40PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds
04:37PM	user	STANDARD	ssh	Default Login	10.0.40.56:22	22	OpenBSD OpenSSH 7.6p1 Ubuntu 4ubuntu0.5
04:36PM	admin	STANDARD	ssh	Default Login	10.0.225.100:22	22	OpenBSD OpenSSH 7.6p1 Ubuntu 4ubuntu0.5
04:39PM	tomcat	STANDARD	http	Default Login	10.0.40.103:80	80	Apache Tomcat 9.0.30, Igor Sysoev Nginx
04:57PM	jsmith	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.51:445 10.0.220.52:445 10.0.225.2:445 10.0.229.11:445 10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
04:34PM	Guest	STANDARD	microsoft-ds	Anonymous	10.0.220.51:3389 10.0.220.51:445	445	
05:09PM	nsunkavally	STANDARD	microsoft-ds	Cracked	10.0.220.51:445 10.0.220.52:445 10.0.225.2:445 10.0.229.11:445 10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:42PM	user	STANDARD	microsoft-ds	Man In The Middle	10.0.220.51:445	445	
04:57PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.11:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:39PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.51:445	445	
04:46PM		SNMP_COMMUNITY_STRING	snmp	Brute Force	10.0.225.100:161	161	Net-SNMP SNMP Agent
04:46PM		SNMP_COMMUNITY_STRING	snmp	Brute Force	10.0.225.100:161	161	Net-SNMP SNMP Agent
04:56PM	anonymous	STANDARD	ftp	Anonymous	10.0.229.11:21	21	Microsoft Ftpd, Microsoft IIS
04:41PM	user	STANDARD	microsoft-ds	Man In The Middle	10.0.220.52:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05:01PM	admin	STANDARD	http	Default Login	10.0.225.100:8161	8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131
05:01PM	user	STANDARD	http	Default Login	10.0.225.100:8161	8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131
04:58PM	ns$	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
05:10PM	svc_TESTGMSA2$	STANDARD	microsoft-ds	ldap_get_gmsa	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
05:00PM	fs$	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:39PM	ADMIN	STANDARD	http	Default Login	10.0.100.100:80	80	ATEN/Supermicro IPMI Web Interface, Supermicro Intelligent Platform Management Firmware
04:46PM	anonymous	STANDARD	ftp	Anonymous	10.0.225.100:9090	9090	vsFTPd Project vsFTPd 3.0.3
04:47PM	root	STANDARD	asf-rmcp	Plaintext/ Hash Dump	10.0.100.101:623	623	
04:45PM	ADMIN	STANDARD	asf-rmcp	Plaintext/ Hash Dump	10.0.100.100:623	623	
04:40PM	iwam_win2k3	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
04:41PM	aspnet	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds
04:38PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.225.2:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:40PM	iusr_win2k3	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds
04:33PM	Guest	STANDARD	netbios-ssn	Anonymous	10.0.50.2:445	445	Samba Smbd 4.6.2

