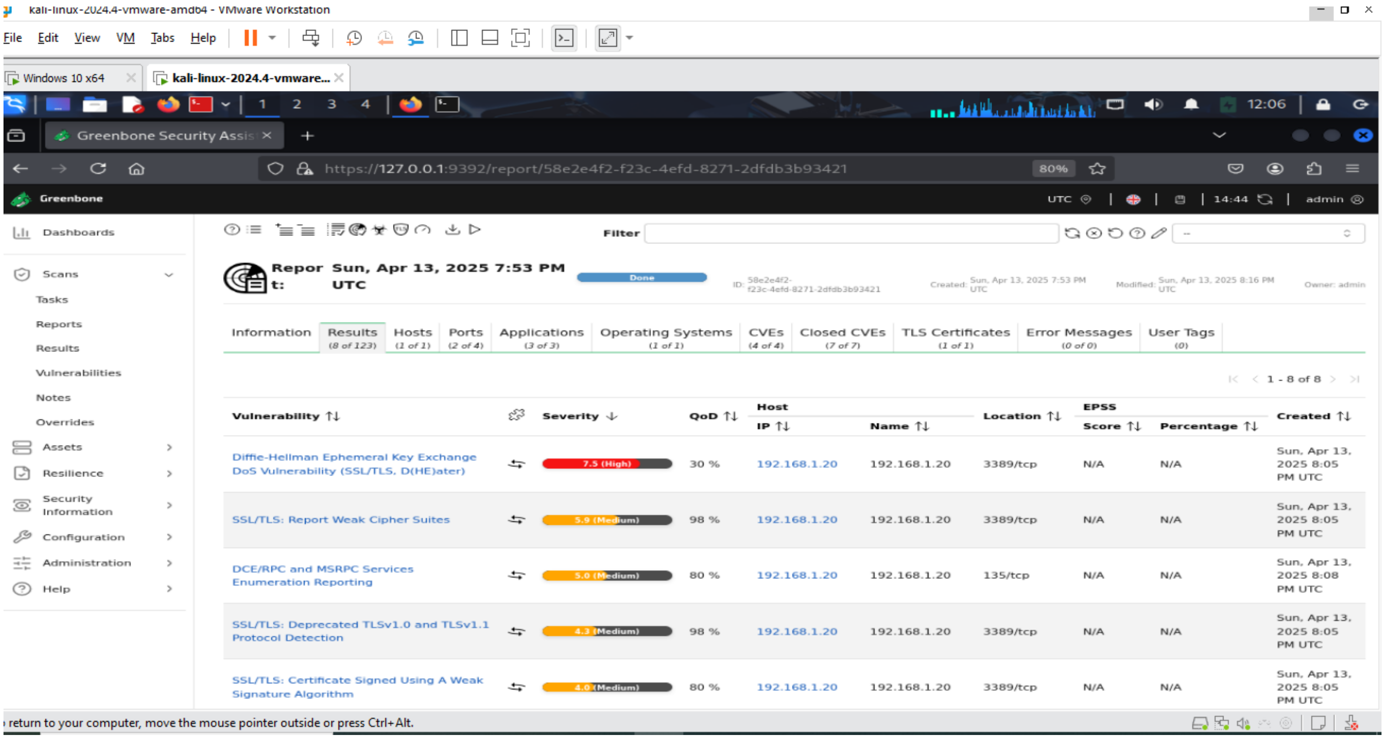
Scan Windows 10 machine (192.168.1.20) with OpenVAS

After Scan these vulnerabilities appeared:

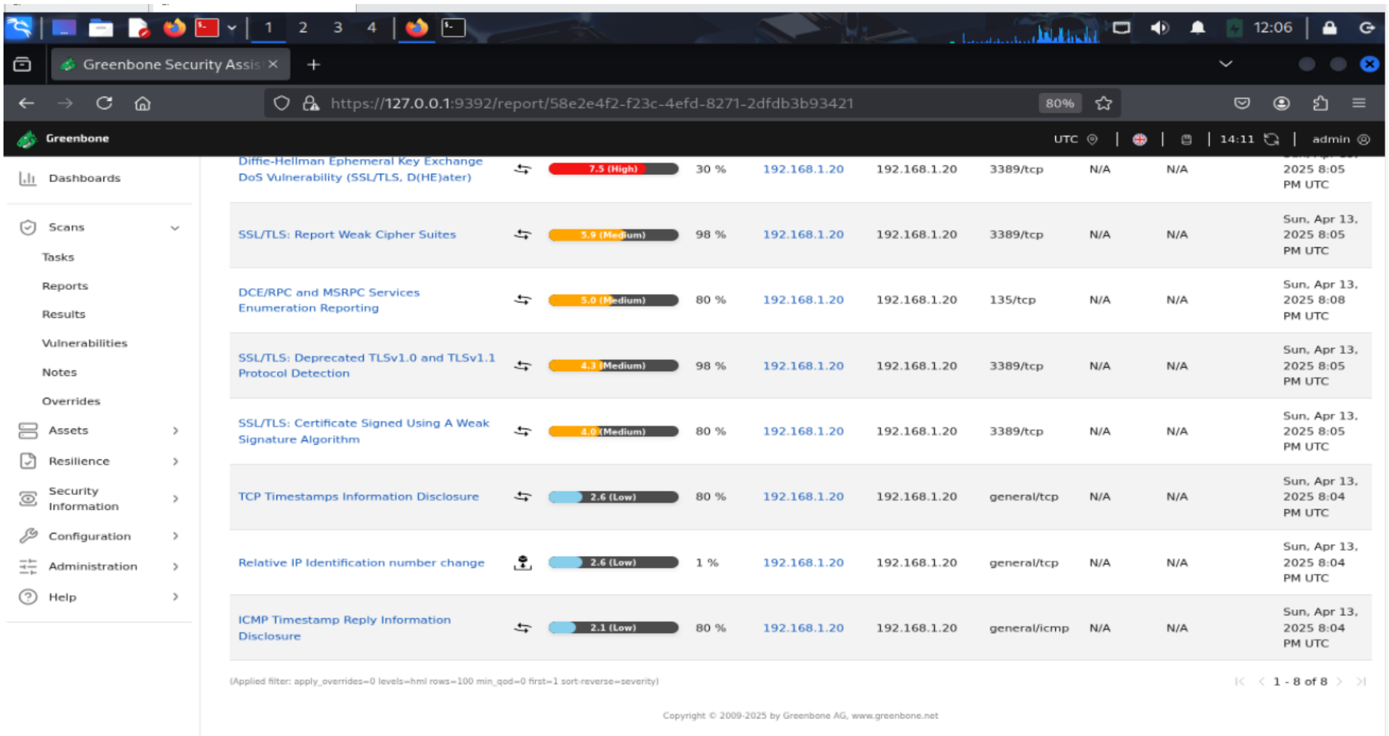


Report: Sun, Apr 13, 2025 7:53 PM UTC

ID: 58e2e4f2-f23c-4efd-8271-2dfdb3b93421 Created: Sun, Apr 13, 2025 7:53 PM UTC Modified: Sun, Apr 13, 2025 8:16 PM UTC Owner: admin

Vulnerability		Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage	Created
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	⇆	7.5 (High)	30 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	5.9 (Medium)	98 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	192.168.1.20	192.168.1.20	135/tcp	N/A	N/A	Sun, Apr 13, 2025 8:08 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	⇆	4.0 (Medium)	80 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC

return to your computer, move the mouse pointer outside or press Ctrl+Alt.



