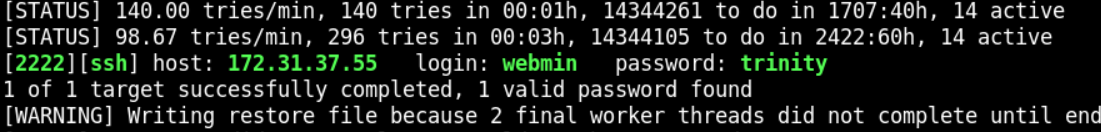
**KALI: 172.31.37.101/20**

* **(172.31.37.55)**



**define( 'DB\_PASSWORD', '5PR1NG2021@' );**

**| 1 | admin | $P$BHU6FQGrmyWtcwlDOsqPe0nrIDZZ7A/ | admin | admin@vanguard.local**

**| 2 | flag\_hunter | b25lYm94ZG93bgo= | Flag Hunter | flagman@flags.com**

**| 3 | webmin | ee2055701c742262f93d083f854350b9 | webmin | webmin@vanguard.local**

**| 4 | charlie-winrm | 7bb59d53b3688ad2e65c05e07f7f1529 | charlie-WS01 | charlie@hq.vanguard.bank**

**FLAG DE FLAG\_HUNTER DECODE64: oneboxdown**

**mysql -h localhost -uwordpress –p 5PR1NG2021@**

# Automatically generated for Debian scripts. DO NOT TOUCH!

[client]

host = localhost

user = debian-sys-maint

password = **WtHX8CsjqWrvKB22**

socket = /var/run/mysqld/mysqld.sock

[mysql\_upgrade]

host = localhost

user = debian-sys-maint

password = WtHX8CsjqWrvKB22

socket = /var/run/mysqld/mysqld.sock

mysql> select User,authentication\_string from user;

+------------------+------------------------------------------------------------------------+

| User | authentication\_string |

+------------------+------------------------------------------------------------------------+

| debian-sys-maint | $A$005$qa▒[+s(X/2aeLmzPhpimZeHT0MvNhWaf1hQ5j8ZDGgDOwtwb33qtNpweAMR2 |

| root | |

| wordpress | $A$005$K.v Mr2Y] jClKGt3a8CzsVSchG1jWzKIW6tbuCdGPMSjdOuwlET8R33 |

* **(172.31.37.83)**

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3389/tcp open ms-wbt-server

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

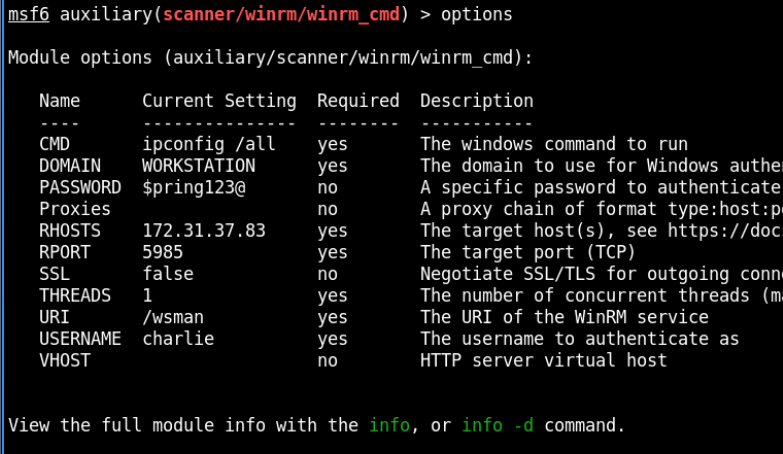
49669/tcp open unknown

49670/tcp open unknown

49679/tcp open unknown

49680/tcp open unknown

MAC Address: 02:8F:03:CA:D8:FF (Unknown)