3.1.2. Potential Credentials

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
04:57PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.11:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:58PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:33PM	root	STANDARD	mysql	Default Login	10.0.225.100:3306	3306	MySQL 8.0.20
04:59PM	a-jsmith	STANDARD	microsoft-ds	Cracked	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:33PM	sa	STANDARD	ms-sql-s	Default Login	10.0.225.100:1433	1433	Microsoft SQL Server 2019 15.00.4033
05:00PM	postgres	STANDARD	postgresql	Default Login	10.0.225.100:5433	5433	PostgreSQL DB 11.3 - 11.7
04:37PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.225.2:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:39PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.52:445	445	Microsoft Windows 7 - 10 Microsoft-ds
04:40PM	administrator	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds
04:37PM	user	STANDARD	ssh	Default Login	10.0.40.56:22	22	OpenBSD OpenSSH 7.6p1 Ubuntu 4ubuntu0.5
04:36PM	admin	STANDARD	ssh	Default Login	10.0.225.100:22	22	OpenBSD OpenSSH 7.6p1 Ubuntu 4ubuntu0.5
04:39PM	tomcat	STANDARD	http	Default Login	10.0.40.103:80	80	Apache Tomcat 9.0.30, Igor Sysoev Nginx
04:57PM	jsmith	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.51:445 10.0.220.52:445 10.0.225.2:445 10.0.229.11:445 10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
04:34PM	Guest	STANDARD	microsoft-ds	Anonymous	10.0.220.51:3389 10.0.220.51:445	445	
05:09PM	nsunkavally	STANDARD	microsoft-ds	Cracked	10.0.220.51:445 10.0.220.52:445 10.0.225.2:445 10.0.229.11:445 10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:42PM	user	STANDARD	microsoft-ds	Man In The Middle	10.0.220.51:445	445	
04:57PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.11:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:39PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.51:445	445	
04:46PM		SNMP_COMMUNITY_STRING	snmp	Brute Force	10.0.225.100:161	161	Net-SNMP SNMP Agent
04:46PM		SNMP_COMMUNITY_STRING	snmp	Brute Force	10.0.225.100:161	161	Net-SNMP SNMP Agent
04:56PM	anonymous	STANDARD	ftp	Anonymous	10.0.229.11:21	21	Microsoft Ftpd, Microsoft IIS
04:41PM	user	STANDARD	microsoft-ds	Man In The Middle	10.0.220.52:445	445	Microsoft Windows 7 - 10 Microsoft-ds
05:01PM	admin	STANDARD	http	Default Login	10.0.225.100:8161	8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131
05:01PM	user	STANDARD	http	Default Login	10.0.225.100:8161	8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131
04:58PM	ns$	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
05:10PM	svc_TESTGMSA2$	STANDARD	microsoft-ds	ldap_get_gmsa	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
05:00PM	fs$	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.229.1:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:39PM	ADMIN	STANDARD	http	Default Login	10.0.100.100:80	80	ATEN/Supermicro IPMI Web Interface, Supermicro Intelligent Platform Management Firmware
04:46PM	anonymous	STANDARD	ftp	Anonymous	10.0.225.100:9090	9090	vsFTPd Project vsFTPd 3.0.3
04:47PM	root	STANDARD	asf-rmcp	Plaintext/ Hash Dump	10.0.100.101:623	623	
04:45PM	ADMIN	STANDARD	asf-rmcp	Plaintext/ Hash Dump	10.0.100.100:623	623	
04:40PM	iwam_win2k3	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds

First Seen	Username	Type	Iana Svc Name	Source	IP Addr	Port	Product
04:41PM	aspnet	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds
04:38PM	xadmin	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.225.2:445	445	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds
04:40PM	iusr_win2k3	STANDARD	microsoft-ds	Plaintext/ Hash Dump	10.0.220.55:445	445	Microsoft Windows 2003 Or 2008 Microsoft-ds
04:33PM	Guest	STANDARD	netbios-ssn	Anonymous	10.0.50.2:445	445	Samba Smbd 4.6.2

3.2. Hosts

The pentest discovered **44 hosts** in the following subnets:

- **Included subnets:**
  10.0.220.0/24, 10.0.225.0/24, 10.0.229.0/24, 10.0.100.96/28, 10.0.50.2, 10.0.40.99, 10.0.40.56, 10.0.40.103
- **Excluded subnets:**
  10.0.225.101, 10.0.220.53, 10.0.220.56

3.2.1. In Scope Hosts

First Seen	Host Name	IP	OS	Weaknesses	Data Res	Creds	Services	Web
04:32PM	vcsa.smoke.net	10.0.40.99	VMware ESXi, VMware vCenter Server 6.7.0	3	0	0	19	3
04:32PM	win10.smoke.net	10.0.220.52	Microsoft Windows 10 Pro 10240	3	3	5	9	4
04:32PM	winxp	10.0.220.54	Microsoft Windows XP	4	0	0	10	0
04:32PM	win2k3	10.0.220.55	Microsoft Windows Server 2003 Service Pack 2 3790	4	2	4	13	2
04:32PM	ns.smoke.net	10.0.225.2	Microsoft Windows R2, Microsoft Windows Server 2008 R2 Service Pack 1 Enterprise 7601	7	3	5	16	0
04:32PM		10.0.225.100	Debian Linux, HP LaserJet 4200, Linux 4.15.0-101-generic, Ubuntu Linux 12.04.5, Unix	17	21	10	28	9
04:33PM	dc.smoke.net	10.0.229.1	Microsoft Windows Server 2012 R2 Standard 9600	4	4	7	26	7