Vulnerability		Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage	Created
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	⇆	7.5 (High)	30 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	2025 8:05 PM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	5.9 (Medium)	98 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	192.168.1.20	192.168.1.20	135/tcp	N/A	N/A	Sun, Apr 13, 2025 8:08 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	⇆	4.0 (Medium)	80 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC
TCP Timestamps Information Disclosure	⇆	2.6 (Low)	80 %	192.168.1.20	192.168.1.20	general/tcp	N/A	N/A	Sun, Apr 13, 2025 8:04 PM UTC
Relative IP Identification number change		2.6 (Low)	1 %	192.168.1.20	192.168.1.20	general/tcp	N/A	N/A	Sun, Apr 13, 2025 8:04 PM UTC
ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)	80 %	192.168.1.20	192.168.1.20	general/icmp	N/A	N/A	Sun, Apr 13, 2025 8:04 PM UTC

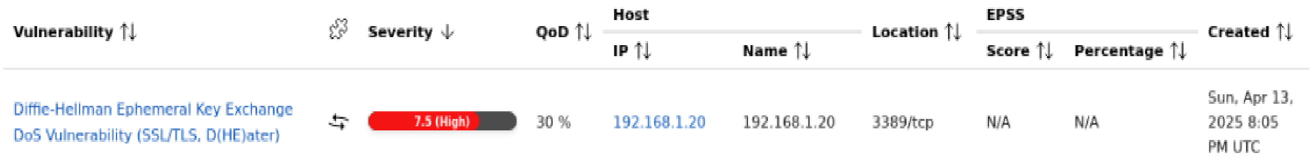
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=0 first=1 sort-reverse=severity)

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

1.Diffie-Hellman Ephemeral key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

Summary:

The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.



Vulnerability		Severity	QoD	Host		Location	EPSS		Created
				IP	Name		Score	Percentage	
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	⇆	7.5 (High)	30 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC

Impact:

This vulnerability allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)ater attack.

There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.

Solution>> Mitigation:

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.

- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

References:

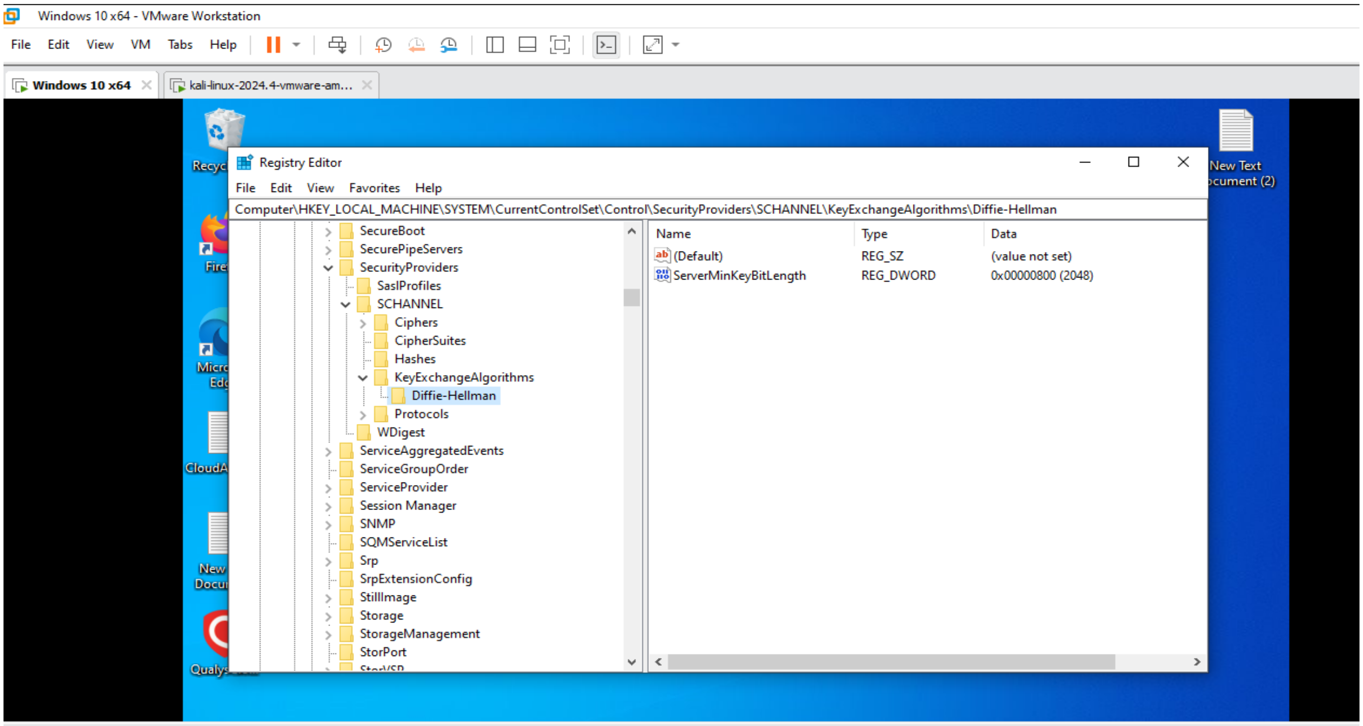
CVE-2022-40735 / CVE-2024-41996 / CVE-2002-20001

Fix vulnerability:

- Open Registry Editor.
- Access the following registry location:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]

- Update the following DWORD value to: "ServerMinKeyBitLength"=dword:00000800



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman

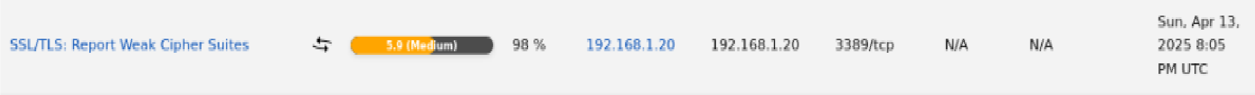
Name	Type	Data
(Default)	REG_SZ	(value not set)
ServerMinKeyBitLength	REG_DWORD	0x00000800 (2048)