orest : vanguard.bank

DomainControllers : {DC02.hq.vanguard.bank}

Children : {}

DomainMode : Unknown

DomainModeLevel : 7

Parent : vanguard.bank

PdcRoleOwner : DC02.hq.vanguard.bank

RidRoleOwner : DC02.hq.vanguard.bank

InfrastructureRoleOwner : DC02.hq.vanguard.bank

Name : hq.vanguard.bank

Get-DomainSID

S-1-5-21-1599302502-2451511074-3336417734

* **(172.31.40.89)**

53/tcp open domain

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3389/tcp open ms-wbt-server

5985/tcp open wsman

9389/tcp open adws

47001/tcp open winrm

49664/tcp open unknown

49665/tcp open unknown

49666/tcp open unknown

49667/tcp open unknown

49668/tcp open unknown

49672/tcp open unknown

49689/tcp open unknown

49690/tcp open unknown

49692/tcp open unknown

49695/tcp open unknown

49706/tcp open unknown

49718/tcp open unknown

49827/tcp open unknown

MAC Address: 02:2A:FF:CD:5B:13 (Unknown)

* **(172.31.40.162)**

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3389/tcp open ms-wbt-server

5985/tcp open wsman

9389/tcp open adws

47001/tcp open winrm

49664/tcp open unknown

49665/tcp open unknown

49666/tcp open unknown

49667/tcp open unknown

49669/tcp open unknown

49672/tcp open unknown

49675/tcp open unknown

49676/tcp open unknown

49680/tcp open unknown

49685/tcp open unknown

49696/tcp open unknown

49707/tcp open unknown

49719/tcp open unknown

62029/tcp open unknown

MAC Address: 02:A7:C8:0F:92:81 (Unknown)

* **(172.31.45.221)**

21/tcp open ftp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3389/tcp open ms-wbt-server

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

49678/tcp open unknown

49679/tcp open unknown

49680/tcp open unknown

MAC Address: 02:5C:DB:4E:3A:35 (Unknown)

**ESCANEO SNIPPER**

* **172.31.37.55 LINUX, WORDPRESS**

root@kali:~# nmap -O -A -sV -p- **172.31.37.55**

25/tcp open smtp OpenSMTPD

| smtp-commands: 11b55bf54bac Hello ip-172-31-37-55.eu-central-1.compute.internal [172.31.37.101], pleased to meet you, 8BITMIME, ENHANCEDSTATUSCODES, SIZE 36700160, DSN, HELP

|\_ 2.0.0 This is **OpenSMTPD 2.0.0** To report bugs in the implementation, please contact bugs@openbsd.org 2.0.0 with full details 2.0.0 End of HELP info

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

| http-robots.txt: 1 disallowed entry

|\_/wp-admin/

|\_http-generator: WordPress 6.5.2

|\_http-server-header: Apache/2.4.41 (Ubuntu)

|\_http-title: Vanguard Trust Bank

2222/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 a0:94:81:71:7a:df:43:1d:08:77:a3:5e:fe:f9:f3:a5 (RSA)

| 256 d4:ff:7a:12:a8:31:0d:87:39:6f:07:67:8b:d0:78:ce (ECDSA)

|\_ 256 e9:f9:37:4f:4d:9d:54:4b:15:4c:1b:9a:c6:ff:72:8c (ED25519)

3389/tcp open ms-wbt-server xrdp

8080/tcp open http-proxy

|\_http-title: Login Page

|\_http-open-proxy: Proxy might be redirecting requests

| Allow: GET,HEAD,OPTIONS

SF-Port8080-TCP:V=7.94%I=7%D=8/19%Time=66C35977%P=x86\_64**-pc-linux-gnu**%r(Ge

MAC Address: 02:25:84:BE:65:BB (Unknown)

Device type: general purpose

**Running: Linux 4.X|5.X**

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.8

Service Info: Host: 11b55bf54bac; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

root@kali:~# wpscan --url http://172.31.37.55 --enumerate u,p,t,m

[+] Headers

| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] robots.txt found: http://172.31.37.55/robots.txt

| Interesting Entries:

| - /wp-admin/

| - /wp-admin/admin-ajax.php

| Found By: Robots Txt (Aggressive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: http://172.31.37.55/xmlrpc.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC\_Pingback\_API