First Seen	Host Name	IP	OS	Weaknesses	Data Res	Creds	Services	Web
04:33PM	fs.smoke.net	10.0.229.11	Microsoft Windows Server 2016 Standard 14393	4	7	6	10	2
04:32PM		10.0.220.254	Cisco IOS, Unix	1	0	0	3	0
04:35PM		10.0.229.254	Unix	1	0	0	3	0
04:32PM		10.0.40.56	Debian Linux	2	0	1	7	4
04:32PM		10.0.100.101		2	0	1	5	1
04:32PM		10.0.100.102		2	0	0	5	1
04:32PM	win7.smoke.net	10.0.220.51	Linux, Microsoft Windows	6	1	5	5	0
04:32PM		10.0.40.103	Linux	2	0	1	5	4
04:32PM		10.0.100.100	Linux, Supermicro Intelligent Platform Management Firmware	3	0	2	6	3
04:32PM	cronus.olympus	10.0.50.2	Linux	3	2	1	11	1
04:32PM		10.0.100.103		0	0	0	5	1
04:32PM		10.0.100.104		0	0	0	5	1
04:32PM		10.0.100.105		0	0	0	5	1
04:33PM	dc2.smoke.net	10.0.229.2	Microsoft Windows Server 2016 Standard 14393	1	0	0	26	12
04:35PM		10.0.225.254	Cisco IOS, Unix	0	0	0	3	0

3.2.2. Out of Scope Hosts

First Seen	Host Name	IP	OS	Weaknesses	Data Res	Creds	Services	Web
04:32PM	s3-website.us-east-2.amazonaws.com	52.219.102.44		2	0	0	0	0
04:32PM	rancher-external-alb-2063859640.us-east-1.elb.amazonaws.com	3.231.0.221		0	0	0	0	0
04:32PM	docker.develop.h3ai.io	3.233.178.136		0	0	0	0	0
04:33PM	ex.smoke.net	10.0.229.3		0	0	0	0	0
04:33PM	ex2.smoke.net	10.0.229.4		0	0	0	0	0
04:33PM	tomcat.smoke.net	10.0.229.10		0	0	0	0	0
04:33PM	zachhanley2255.smoke.net	10.211.55.5		0	0	0	0	0
04:32PM	docker.develop.h3ai.io	18.204.152.120		0	0	0	0	0

First Seen	Host Name	IP	OS	Weaknesses	Data Res	Creds	Services	Web
04:32PM	docker.develop.h3ai.io	18.208.105.53		0	0	0	0	0
04:32PM	portal.develop.h3ai.io	18.210.164.76		0	0	0	0	0
04:32PM	api.develop.h3ai.io	34.200.69.32		0	0	0	0	0
04:32PM	api.develop.h3ai.io	34.233.74.89		0	0	0	0	0
04:32PM	portal.develop.h3ai.io	34.235.51.190		0	0	0	0	0
04:32PM	docker-nexus.h3ai.io	50.19.164.167		0	0	0	0	0
04:32PM	rancher-external-alb-2063859640.us-east-1.elb.amazonaws.com	52.22.126.123		0	0	0	0	0
04:32PM	docker-nexus.h3ai.io	52.54.208.186		0	0	0	0	0
04:32PM	rancher-external-alb-2063859640.us-east-1.elb.amazonaws.com	52.204.6.221		0	0	0	0	0
04:32PM	11285521401250.s3-website.us-east-2.amazonaws.com	52.219.96.19		0	0	0	0	0
04:32PM	11285521401250.s3-website.us-east-2.amazonaws.com	52.219.107.64		0	0	0	0	0
04:32PM	portal.develop.h3ai.io	54.80.43.16		0	0	0	0	0
04:32PM	api.develop.h3ai.io	54.87.180.67		0	0	0	0	0
04:32PM	docker-nexus.h3ai.io	100.25.195.81		0	0	0	0	0

3.3. Data Resources

The pentest discovered **7.4M data resources** on **53 stores** containing potentially sensitive information.

