Scan Report

January 4, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "hi". The scan started at Sat Jan 4 15:46:42 2025 UTC and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.1	0	2	1	0	0
192.168.1.17	0	0	2	0	0
192.168.1.18	0	0	1	0	0
192.168.1.16	0	0	1	0	0
192.168.1.5	0	0	1	0	0
Total: 5	0	2	6	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 8 results selected by the filtering described above. Before filtering there were 105 results.

2 Results per Host

2.1 192.168.1.1

Host scan start   Sat Jan 4 15:48:03 2025 UTC
Host scan end

Service (Port)	Threat Level
53/udp	Medium
80/tcp	Medium
general/tcp	Low

2.1.1 Medium 53/udp

Medium (CVSS: 5.0)
NVT: DNS Cache Snooping Vulnerability (UDP) - Active Check
Summary
. . . continues on next page . . .

The DNS server is prone to a cache snooping vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
Received (an) answer(s) for a non-recursive query for "example.com".
Result:
93.184.215.14
```

Impact
Attackers might gain information about cached DNS records which might lead to further attacks.
Note: This finding might be an acceptable risk if you:
- trust all clients which can reach the server
- do not allow recursive queries from outside your trusted client network.

Solution:
Solution type: Mitigation
There are multiple possible mitigation steps depending on location and functionality needed by the DNS server:
- Disable recursion
- Don't allow public access to DNS Servers doing recursion
- Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients

Vulnerability Insight
DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.
This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.
This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.
DNS cache snooping is possible even if the DNS server is not configured to resolve recursively for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a. 'lame requests').

Vulnerability Detection Method
Sends a crafted DNS query and checks the response.
Details: `DNS Cache Snooping Vulnerability (UDP) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.146591
Version used: `2023-03-24T10:19:42Z`

References
```
url: https://www.cs.unc.edu/~fabian/course_papers/cache_snooping.pdf
url: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns
```

```
↪-server-cache-snooping-attacks
url: https://kb.isc.org/docs/aa-00509
url: https://kb.isc.org/docs/aa-00482
```

[return to 192.168.1.1]

2.1.2   Medium 80/tcp

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The following input fields were identified (URL:input name):
http://192.168.1.1/:Frm_Password
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`

OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 192.168.1.1]

2.1.3   Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`It was detected that the host implements RFC1323/RFC7323.`
`The following timestamps were retrieved with a delay of 1 seconds in-between:`
`Packet 1: 23602019`
`Packet 2: 23602129`

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

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.
Vulnerability Detection Method   Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.   Details: `TCP Timestamps Information Disclosure`   OID:1.3.6.1.4.1.25623.1.0.80091   Version used: `2023-12-15T16:10:08Z`
References   url: `https://datatracker.ietf.org/doc/html/rfc1323`   url: `https://datatracker.ietf.org/doc/html/rfc7323`   url: `https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`   ↪`ownload/details.aspx?id=9152`   url: `https://www.fortiguard.com/psirt/FG-IR-16-090`

2.2 192.168.1.17

Host scan start	Sat Jan 4 15:48:03 2025 UTC
Host scan end	Sat Jan 4 16:02:45 2025 UTC

Service (Port)	Threat Level
general/tcp	Low
general/icmp	Low

2.2.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
Summary   The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%

Vulnerability Detection Result
 `It was detected that the host implements RFC1323/RFC7323.`
 `The following timestamps were retrieved with a delay of 1 seconds in-between:`
 `Packet 1: 3672544858`

Packet 2: 3672545922

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

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: TCP Timestamps Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2023-12-15T16:10:08Z

References
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

2.2.2   Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

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

Solution:
Solution type: 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)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.1.17]

2.3   192.168.1.18

Host scan start   Sat Jan 4 15:48:03 2025 UTC
Host scan end

Service (Port)	Threat Level
general/tcp	Low

2.3.1   Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3695514
Packet 2: 3695790
```

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

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091

. . . continues on next page . . .

Version used: 2023-12-15T16:10:08Z
References url: https://datatracker.ietf.org/doc/html/rfc1323 url: https://datatracker.ietf.org/doc/html/rfc7323 url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d ↪ownload/details.aspx?id=9152 url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 192.168.1.18]

2.4   192.168.1.16

Host scan start   Sat Jan 4 15:48:03 2025 UTC
Host scan end   Sat Jan 4 15:58:30 2025 UTC

Service (Port)	Threat Level
general/tcp	Low

2.4.1   Low general/tcp

Low (CVSS: 2.6)
NVT: TCP Timestamps Information Disclosure
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.
Quality of Detection (QoD): 80%

Vulnerability Detection Result
`It was detected that the host implements RFC1323/RFC7323.`
`The following timestamps were retrieved with a delay of 1 seconds in-between:`
`Packet 1: 1310326672`
`Packet 2: 1310327757`

Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Solution: **Solution type:** Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

. . . continued from previous page . . .

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
url: `https://datatracker.ietf.org/doc/html/rfc1323`
url: `https://datatracker.ietf.org/doc/html/rfc7323`
url: `https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
↪`ownload/details.aspx?id=9152`
url: `https://www.fortiguard.com/psirt/FG-IR-16-090`

2.5   192.168.1.5

Host scan start	Sat Jan 4 15:48:03 2025 UTC
Host scan end	Sat Jan 4 15:52:26 2025 UTC

Service (Port)	Threat Level
general/icmp	Low

2.5.1   Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
. . . continues on next page . . .

The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

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

Solution:
Solution type: 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)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.1.5]

This file was automatically generated.