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_ghost\_scanner/

| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\_xmlrpc\_dos/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_xmlrpc\_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_pingback\_access/

[+] WordPress readme found: http://172.31.37.55/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://172.31.37.55/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5 identified (Latest, released on 2024-04-02).

| Found By: Unique Fingerprinting (Aggressive Detection)

| - http://172.31.37.55/readme.html md5sum is 015924092c38a9ffa6ba116c3aec0686

**[i] Theme(s) Identified:**

[+] twentytwentyfour

| Location: http://172.31.37.55/wp-content/themes/twentytwentyfour/

| Latest Version: 1.1 (up to date)

| Last Updated: 2024-04-02T00:00:00.000Z

| Readme: http://172.31.37.55/wp-content/themes/twentytwentyfour/readme.txt

| Style URL: http://172.31.37.55/wp-content/themes/twentytwentyfour/style.css

| Style Name: Twenty Twenty-Four

| Style URI: https://wordpress.org/themes/twentytwentyfour/

| Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...

| Author: the WordPress team

| Author URI: https://wordpress.org

|

| Found By: Known Locations (Aggressive Detection)

| - http://172.31.37.55/wp-content/themes/twentytwentyfour/, status: 403

|

| Version: 1.1 (80% confidence)

| Found By: Style (Passive Detection)

| - http://172.31.37.55/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'

[+] twentytwentythree

| Location: http://172.31.37.55/wp-content/themes/twentytwentythree/

| Latest Version: 1.4 (up to date)

| Last Updated: 2024-04-02T00:00:00.000Z

| Readme: http://172.31.37.55/wp-content/themes/twentytwentythree/readme.txt

| Style URL: http://172.31.37.55/wp-content/themes/twentytwentythree/style.css

| Style Name: Twenty Twenty-Three

| Style URI: https://wordpress.org/themes/twentytwentythree

| Description: Twenty Twenty-Three is designed to take advantage of the new design tools introduced in WordPress 6....

| Author: the WordPress team

| Author URI: https://wordpress.org

|

| Found By: Known Locations (Aggressive Detection)

| - http://172.31.37.55/wp-content/themes/twentytwentythree/, status: 403

|

| Version: 1.4 (80% confidence)

| Found By: Style (Passive Detection)

| - http://172.31.37.55/wp-content/themes/twentytwentythree/style.css, Match: 'Version: 1.4'

[+] twentytwentytwo

| Location: http://172.31.37.55/wp-content/themes/twentytwentytwo/

| Latest Version: 1.7 (up to date)

| Last Updated: 2024-04-02T00:00:00.000Z

| Readme: http://172.31.37.55/wp-content/themes/twentytwentytwo/readme.txt

| Style URL: http://172.31.37.55/wp-content/themes/twentytwentytwo/style.css

| Style Name: Twenty Twenty-Two

| Style URI: https://wordpress.org/themes/twentytwentytwo/

| Description: Built on a solidly designed foundation, Twenty Twenty-Two embraces the idea that everyone deserves a...

| Author: the WordPress team

| Author URI: https://wordpress.org/

|

| Found By: Known Locations (Aggressive Detection)

| - http://172.31.37.55/wp-content/themes/twentytwentytwo/, status: 200

|

| Version: 1.7 (80% confidence)

| Found By: Style (Passive Detection)

| - http://172.31.37.55/wp-content/themes/twentytwentytwo/style.css, Match: 'Version: 1.7'

**[i] User(s) Identified:**

[+] admin

| Found By: Wp Json Api (Aggressive Detection)

| - http://172.31.37.55/wp-json/wp/v2/users/?per\_page=100&page=1

| Confirmed By:

| Rss Generator (Aggressive Detection)

| Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Login Error Messages (Aggressive Detection)