Git Repositories

Source	Account Name	Name	Clone Url	Forked	Sensitive Findings	Severity
GitLab	kbuch	fakegit2	https://gitlab.com/kbuch/fakegit2.git		2	HIGH

Source	Account Name	Name	Clone Url	Forked	Sensitive Findings	Severity
Bitbucket	kbuch07	webdl	https://bitbucket.org/kbuch07/webdl.git	true	7	HIGH
GitLab	kbuch	secret_test	https://gitlab.com/kbuch/secret_test.git	true	2	HIGH
Bitbucket	kbuch07	fakegit	https://bitbucket.org/kbuch07/fakegit.git		2	HIGH
GitLab	kbuch	Test_truffle	https://gitlab.com/kbuch/test_truffle.git		2	HIGH
Bitbucket	kbuch07	fakegit2	https://bitbucket.org/kbuch07/fakegit2.git		2	HIGH

S3 Buckets

Name	Service	Resources Count	Permissions	Severity
doodle.h3ai.io	AWS S3	4	list,read,read_acl	LOW
11285521401250	AWS S3	2	list,read	LOW
h3ai-web	AWS S3	0		INFO
h3ai	AWS S3	0		INFO

Databases

Service Name	IP	Port	Database Name	Total Records	Permissions	Authenticated	Severity
MySQL	10.0.225.100	tcp/3306	employees	3,919,015	list,read,write	true	HIGH
PostgreSQL	10.0.225.100	tcp/5433	postgres	2,141,275	list,read,write	true	HIGH
MySQL	10.0.225.100	tcp/3306	performance_schema	358,456	list,read,write	true	HIGH

Service Name	IP	Port	Database Name	Total Records	Permissions	Authenticated	Severity
MySQL	10.0.225.100	tcp/3306	mysql	141,445	list,read,write	true	HIGH
Microsoft SQL Server	10.0.225.100	tcp/1433	Northwind	3,308	list,read,write	true	MEDIUM
Microsoft SQL Server	10.0.225.100	tcp/1433	AdventureWorks2017	1,597	list,read,write	true	MEDIUM
Microsoft SQL Server	10.0.225.100	tcp/1433	msdb	1,619	list,read,write	true	MEDIUM
Microsoft SQL Server	10.0.225.100	tcp/1433	Pubs	255	list,read,write	true	MEDIUM
MySQL	10.0.225.100	tcp/3306	sys	6	list,read,write	true	MEDIUM
Microsoft SQL Server	10.0.225.100	tcp/1433	master	4	list,read,write	true	MEDIUM
Microsoft SQL Server	10.0.225.100	tcp/1433	WideWorldImporters	0	list,read,write	true	MEDIUM
Microsoft SQL Server	10.0.225.100	tcp/1433	model	0	list,read,write	true	MEDIUM
MySQL	10.0.225.100	tcp/3306	information_schema	0	list,read,write	true	MEDIUM
PostgreSQL	10.0.225.100	tcp/5433	template1	0	list,read,write	true	MEDIUM
PostgreSQL	10.0.225.100	tcp/5433	template0	0	list	true	INFO
Microsoft SQL Server	10.0.225.100	tcp/1433	tempdb	0	list	true	INFO

File Shares

Type	IP	Port	Share Name	Product	Files	Permissions	Authenticated	Severity
SMB	10.0.229.1	tcp/445	C$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	101,819	read,write	true	CRITICAL
SMB	10.0.229.11	tcp/445	C$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	113,316	read,write	true	CRITICAL
SMB	10.0.225.2	tcp/445	C$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	61,543	read,write	true	HIGH
SMB	10.0.229.11	tcp/445	ADMIN$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	102,036	read,write	true	HIGH
SMB	10.0.225.2	tcp/445	ADMIN$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	59,824	read,write	true	HIGH
SMB	10.0.229.1	tcp/445	ADMIN$	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	93,422	read,write	true	HIGH
SMB	10.0.220.51	tcp/445	Guests		250,006	read,write	true	HIGH
SMB	10.0.220.55	tcp/445	C$	Microsoft Windows 2003 Or 2008 Microsoft-ds	14,657	read,write	true	HIGH

