Report generated by Nessus™

customersrus.co.uk basic scan nessus 040222

Fri, 04 Feb 2022 18:51:07 China Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

Collapse All | Expand All

15855 (1) - POP3 Cleartext Logins Permitted -

Synopsis

The remote POP3 daemon allows credentials to be transmitted in cleartext.

Description

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

See Also

https://tools.ietf.org/html/rfc2222
https://tools.ietf.org/html/rfc2595

Solution

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2004/11/30, Modified: 2017/06/12

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/110/pop3)

```
The following cleartext methods are supported :
USER
SASL PLAIN LOGIN
```

54582 (1) - SMTP Service Cleartext Login Permitted -

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

https://tools.ietf.org/html/rfc4422
https://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2011/05/19, Modified: 2021/01/19

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/587/smtp)

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 587 :

All supported methods : LOGIN, PLAIN
Cleartext methods : LOGIN, PLAIN
```

11219 (16) - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2022/02/02

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/21/ftp)

```
Port 21/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/53/dns)

```
Port 53/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/80/www)

```
Port 80/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/110/pop3)

```
Port 110/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/143/imap)

```
Port 143/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/443/www)

```
Port 443/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/587/smtp)

```
Port 587/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/993/imap)

```
Port 993/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/2078/www)

```
Port 2078/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/2082/www)

```
Port 2082/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/2087/www)

```
Port 2087/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/2096/www)

```
Port 2096/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/3306/mysql)

```
Port 3306/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/5060)

```
Port 5060/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/5432)

```
Port 5432/tcp was found to be open
```

68.66.247.187.static.a2webhosting.com (tcp/8080)

```
Port 8080/tcp was found to be open
```

22964 (15) - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2021/04/14

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/21/ftp)

```
An FTP server is running on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/80/www)

```
A web server is running on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/110/pop3)

```
A POP3 server is running on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/143/imap)

```
An IMAP server is running on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/443/www)

```
A TLSv1.2 server answered on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/443/www)

```
A web server is running on this port through TLSv1.2.
```

68.66.247.187.static.a2webhosting.com (tcp/587/smtp)

```
An SMTP server is running on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/993/imap)

```
A TLSv1.1 server answered on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/993/imap)

```
An IMAP server is running on this port through TLSv1.1.
```

68.66.247.187.static.a2webhosting.com (tcp/2078/www)

```
A TLSv1.2 server answered on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/2078/www)

```
A web server is running on this port through TLSv1.2.
```

68.66.247.187.static.a2webhosting.com (tcp/2087/www)

```
A TLSv1.2 server answered on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/2087/www)

```
A web server is running on this port through TLSv1.2.
```

68.66.247.187.static.a2webhosting.com (tcp/2096/www)

```
A TLSv1.2 server answered on this port.
```

68.66.247.187.static.a2webhosting.com (tcp/2096/www)

```
A web server is running on this port through TLSv1.2.
```

10107 (2) - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/443/www)

```
The remote web server type is :

Apache
```

68.66.247.187.static.a2webhosting.com (tcp/2078/www)

```
The remote web server type is :

cPanel
```

11002 (2) - DNS Server Detection -

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/53/dns)
68.66.247.187.static.a2webhosting.com (udp/53/dns)

11414 (2) - IMAP Service Banner Retrieval -

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/143/imap)

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

68.66.247.187.static.a2webhosting.com (tcp/993/imap)

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

10028 (1) - DNS Server BIND version Directive Remote Version Detection -

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

68.66.247.187.static.a2webhosting.com (udp/53/dns)

```
Version : 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8
```

10092 (1) - FTP Server Detection -

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/21/ftp)

```
The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 2 of 80 allowed.
220-Local time is now 10:55. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure -

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

0.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS v2.0 Base Score

0.0 (CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2019/10/04

Plugin Output

68.66.247.187.static.a2webhosting.com (icmp/0)

```
The remote clock is synchronized with the local clock.
```

10180 (1) - Ping the remote host -

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2021/10/04

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
The remote host is up
The remote host replied to an ICMP echo packet
```

10185 (1) - POP Server Detection -

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

https://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/110/pop3)

```
Remote POP server banner :

+OK Dovecot ready.
```

10263 (1) - SMTP Server Detection -

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/587/smtp)

```
Remote SMTP server banner :

220-nl1-ss5.a2hosting.com ESMTP Exim 4.94.2 #2 Fri, 04 Feb 2022 10:53:01 +0100
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

10287 (1) - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

68.66.247.187.static.a2webhosting.com (udp/0)