[+] webmin

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] FlagHunter

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] charlie-WS01

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

* **172.31.37.83 WINDOWS SERVER 2019 WS01.hq.vanguard.bank**

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

3389/tcp open ms-wbt-server Microsoft Terminal Services

| ssl-cert: Subject: commonName=WS01.hq.vanguard.bank

| Not valid before: 2024-04-06T14:28:53

|\_Not valid after: 2024-10-06T14:28:53

| rdp-ntlm-info:

| Target\_Name: HQ

| NetBIOS\_Domain\_Name: HQ

| NetBIOS\_Computer\_Name: WS01

| DNS\_Domain\_Name: hq.vanguard.bank

| DNS\_Computer\_Name: WS01.hq.vanguard.bank

| Product\_Version: 10.0.17763

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

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

49670/tcp open msrpc Microsoft Windows RPC

49679/tcp open msrpc Microsoft Windows RPC

49680/tcp open msrpc Microsoft Windows RPC

MAC Address: 02:8F:03:CA:D8:FF (Unknown)

**OS details: Microsoft Windows Server 2019**

Host script results:

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled but not required

|\_nbstat: NetBIOS name: WS01, NetBIOS user: <unknown>, NetBIOS MAC: 02:8f:03:ca:d8:ff

Looking up status of 172.31.37.83

WS01 <00> - B <ACTIVE> Workstation Service

HQ <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

WS01 <20> - B <ACTIVE> File Server Service

MAC Address = 02-8F-03-CA-D8-FF

* **172.31.40.89 WINDOWS SERVER 2019 DC01.vanguard.bank**

53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-08-19 14:58:07Z)

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: vanguard.bank0., Site: Default-First-Site-Name)

|\_ssl-date: 2024-08-19T14:59:10+00:00; 0s from scanner time.

| ssl-cert: Subject: commonName=**DC01.vanguard.bank**

| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.vanguard.bank

| Not valid before: 2024-04-07T16:53:28

|\_Not valid after: 2025-04-07T16:53:28

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: vanguard.bank0., Site: Default-First-Site-Name)

|\_ssl-date: 2024-08-19T14:59:10+00:00; 0s from scanner time.

| ssl-cert: Subject: commonName=DC01.vanguard.bank

| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.vanguard.bank

| Not valid before: 2024-04-07T16:53:28

|\_Not valid after: 2025-04-07T16:53:28

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: vanguard.bank0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC01.vanguard.bank

| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.vanguard.bank

| Not valid before: 2024-04-07T16:53:28

|\_Not valid after: 2025-04-07T16:53:28

|\_ssl-date: 2024-08-19T14:59:10+00:00; 0s from scanner time.

3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: vanguard.bank0., Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=DC01.vanguard.bank

| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:DC01.vanguard.bank

| Not valid before: 2024-04-07T16:53:28

|\_Not valid after: 2025-04-07T16:53:28

|\_ssl-date: 2024-08-19T14:59:10+00:00; 0s from scanner time.

3389/tcp open ms-wbt-server Microsoft Terminal Services

| ssl-cert: Subject: commonName=DC01.vanguard.bank

| Not valid before: 2024-04-06T00:14:36

|\_Not valid after: 2024-10-06T00:14:36

|\_ssl-date: 2024-08-19T14:59:10+00:00; 0s from scanner time.

| rdp-ntlm-info:

| Target\_Name: VANGUARD

| NetBIOS\_Domain\_Name: VANGUARD

| NetBIOS\_Computer\_Name: DC01

| **DNS\_Domain\_Name: vanguard.bank**

**| DNS\_Computer\_Name: DC01.vanguard.bank**

| Product\_Version: 10.0.17763

|\_ System\_Time: 2024-08-19T14:59:03+00:00

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

9389/tcp open mc-nmf .NET Message Framing

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

49672/tcp open msrpc Microsoft Windows RPC

49689/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

49690/tcp open msrpc Microsoft Windows RPC

49692/tcp open msrpc Microsoft Windows RPC

49695/tcp open msrpc Microsoft Windows RPC

49706/tcp open msrpc Microsoft Windows RPC

49718/tcp open msrpc Microsoft Windows RPC

49827/tcp open msrpc Microsoft Windows RPC

MAC Address: 02:2A:FF:CD:5B:13 (Unknown)