Type	IP	Port	Share Name	Product	Files	Permissions	Authenticated	Severity
SMB	10.0.220.52	tcp/445	Visitors	Microsoft Windows 7 - 10 Microsoft-ds	2	read,write	true	HIGH
SMB	10.0.220.52	tcp/445	Bitnami	Microsoft Windows 7 - 10 Microsoft-ds	20,060	read,write	true	HIGH
SMB	10.0.220.55	tcp/445	ADMIN$	Microsoft Windows 2003 Or 2008 Microsoft-ds	14,101	read,write	true	HIGH
SMB	10.0.229.11	tcp/445	FTP	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	169	read,write	true	MEDIUM
FTP	10.0.229.11	tcp/21		Microsoft Ftpd, Microsoft IIS	169	read,write		MEDIUM
NFS	10.0.225.2	tcp/2049	/Logs		152	read,write		MEDIUM
SMB	10.0.229.11	tcp/445	Users	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	2	read,write	true	MEDIUM
SMB	10.0.229.1	tcp/445	NETLOGON	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	0	read,write	true	MEDIUM
SMB	10.0.229.11	tcp/445	Public	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	1	read,write	true	MEDIUM
SMB	10.0.229.11	tcp/445	CertEnroll	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	1	read,write	true	MEDIUM
SMB	10.0.50.2	tcp/445	TV Shows	Samba Smbd 4.6.2	2,090	read		LOW
SMB	10.0.220.52	tcp/445	Users	Microsoft Windows 7 - 10 Microsoft-ds	2,025	read	true	LOW
FTP	10.0.225.100	tcp/9090		vsFTPd Project vsFTPd 3.0.3	149	read		LOW
SMB	10.0.229.1	tcp/445	SYSVOL	Microsoft Windows Server 2008 R2 - 2012 Microsoft-ds	21	read	true	LOW
SMB	10.0.50.2	tcp/445	Movies	Samba Smbd 4.6.2	0	read		INFO

Docker Registries

IP	Port	Registry Name	Product	Permissions	Authenticated	Severity
10.0.225.100	tcp/5001	test/test	Redhat Docker Registry	list,read,write		MEDIUM
10.0.225.100	tcp/5001	busybox	Redhat Docker Registry	list,read,write		MEDIUM
10.0.225.100	tcp/5001	python	Redhat Docker Registry	list,read,write		MEDIUM
10.0.225.100	tcp/5001	ubuntu	Redhat Docker Registry	list,read,write		MEDIUM

3.4. Web Resources & Certificates

The pentest crawled **183 web resources** on **56 web applications** and discovered **13 web certificates** containing potentially sensitive information.

3.4.1. Applications

First Seen	IP	Port	Product	Total Resources	Login Pages
04:32PM	10.0.40.103	tcp/80	Apache Tomcat 9.0.30, Igor Sysoev Nginx	67	1
04:32PM	10.0.225.100	tcp/4443	Apache HTTPD 2.4.46	18	0
04:32PM	10.0.225.100	tcp/8080	Eclipse Jetty 9.4.27.v20200227, Jenkins	16	2
04:56PM	10.0.225.100	tcp/8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131	12	1
04:56PM	10.0.225.100	tcp/8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131	12	1
04:32PM	10.0.40.103	tcp/80	Apache Tomcat 9.0.30, Igor Sysoev Nginx	5	1
04:32PM	10.0.40.99	tcp/443	VMware vSphere Http Config	2	0
04:56PM	10.0.225.100	tcp/8161	Apache ActiveMQ, Eclipse Jetty 7.6.9.v20130131	2	1
04:32PM	10.0.40.103	tcp/8080	Apache Solr	2	0
04:32PM	10.0.40.56	tcp/9200	Elasticsearch Kibana, Elasticsearch REST API 7.15.0	1	0
04:32PM	10.0.225.100	tcp/8443	Apache HTTPD 2.2.22	1	0
04:56PM	10.0.225.100	tcp/61614	Eclipse Jetty 7.6.9.v20130131	1	0
04:32PM	10.0.100.100	tcp/443	ATEN/Supermicro IPMI Web Interface, Supermicro Intelligent Platform Management Firmware	1	2
04:32PM	10.0.100.103	tcp/443	Mbedthis Mbedthis-Appweb 2.4.2, Mbedthis Software Appweb 2.4.2	1	0
04:32PM	10.0.220.55	tcp/80	Microsoft IIS 6.0, Microsoft IIS Httpd 6.0	1	0
04:32PM	10.0.220.55	tcp/80	Microsoft IIS 6.0, Microsoft IIS Httpd 6.0	1	0
04:32PM	10.0.40.56	tcp/8000	Apache HTTPD 2.4.48	1	0
04:56PM	10.0.229.11	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.11	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:32PM	10.0.40.56	tcp/8081	Apache HTTPD 2.4.38, Glpi Project	1	1
04:56PM	10.0.40.99	tcp/5480	Lighttpd 1.4.45	1	1
04:56PM	10.0.40.99	tcp/5480	Lighttpd 1.4.45	1	1
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0

