CS581 (Computer & Network Security)

Lab-02

Date: 10/21/2015

Group No.: 05
Group Members:
01. Rajnish Kumar (CIN: 304470392)
02. Jay Purohit (CIN: 304455065)
03. Rupal Jaiswal (CIN: 304442169)
04. Gaurav Prajapati (CIN: 304470132)

Penetration and Vulnerability testing

Install a network-based vulnerability scanner Nessus (www.nessus.org) onto your computer and perform a vulnerability scan of another computer. Submit vulnerability report of services that pose medium or high security risk. Be sure to temporarily turn off any host-based firewall software if needed to get meaningful output.

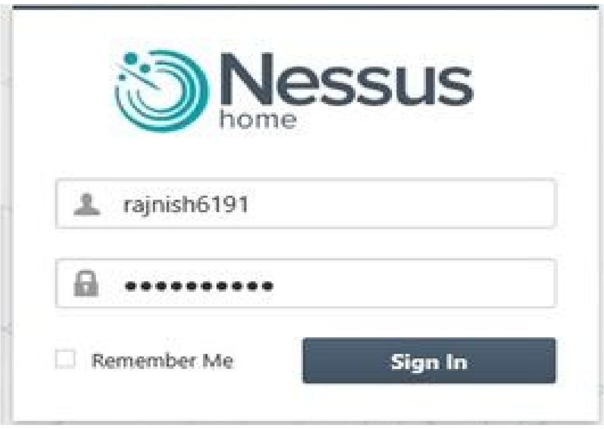
We, Group No. 5, going to perform this lab in below steps:

Step 1: Downloading & Installing nessus software

Step 2: Screenshots of vulnerability report of services (with details)

Step 1: Downloading & Installing nessus software

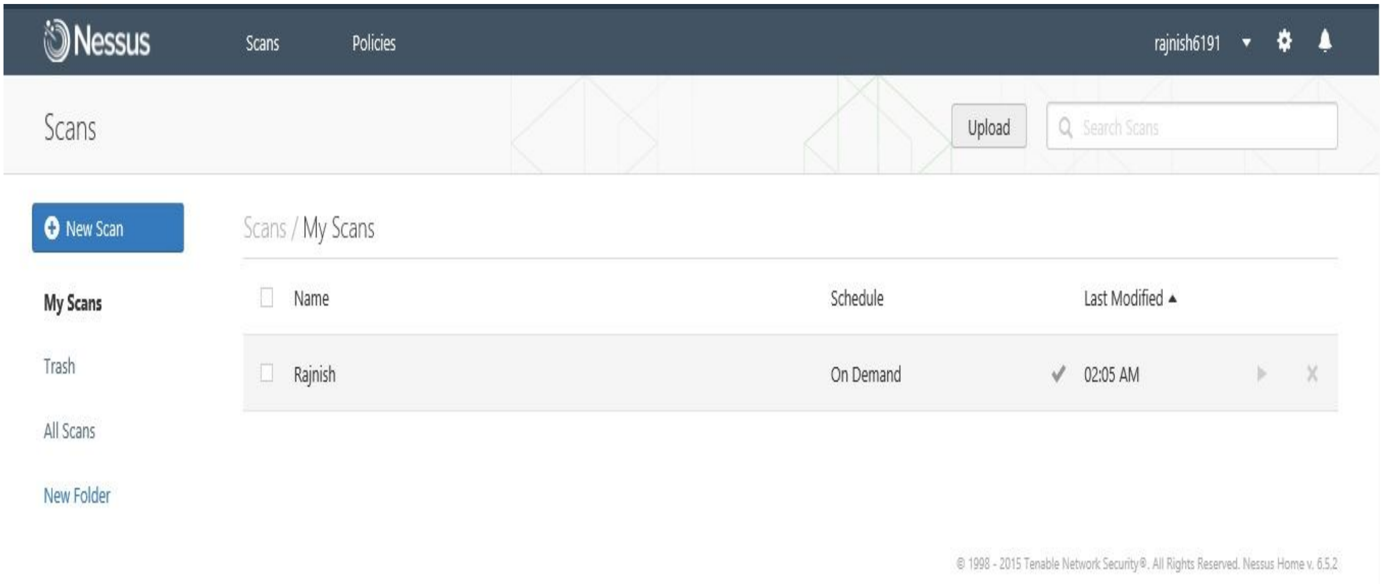
- ⇨ We downloaded the nessus Home software from www.nessus.org and installed.
- ⇨ Below is the screenshot of nessus with login credentials.