**Running: Microsoft Windows 2019**

OS details: Microsoft Windows Server 2019

Host script results:

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled and required

|\_nbstat: NetBIOS name: DC01, NetBIOS user: <unknown>, NetBIOS MAC: 02:2a:ff:cd:5b:13 (unknown)

| smb2-time:

| date: 2024-08-19T14:59:03

|\_ start\_date: N/A

Looking up status of 172.31.40.89

DC01 <00> - B <ACTIVE> Workstation Service

VANGUARD <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

VANGUARD <1c> - <GROUP> B <ACTIVE> Domain Controllers

DC01 <20> - B <ACTIVE> File Server Service

VANGUARD <1b> - B <ACTIVE> Domain Master Browser

MAC Address = 02-2A-FF-CD-5B-13

===================================( Session Check on 172.31.40.89 )===================================

[+] Server 172.31.40.89 allows sessions using username '', password ''

* **172.31.40.162 WINDOWS SERVER 2019 DC02.hq.vanguard.bank 172.31.40.162**

53/tcp open domain Simple DNS Plus

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-title: IIS Windows Server

|\_http-server-header: Microsoft-IIS/10.0

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-08-19 14:58:21Z)

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: vanguard.bank0., Site: Default-First-Site-Name)

| ssl-cert: Subject:

| Subject Alternative Name: othername: UPN::DC02$@hq.vanguard.bank, DNS:DC02.hq.vanguard.bank, DNS:hq.vanguard.bank, DNS:HQ

| Not valid before: 2024-04-07T03:08:13

|\_Not valid after: 2026-04-07T03:18:13

|\_ssl-date: 2024-08-19T14:59:25+00:00; 0s from scanner time.

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0 **NO RESUELVE**

636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: vanguard.bank0., Site: Default-First-Site-Name)

| ssl-cert: Subject:

| Subject Alternative Name: othername: UPN::DC02$@hq.vanguard.bank, DNS:DC02.hq.vanguard.bank, DNS:hq.vanguard.bank, DNS:HQ

| Not valid before: 2024-04-07T03:08:13

|\_Not valid after: 2026-04-07T03:18:13

|\_ssl-date: 2024-08-19T14:59:25+00:00; 0s from scanner time.

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: vanguard.bank0., Site: Default-First-Site-Name)

|\_ssl-date: 2024-08-19T14:59:25+00:00; 0s from scanner time.

| ssl-cert: Subject:

| Subject Alternative Name: othername: UPN::DC02$@hq.vanguard.bank, DNS:DC02.hq.vanguard.bank, DNS:hq.vanguard.bank, DNS:HQ

| Not valid before: 2024-04-07T03:08:13

|\_Not valid after: 2026-04-07T03:18:13

3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: vanguard.bank0., Site: Default-First-Site-Name)

| ssl-cert: Subject:

| Subject Alternative Name: othername: UPN::DC02$@hq.vanguard.bank, DNS:DC02.hq.vanguard.bank, DNS:hq.vanguard.bank, DNS:HQ

| Not valid before: 2024-04-07T03:08:13

|\_Not valid after: 2026-04-07T03:18:13

|\_ssl-date: 2024-08-19T14:59:25+00:00; 0s from scanner time.