We continue to encourage customers to follow our Protect Your Computer guidance of enabling a firewall, getting software updates and installing antivirus software

2.SSL/TLS: Report Weak Cipher Suites

Summary:

This routine reports all weak SSL/TLS cipher suites accepted by a service



SSL/TLS: Report Weak Cipher Suites	5.9 (Medium)	98 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC

Impact:

This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

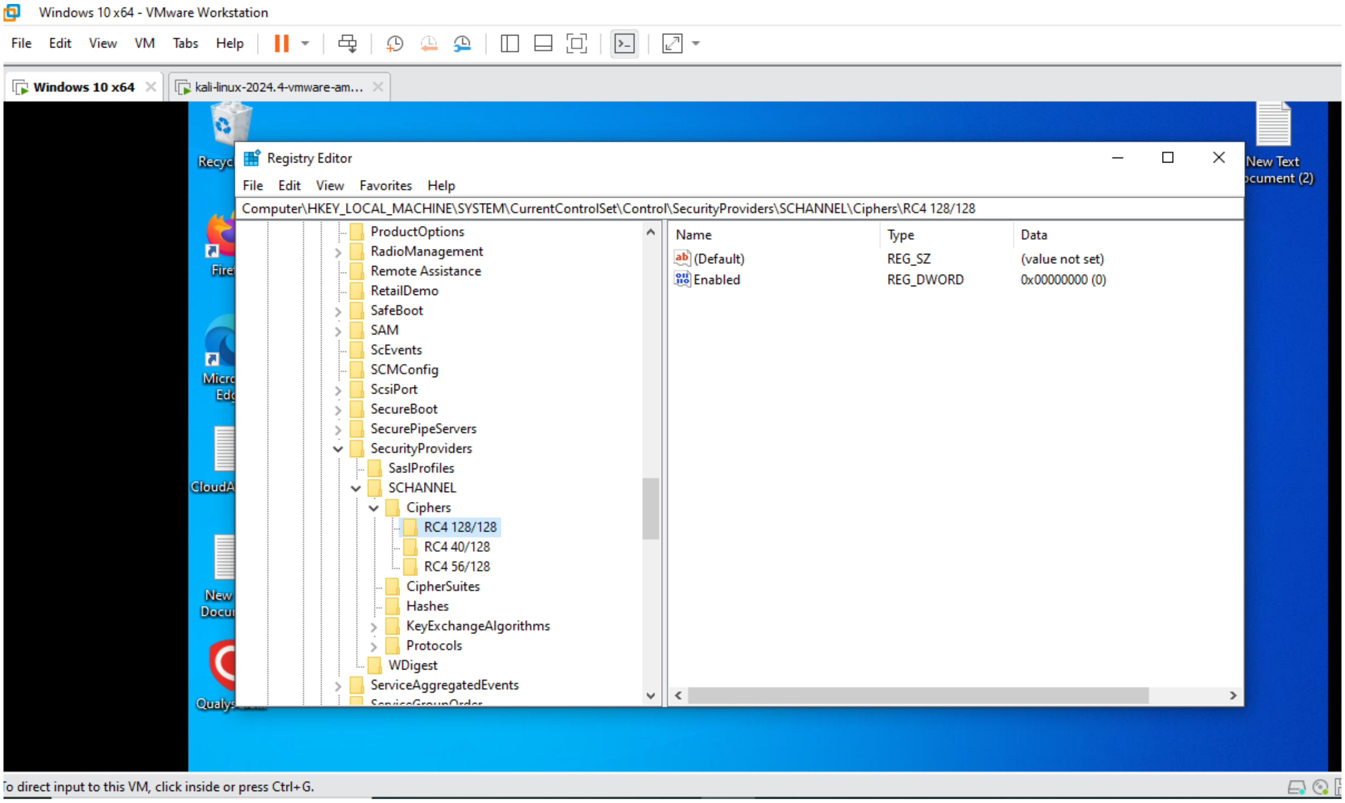
References:

CVE-2013-2566 / CVE-2015-2808 / CVE-2015-4000

Fix vulnerability:

We can use the following registry keys and their values to disable RC4

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]
  "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]
  "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]
  "Enabled"=dword:00000000

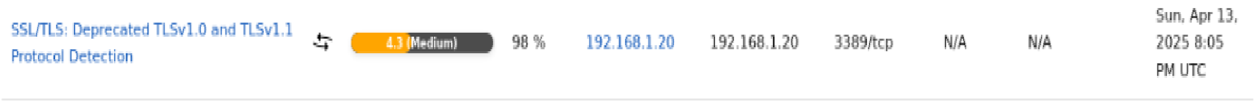


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128

Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

3.SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection vulnerability

Summary: It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system. It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.



SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	192.168.1.20	192.168.1.20	3389/tcp	N/A	N/A	Sun, Apr 13, 2025 8:05 PM UTC

Impact:

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore, newly uncovered vulnerabilities in these protocols won't receive security updates anymore.

Solution: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

References:

CVE-2011-3389 / CVE-2015-0204

Fix vulnerability:

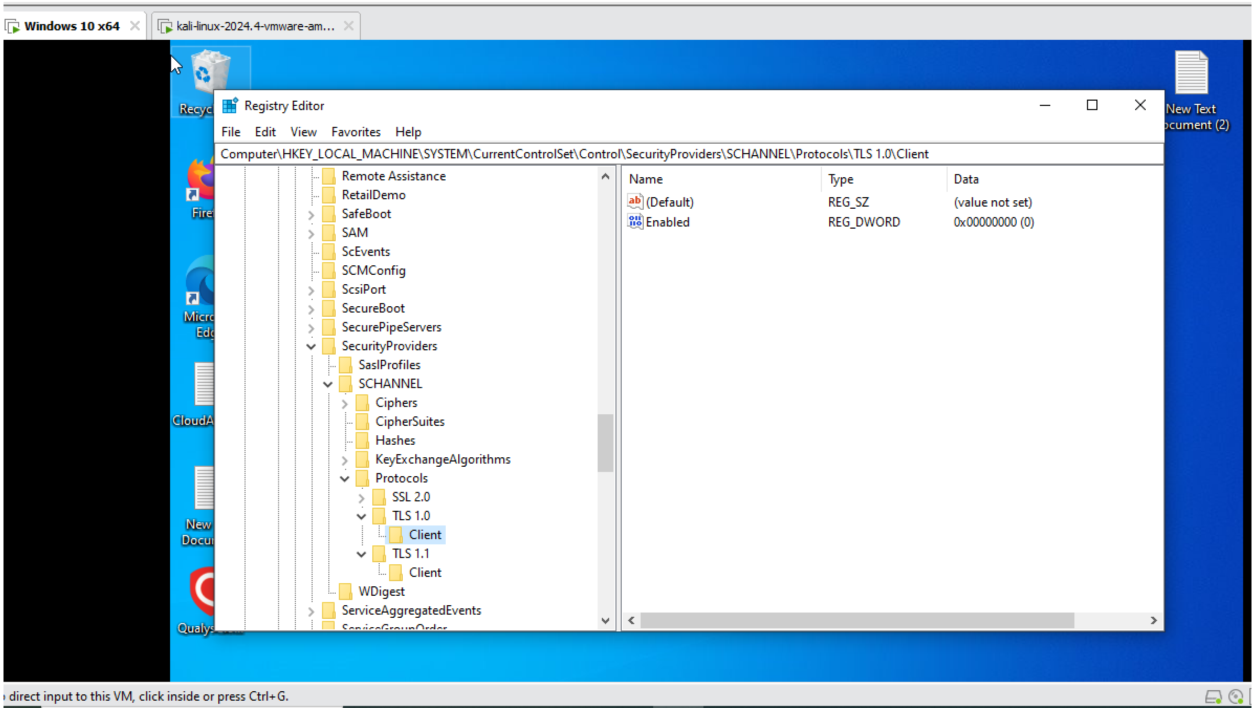
We can use the following registry keys and their values to disable TLS 1.0 and TLS 1.1

>>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.0\Client

Enabled = 0

>>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.0\Client

Enabled = 0



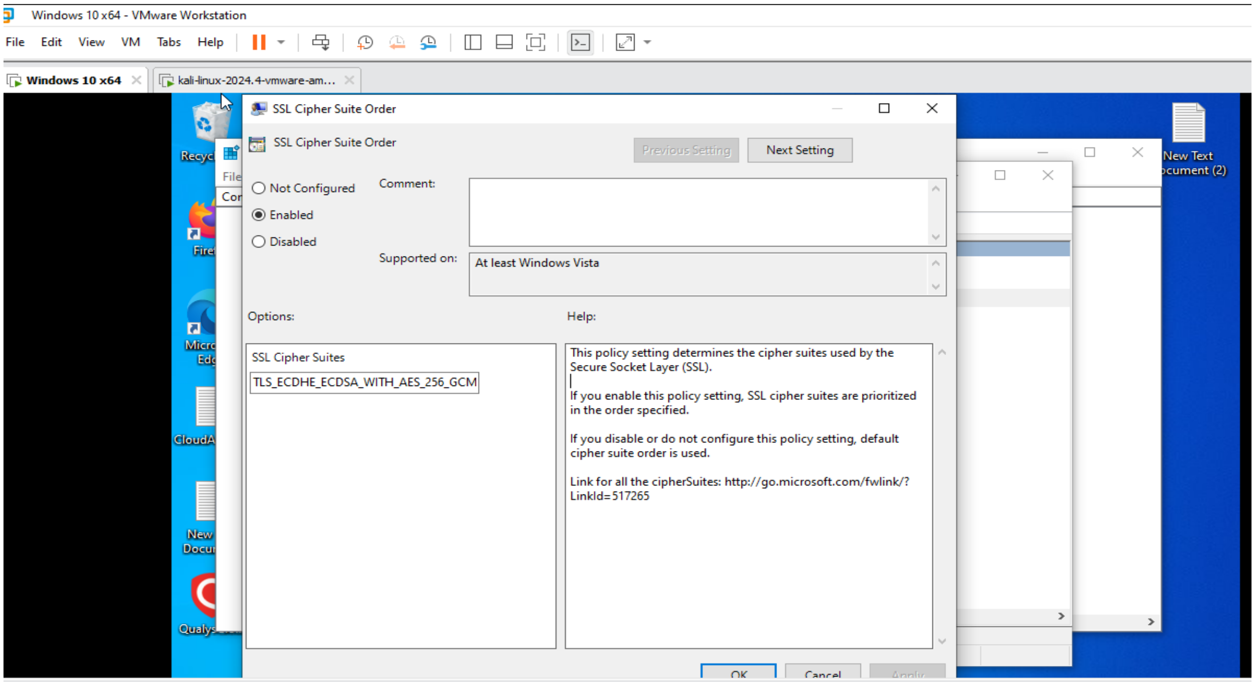
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client

Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000000 (0)

Configuring TLS Cipher Suite Order by using Group Policy

You can use the SSL Cipher Suite Order Group Policy settings to configure the default TLS cipher suite order.

1. From the Group Policy Management Console, go to Computer Configuration > Administrative Templates > Network > SSL Configuration Settings.
2. Double-click SSL Cipher Suite Order, and then click the Enabled option.
3. Right-click SSL Cipher Suites box and select Select all from the pop-up menu.
4. Right-click the selected text, and select copy from the pop-up menu.
5. Paste the text into a text editor such as notepad.exe and update with the new cipher suite order list.
6. Replace the list in the **SSL Cipher Suites** with the updated ordered list.
7. Click **OK** or **Apply**.



SSL Cipher Suite Order

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

SSL Cipher Suites
TLS_ECDHE_ECDSA_WITH_AES_256_GCM

This policy setting determines the cipher suites used by the Secure Socket Layer (SSL).

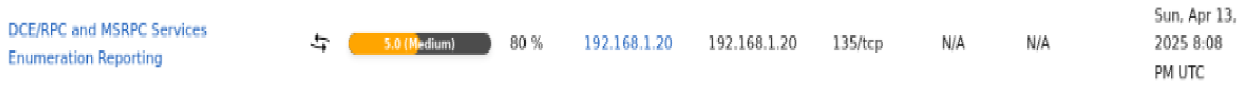
If you enable this policy setting, SSL cipher suites are prioritized in the order specified.

If you disable or do not configure this policy setting, default cipher suite order is used.

Link for all the cipherSuites: http://go.microsoft.com/fwlink/?LinkId=517265

4.DCE/RPC and MSRPC Services Enumeration Reporting

Summary: Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.



DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.1.20	192.168.1.20	135/tcp	N/A	N/A	Sun, Apr 13, 2025 8:08 PM UTC

Impact:

An attacker may use this fact to gain more knowledge about the remote host.