First Seen	IP	Port	Product	Total Resources	Login Pages
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0
04:56PM	10.0.229.1	tcp/80	Microsoft IIS 8.5, Microsoft IIS Httpd 8.5	1	0
04:56PM	10.0.229.2	tcp/443	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/443	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/443	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/443	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/443	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/443	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:32PM	10.0.40.103	tcp/8081	Edgecast CDN Httpd	1	0
04:32PM	10.0.220.52	tcp/80	Apache HTTPD	1	0
04:32PM	10.0.220.52	tcp/80	Apache HTTPD	1	0
04:32PM	10.0.100.102	tcp/443	Mbedthis Mbedthis-Appweb 2.4.2, Mbedthis Software Appweb 2.4.2	1	0
04:56PM	10.0.229.2	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:56PM	10.0.229.2	tcp/80	Microsoft IIS 10.0, Microsoft IIS Httpd 10.0	1	0
04:32PM	10.0.100.104	tcp/443	Mbedthis Mbedthis-Appweb 2.4.2, Mbedthis Software Appweb 2.4.2	1	0
04:32PM	10.0.225.100	tcp/8000	Apache HTTPD 2.4.50	1	0
04:32PM	10.0.100.101	tcp/443	Mbedthis Mbedthis-Appweb 2.4.2, Mbedthis Software Appweb 2.4.2	1	0
04:32PM	10.0.40.56	tcp/80	Apache HTTPD 2.4.48	1	0
04:32PM	10.0.225.100	tcp/8888	Apache HTTPD 2.4.49	1	0
04:32PM	10.0.100.105	tcp/443	Mbedthis Mbedthis-Appweb 2.4.2, Mbedthis Software Appweb 2.4.2	1	0
04:32PM	10.0.100.100	tcp/80	ATEN/Supermicro IPMI Web Interface, Supermicro Intelligent Platform Management Firmware	1	2

First Seen	IP	Port	Product	Total Resources	Login Pages
04:32PM	10.0.100.100	tcp/80	ATEN/Supermicro IPMI Web Interface, Supermicro Intelligent Platform Management Firmware	1	2
04:32PM	10.0.50.2	tcp/443	Igor Sysoev Nginx	1	1
04:32PM	10.0.220.52	tcp/443	Apache HTTPD	1	0
04:32PM	10.0.220.52	tcp/443	Apache HTTPD	1	0

3.4.2. Certificates

First Seen	IP	Port	Expiration	Issuer	Common Name	Signed?
04:36PM	10.0.100.100	443	03/16/18	IPMI (Super Micro Computer from US)	IPMI	No
04:38PM	10.0.220.52	443	10/3/31	www.example.com (Bitnami)	www.example.com	No
04:38PM	10.0.50.2	443	01/30/30	KERBEROS-CA (HOME from US)	SAN-02	No
04:39PM	10.0.40.99	443	09/24/30	vcsa.smoke.net (vcsa.smoke.net from US)	vcsa.smoke.net	No
04:40PM	10.0.100.101	443				Yes
04:40PM	10.0.100.103	443				Yes
04:42PM	10.0.100.105	443	06/4/24	iDRAC6 default certificate (Dell Inc. from US)	iDRAC6 default certificate	No
04:43PM	10.0.100.102	443	06/4/24	iDRAC6 default certificate (Dell Inc. from US)	iDRAC6 default certificate	No
04:43PM	10.0.100.104	443		C=US,ST=Texas,L=Round Rock,O=Dell Inc.,OU=Remote Access Group,CN=iDRAC6 default certificate		Yes
04:45PM	10.0.225.100	8443	08/1/25	c2712433a4da	c2712433a4da	No
04:46PM	10.0.225.100	4443	07/27/21	Internet Widgits Pty Ltd from AU		No
04:59PM	10.0.229.2	443	05/6/20	smoke-DC2-CA (smoke.net)	smoke-DC2-CA	No
05:03PM	10.0.40.99	5480	09/24/30	vcsa.smoke.net (vcsa.smoke.net from US)	vcsa.smoke.net	No

3.5. Services

The pentest scanned **225 services** during the operation.