3389/tcp open ms-wbt-server Microsoft Terminal Services

| ssl-cert: Subject: commonName=DC02.hq.vanguard.bank

| Not valid before: 2024-04-06T01:20:09

|\_Not valid after: 2024-10-06T01:20:09

| rdp-ntlm-info:

| Target\_Name: HQ

| NetBIOS\_Domain\_Name: HQ

| NetBIOS\_Computer\_Name: DC02

| DNS\_Domain\_Name: hq.vanguard.bank

| DNS\_Computer\_Name: DC02.hq.vanguard.bank

| DNS\_Tree\_Name: vanguard.bank

| Product\_Version: 10.0.17763

|\_ System\_Time: 2024-08-19T14:59:16+00:00

|\_ssl-date: 2024-08-19T14:59:25+00:00; 0s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-title: Not Found

|\_http-server-header: Microsoft-HTTPAPI/2.0

9389/tcp open mc-nmf .NET Message Framing

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-title: Not Found

|\_http-server-header: Microsoft-HTTPAPI/2.0

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

49669/tcp open msrpc Microsoft Windows RPC

49672/tcp open msrpc Microsoft Windows RPC

49675/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

49676/tcp open msrpc Microsoft Windows RPC

49680/tcp open msrpc Microsoft Windows RPC

49685/tcp open msrpc Microsoft Windows RPC

49696/tcp open msrpc Microsoft Windows RPC

49707/tcp open msrpc Microsoft Windows RPC

49719/tcp open msrpc Microsoft Windows RPC

62029/tcp open msrpc Microsoft Windows RPC

MAC Address: 02:A7:C8:0F:92:81 (Unknown)

**Running: Microsoft Windows 2019**

**OS details: Microsoft Windows Server 2019**

**root@kali:~/Desktop/windows-resources/powershell-empire# smbmap -u richard -p 'Winter123!' -H 172.31.40.162**

**[+] IP: 172.31.40.162:445 Name: ip-172-31-40-162.eu-central-1.compute.internal**

**Disk Permissions Comment**

**---- ----------- -------**

**ADMIN$ NO ACCESS Remote Admin**

**C$ NO ACCESS Default share**

**CertEnroll READ ONLY Active Directory Certificate Services share**

**IPC$ READ ONLY Remote IPC**

**NETLOGON READ ONLY Logon server share**

**SYSVOL READ ONLY Logon server share**

Host script results:

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled and required

|\_nbstat: NetBIOS name: DC02, NetBIOS user: <unknown>, NetBIOS MAC: 02:a7:c8:0f:92:81 (unknown)

| smb2-time:

| date: 2024-08-19T14:59:17

|\_ start\_date: N/A

* **172.31.45.221 WINDOWS SERVER 2019 FILESRV01.hq.vanguard.bank**

21/tcp open ftp Microsoft ftpd

| ftp-syst:

|\_ SYST: Windows\_NT

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/10.0

|\_http-title: IIS Windows Server

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target\_Name: HQ

| NetBIOS\_Domain\_Name: HQ

| NetBIOS\_Computer\_Name: FILESRV01

| DNS\_Domain\_Name: hq.vanguard.bank

| DNS\_Computer\_Name: **FILESRV01.hq.vanguard.bank**

| DNS\_Tree\_Name: vanguard.bank

| Product\_Version: 10.0.17763

|\_ System\_Time: 2024-08-19T15:10:25+00:00

| ssl-cert: Subject: commonName=FILESRV01.hq.vanguard.bank

| Not valid before: 2024-04-06T04:00:04

|\_Not valid after: 2024-10-06T04:00:04

|\_ssl-date: 2024-08-19T15:10:29+00:00; 0s from scanner time.

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-title: Not Found

|\_http-server-header: Microsoft-HTTPAPI/2.0

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

49678/tcp open msrpc Microsoft Windows RPC

49679/tcp open msrpc Microsoft Windows RPC

49680/tcp open msrpc Microsoft Windows RPC

MAC Address: 02:5C:DB:4E:3A:35 (Unknown)

**OS details: Microsoft Windows Server 2019**

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_nbstat: NetBIOS name: FILESRV01, NetBIOS user: <unknown>, NetBIOS MAC: 02:5c:db:4e:3a:35 (unknown)

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled but not required