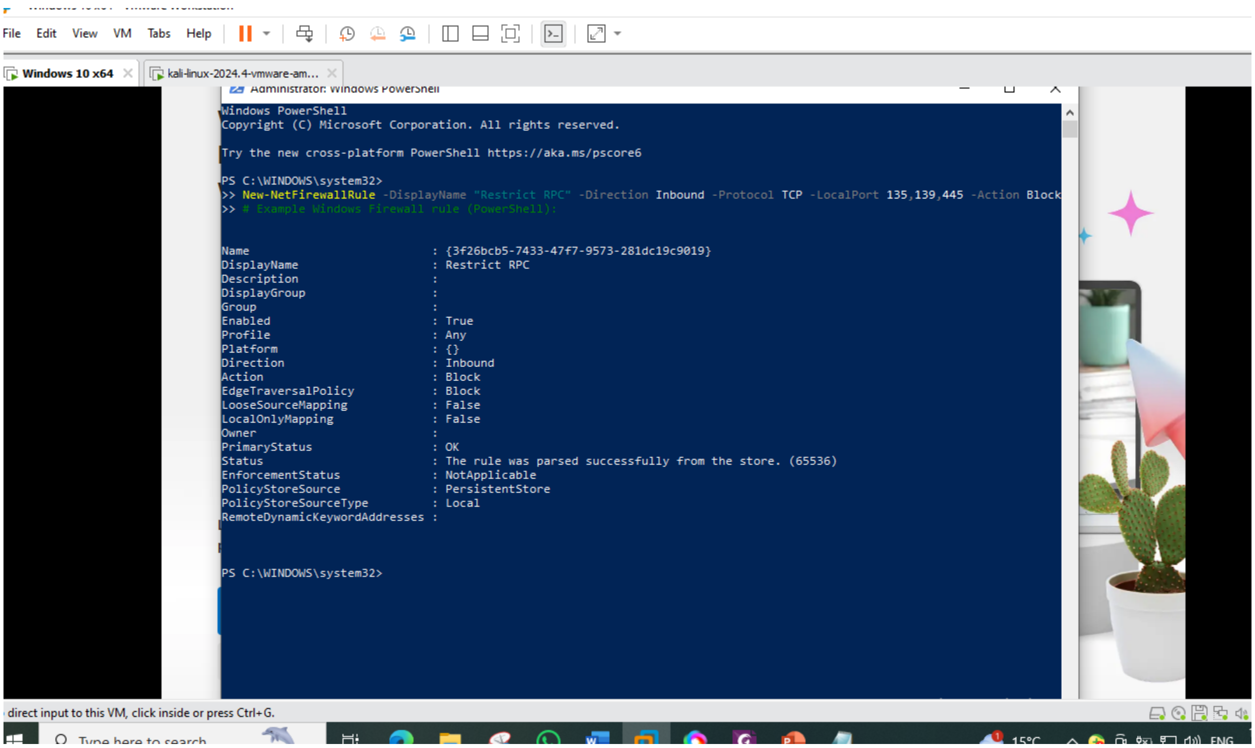
Solution: Filter incoming traffic to these ports.

Fix vulnerability:

1. Restrict Access via Firewall or ACLs

- **Block ports** that are used by DCE/RPC (e.g., **135/tcp**, **139/tcp**, **445/tcp**, and dynamic range **49152–65535/tcp** for RPC).
- Use Windows Firewall to limit access **only to trusted IPs**.
- Example Windows Firewall rule (PowerShell):

New-NetFirewallRule -DisplayName "Restrict RPC" -Direction Inbound -Protocol TCP -LocalPort 135,139,445 -Action Block



File
Edit
View
VM
Tabs
Help
Windows 10 x64
kali-linux-2024.4-vmware-am...
Administrator: Windows PowerShell
direct input to this VM, click inside or press Ctrl+G.
Type here to search
15°C
ENG

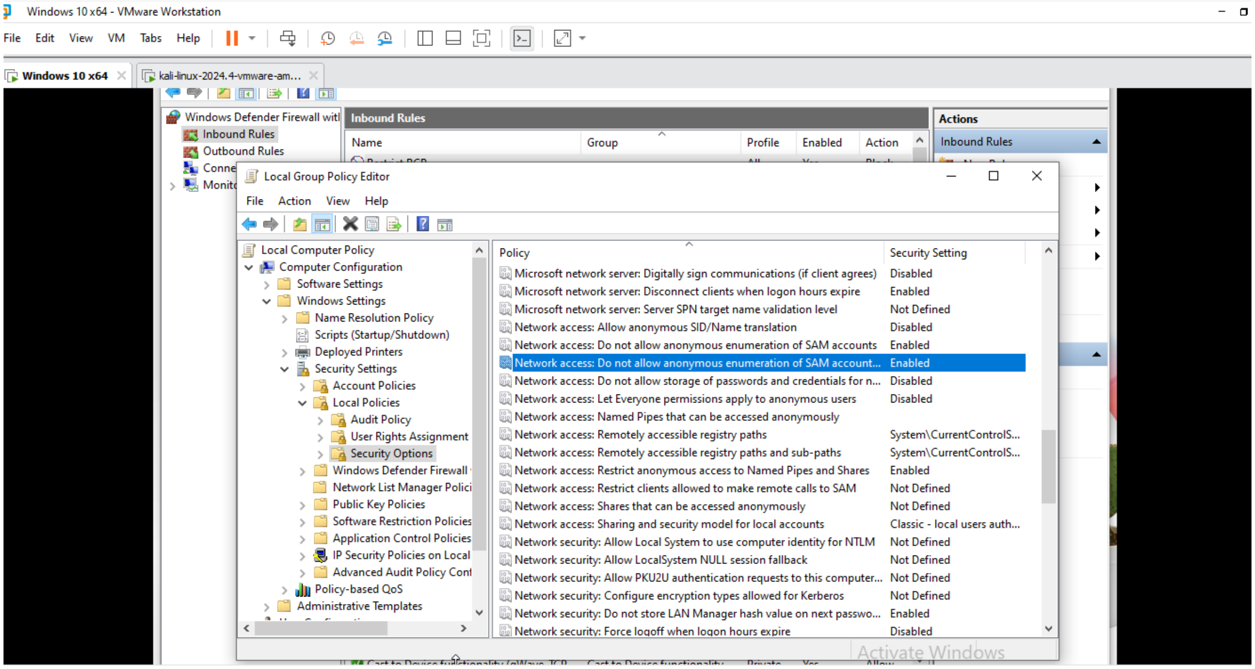
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32>
>> New-NetFirewallRule -DisplayName "Restrict RPC" -Direction Inbound -Protocol TCP -LocalPort 135,139,445 -Action Block
>> # Example Windows Firewall rule (PowerShell):