```
For your information, here is the traceroute from 10.8.3.5 to 68.66.247.187 :
10.8.3.5
68.66.247.187

Hop Count: 1
```

10919 (1) - Open Port Re-check -

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2021/07/23

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
Port 110 was detected as being open but is now unresponsive
Port 3306 was detected as being open but is now unresponsive
Port 587 was detected as being open but is now unresponsive
Port 2096 was detected as being open but is now unresponsive
Port 2087 was detected as being open but is now unresponsive
Port 5432 was detected as being open but is now unresponsive
Port 2082 was detected as being open but is now unresponsive
Port 143 was detected as being open but is now unresponsive
Port 2078 was detected as being open but is now unresponsive
Port 21 was detected as being open but is now unresponsive
Port 53 was detected as being open but is now unresponsive
Port 993 was detected as being open but is now unresponsive
Port 443 was detected as being open but is now unresponsive
```

11153 (1) - Service Detection (HELP Request) -

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/3306/mysql)

```
A MySQL server is running on this port.
```

11936 (1) - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/01/18

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

ICMP::1:1:0:64:1:64:1:0:::0::1:>64:64:0:1:1:2:1:1:1:1:0:64:28960:MSTNW:7:1:1
SinFP:
P1:B10113:F0x12:W65535:O0204ffff:M1256:
P2:B10113:F0x12:W65535:O0204ffff0402080affffffff4445414401030309:M1256:
P3:B00000:F0x00:W0:O0:M0
P4:190100_7_p=443R
HTTP:!:Server: Apache

SMTP:!:220-nl1-ss5.a2hosting.com ESMTP Exim 4.94.2 #2 Fri, 04 Feb 2022 10:53:01 +0100
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.


The remote host is running Linux Kernel 2.6
```

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution -

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
68.66.247.187 resolves as 68.66.247.187.static.a2webhosting.com.
```

19506 (1) - Nessus Scan Information -

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
Information about this scan :

Nessus version : 10.1.0
Nessus build : X20054
Plugin feed version : 202202040249
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : customersrus.co.uk basic scan nessus 040222
Scan policy used : Basic Network Scan
Scanner IP : 10.8.3.5
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 265.021 ms
Thorough tests : yes
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : all_pairs
```

```
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 10 minutes.
Web app tests - Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2022/2/4 16:51 China Standard Time
Scan duration : 7064 sec
```

25220 (1) - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

35371 (1) - DNS Server hostname.bind Map Hostname Disclosure -

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

68.66.247.187.static.a2webhosting.com (udp/53/dns)

```
The remote host name is :

nl1-ss5.a2hosting.com
```

40405 (1) - Web Server Detection (HTTP/1.1) -

Synopsis

A web server is running on this port.

Description

The web server on this port responds to HTTP/1.1 requests and appears to ignore HTTP/1.0 requests, which is unusual.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2019/11/22

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/2082/www)

42088 (1) - SMTP Service STARTTLS Command Support -

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc2487

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/587/smtp)

```
The remote SMTP service responded to the 'STARTTLS' command with a
'220' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

42149 (1) - FTP Service AUTH TLS Command Support -

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS
https://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/15, Modified: 2021/02/24

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/21/ftp)

```
The remote FTP service responded to the 'AUTH TLS' command with a
'234' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

45590 (1) - Common Platform Enumeration (CPE) -

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2022/02/02

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE's matched on the remote system :

cpe:/a:isc:bind:9.11.4-p2-redhat-9.11.4-26.p2.el7_9.8
cpe:/a:isc:bind:9.11.4:p2
```

46215 (1) - Inconsistent Hostname and IP Address -

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information

Published: 2010/05/03, Modified: 2016/08/05

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
The host name '68.66.247.187.static.a2webhosting.com' does not resolve to an IP address
```

54580 (1) - SMTP Authentication Methods -

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422
https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information

Published: 2011/05/19, Modified: 2019/03/05

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/587/smtp)

```
The following authentication methods are advertised by the SMTP
server without encryption :
LOGIN
PLAIN
```

54615 (1) - Device Type -

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

72779 (1) - DNS Server Version Detection -

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2020/09/22

Plugin Output

68.66.247.187.static.a2webhosting.com (tcp/53/dns)

```
DNS server answer for "version.bind" (over TCP) :

9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8
```