Name                          : {3f26bcb5-7433-47f7-9573-281dc19c9019}
DisplayName                   : Restrict RPC
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses :


PS C:\WINDOWS\system32>
```

2. Enforce RPC Security and Hardening

Group Policy Path: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

Set the following:

- Network access: Let Everyone permissions apply to anonymous users → **Disabled**
- Network access: Restrict anonymous access to Named Pipes and Shares → **Enabled**
- Network access: Do not allow anonymous enumeration of SAM accounts → **Enabled**
- Network access: Do not allow anonymous enumeration of SAM accounts and shares → **Enabled**

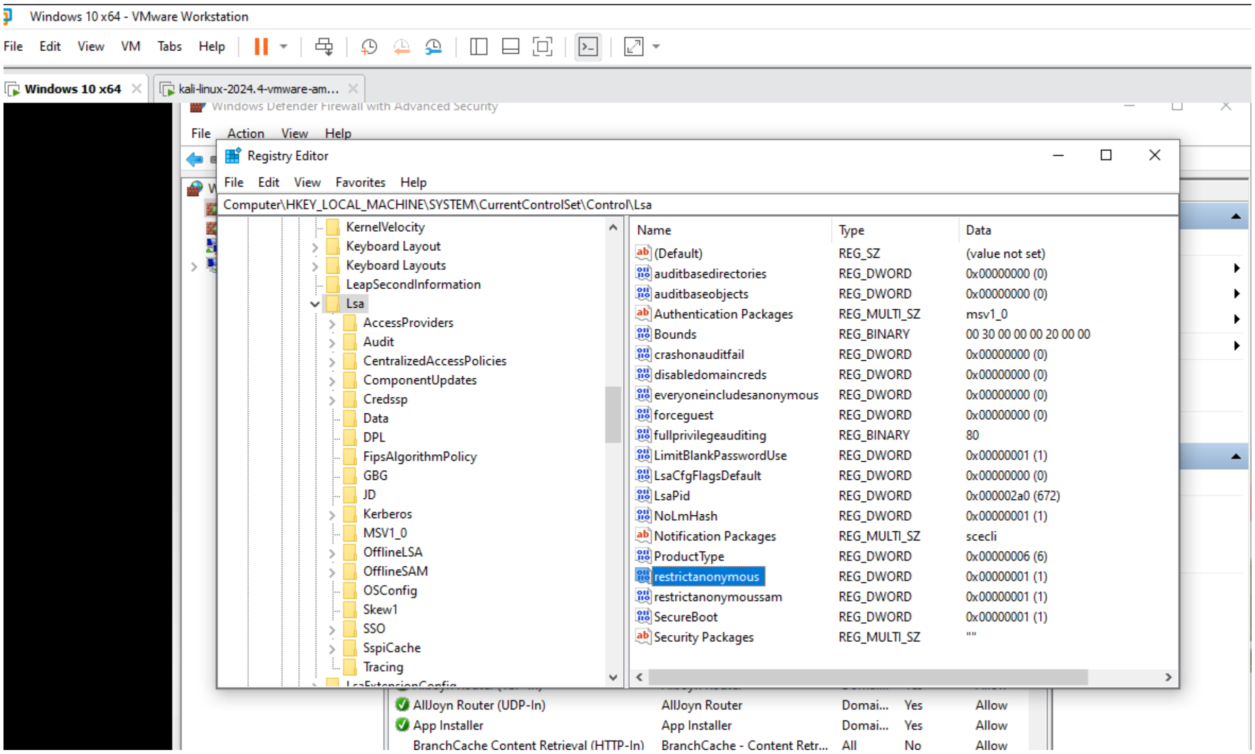


Policy	Security Setting
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM account...	Enabled
Network access: Do not allow storage of passwords and credentials for n...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	
Network access: Remotely accessible registry paths	System\CurrentControlS...
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer...	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next passwo...	Enabled
Network security: Force logoff when logon hours expire	Disabled

3. Modify the registry to restrict remote access:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

"RestrictAnonymous"=dword:00000001

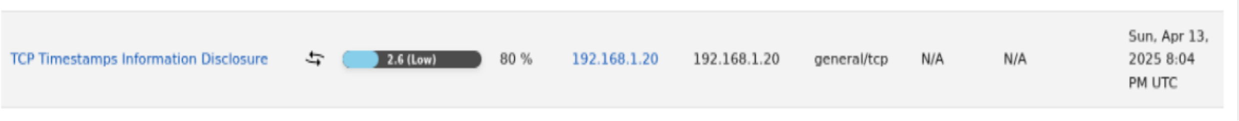

Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
kali-linux-2024.4-vmware-am...
Windows Defender Firewall with Advanced Security
File Action View Help
Registry Editor
File Edit View Favorites Help
KernelVelocity
Keyboard Layout
Keyboard Layouts
LeapSecondInformation
Lsa
AccessProviders
Audit
CentralizedAccessPolicies
ComponentUpdates
Credssp
Data
DPL
FipsAlgorithmPolicy
GBG
JD
Kerberos
MSV1_0
OfflineLSA
OfflineSAM
OSConfig
Skew1
SSO
SspiCache
Tracing
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes Allow
App Installer App Installer Domai... Yes Allow
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No Allow

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbasedirectories	REG_DWORD	0x00000000 (0)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	80
LimitBlankPasswordUse	REG_DWORD	0x00000001 (1)
LsaCfgFlagsDefault	REG_DWORD	0x00000000 (0)
LsaPid	REG_DWORD	0x000002a0 (672)
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Packages	REG_MULTI_SZ	scecli
ProductType	REG_DWORD	0x00000006 (6)
restrictanonymous	REG_DWORD	0x00000001 (1)
restrictanonymoussam	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	""

5.TCP Timestamps Information Disclosure

Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.



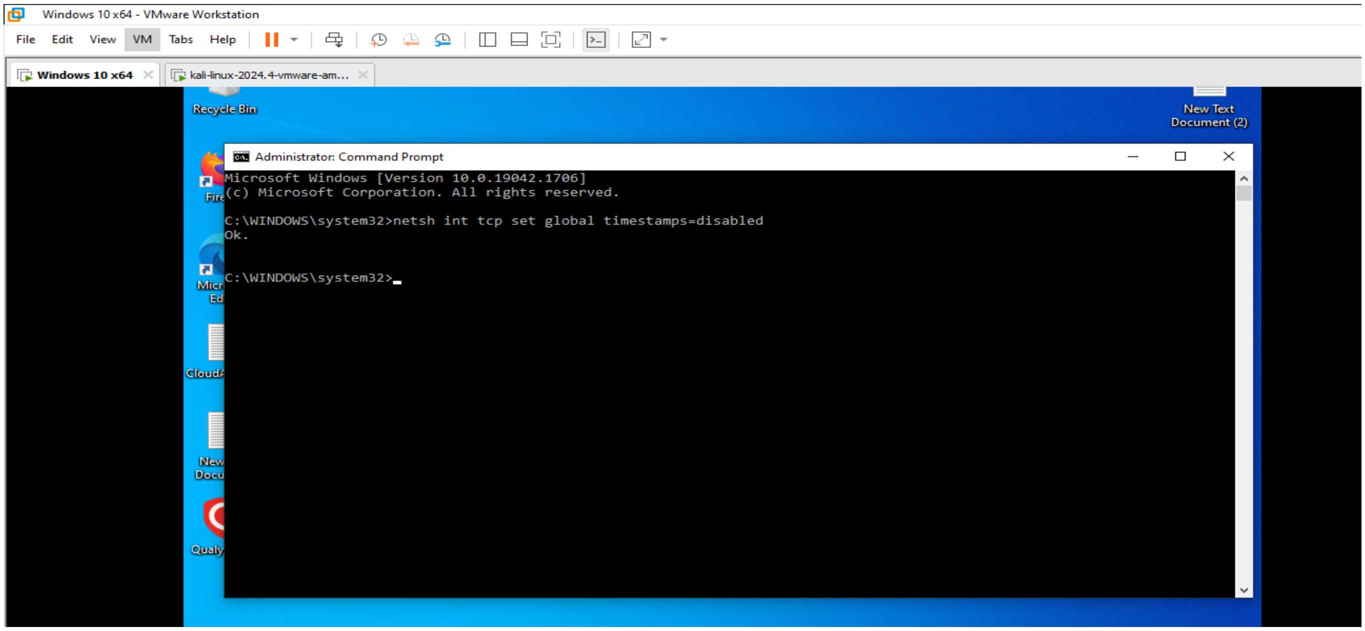
TCP Timestamps Information Disclosure	⇆	2.6 (Low)	80 %	192.168.1.20	192.168.1.20	general/tcp	N/A	N/A	Sun, Apr 13, 2025 8:04 PM UTC

Impact:

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Fix vulnerability:

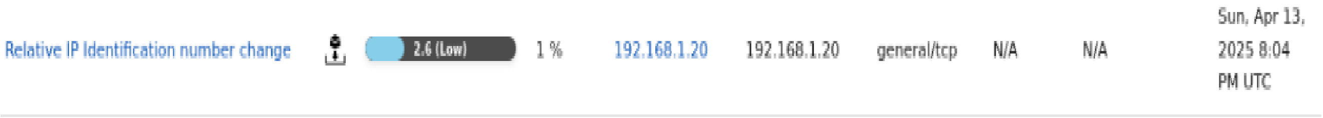
To disable TCP timestamps on Windows, execute 'netsh int tcp set global timestamps=disabled’


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 x64
kali-linux-2024.4-vmware-am...
Recycle Bin
New Text Document (2)
Administrator: Command Prompt
Fire
Micr Ed
CloudA
New Docu
Qualy

```
Microsoft Windows [Version 10.0.19042.1706]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh int tcp set global timestamps=disabled
Ok.


C:\WINDOWS\system32>_
```

6.Relative IP Identification number change vulnerability

Summary: The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.



Relative IP Identification number change		2.6 (Low)	1 %	192.168.1.20	192.168.1.20	general/tcp	N/A	N/A	Sun, Apr 13, 2025 8:04 PM UTC

Impact:

An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind port scan of another network.

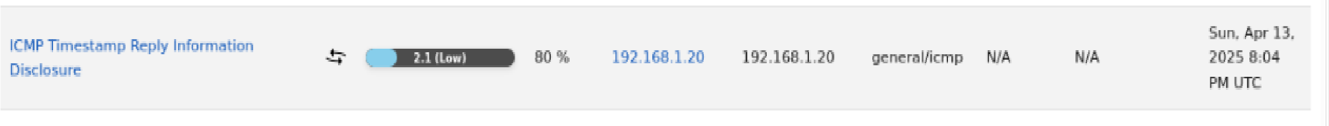
2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.

3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

Solution: update windows

7.ICMP Timestamp Reply Information Disclosure

Summary: The remote host responded to an ICMP timestamp request.



ICMP Timestamp Reply Information Disclosure	⇆	2.1 (Low)	80 %	192.168.1.20	192.168.1.20	general/icmp	N/A	N/A	Sun, Apr 13, 2025 8:04 PM UTC

Impact:

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution: Mitigation

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely.

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks).

References: CVE-1999-0524

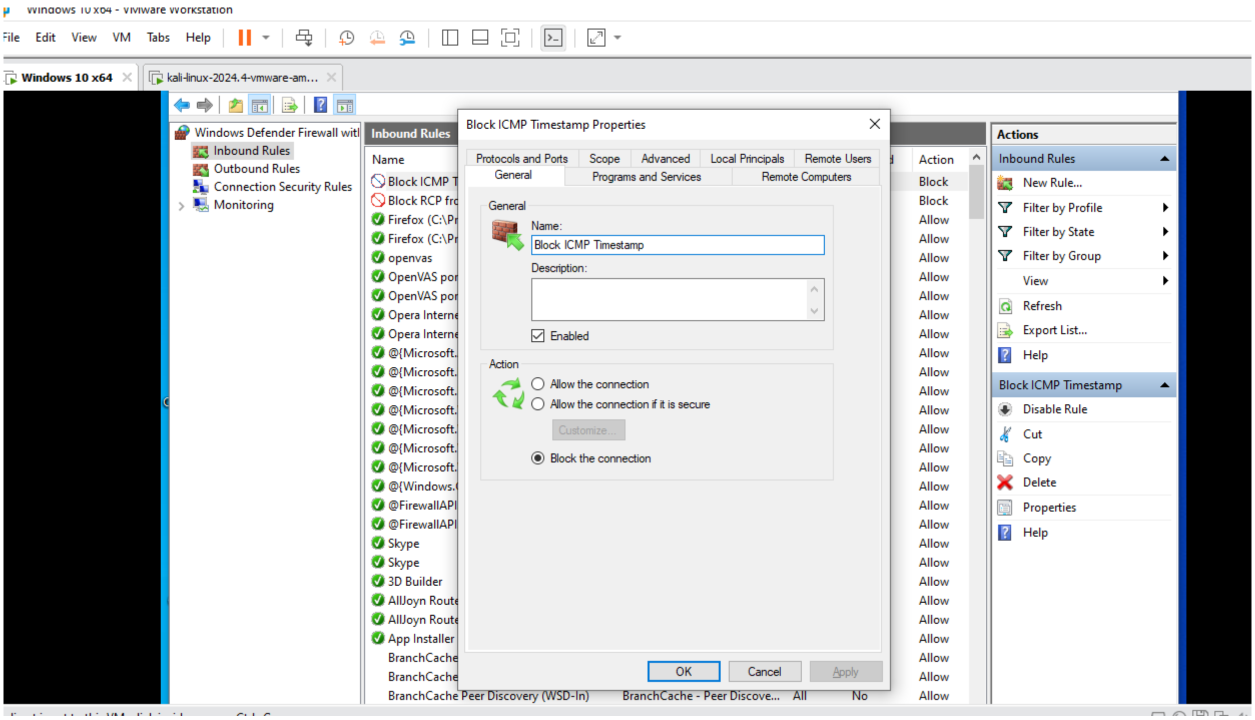
Fix vulnerability:

create a firewall rule for this one with the following settings:

1.Open **Windows Defender Firewall with Advanced Security**

2.Create a **new inbound rule**:

- Type: **Custom**
- Protocol: **ICMPv4**
- ICMP settings: Choose **Specific ICMP types**, and deselect **Timestamp Request**
- Action: **Block**
- Apply to: All profiles
- Name: e.g., *Block ICMP Timestamp*



Block ICMP Timestamp Properties

General

Name: Block ICMP Timestamp

Description:

☑ Enabled

Action

○ Allow the connection

○ Allow the connection if it is secure

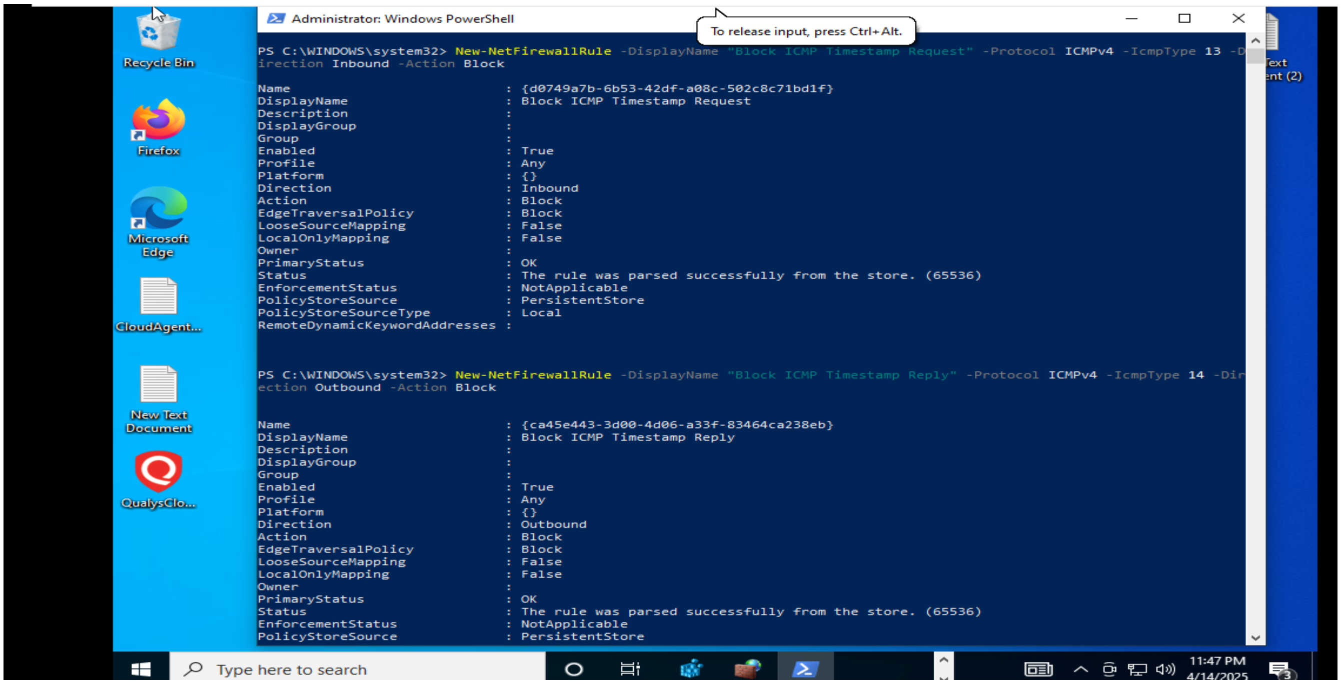
● Block the connection

Name				Action
Block ICMP T				Block
Block RCP fro				Block
Firefox (C:\Pr				Allow
Firefox (C:\Pr				Allow
openvas				Allow
OpenVAS por				Allow
OpenVAS por				Allow
Opera Interne				Allow
Opera Interne				Allow
@{Microsoft.				Allow
@{Microsoft.				Allow
@{Microsoft.				Allow
@{Microsoft.				Allow
@{Microsoft.				Allow
@{Microsoft.				Allow
@{Microsoft.				Allow
@{Windows.				Allow
@FirewallAPI				Allow
@FirewallAPI				Allow
Skype				Allow
Skype				Allow
3D Builder				Allow
AllJoyn Route				Allow
AllJoyn Route				Allow
App Installer				Allow
BranchCache				Allow
BranchCache				Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow

Or use **PowerShell**:

New-NetFirewallRule -DisplayName "Block ICMP Timestamp Request" -Protocol ICMPv4 -IcmpType 13 -Direction Inbound -Action Block

New-NetFirewallRule -DisplayName "Block ICMP Timestamp Reply" -Protocol ICMPv4 -IcmpType 14 -Direction Outbound -Action Block



```
PS C:\WINDOWS\system32> New-NetFirewallRule -DisplayName "Block ICMP Timestamp Request" -Protocol ICMPv4 -IcmpType 13 -D
irection Inbound -Action Block

Name                          : {d0749a7b-6b53-42df-a08c-502c8c71bd1f}
DisplayName                   : Block ICMP Timestamp Request
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses :



PS C:\WINDOWS\system32> New-NetFirewallRule -DisplayName "Block ICMP Timestamp Reply" -Protocol ICMPv4 -IcmpType 14 -Dir
ection Outbound -Action Block


Name                          : {ca45e443-3d00-4d06-a33f-83464ca238eb}
DisplayName                   : Block ICMP Timestamp Reply
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Outbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
```