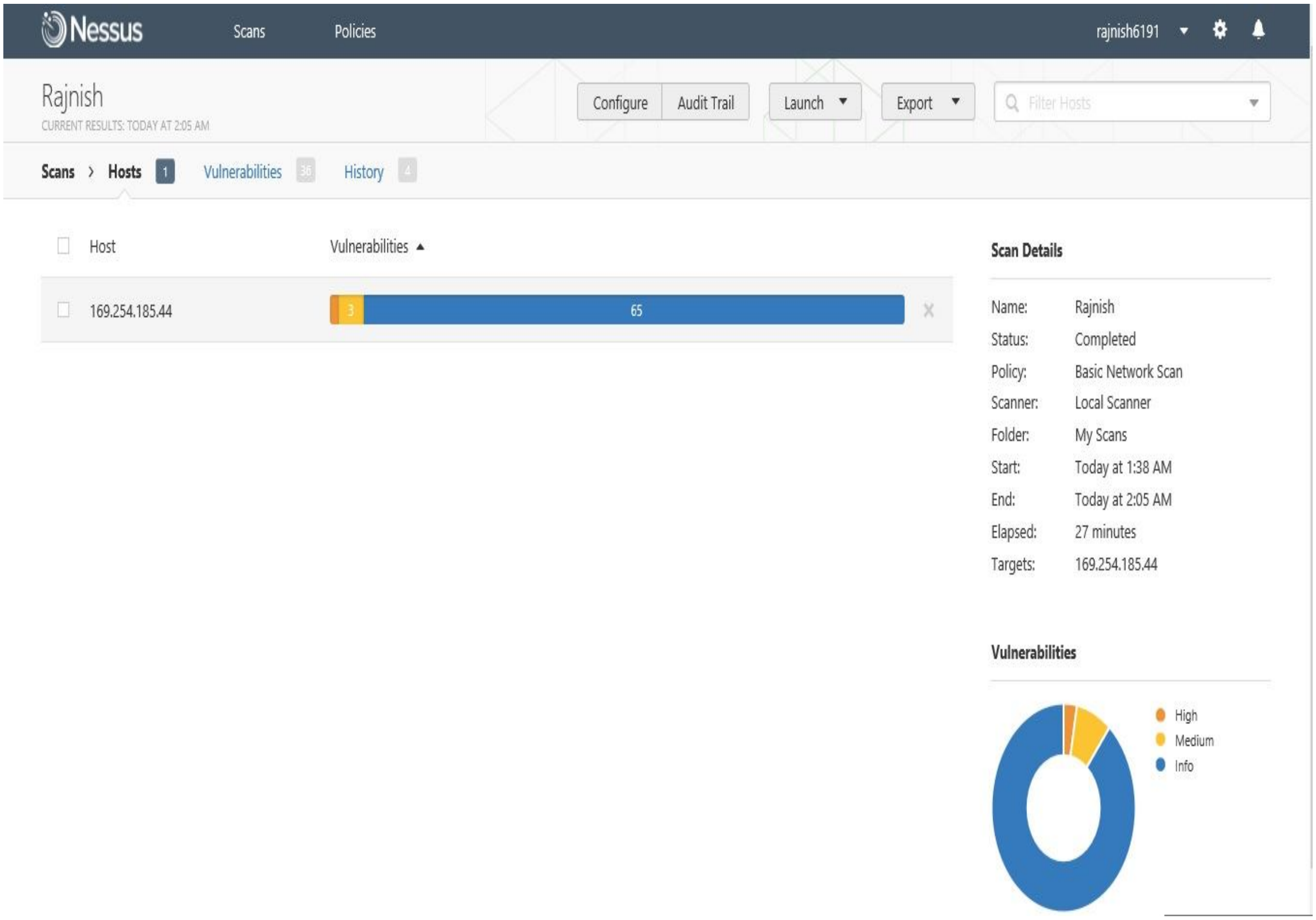
rajnish6191

●●●●●●●●●●●

Step 2: Screenshots of vulnerability report of services (with details)



□	Name	Schedule		Last Modified ▲
□	Rajnish	On Demand	✓	02:05 AM



Rajnish

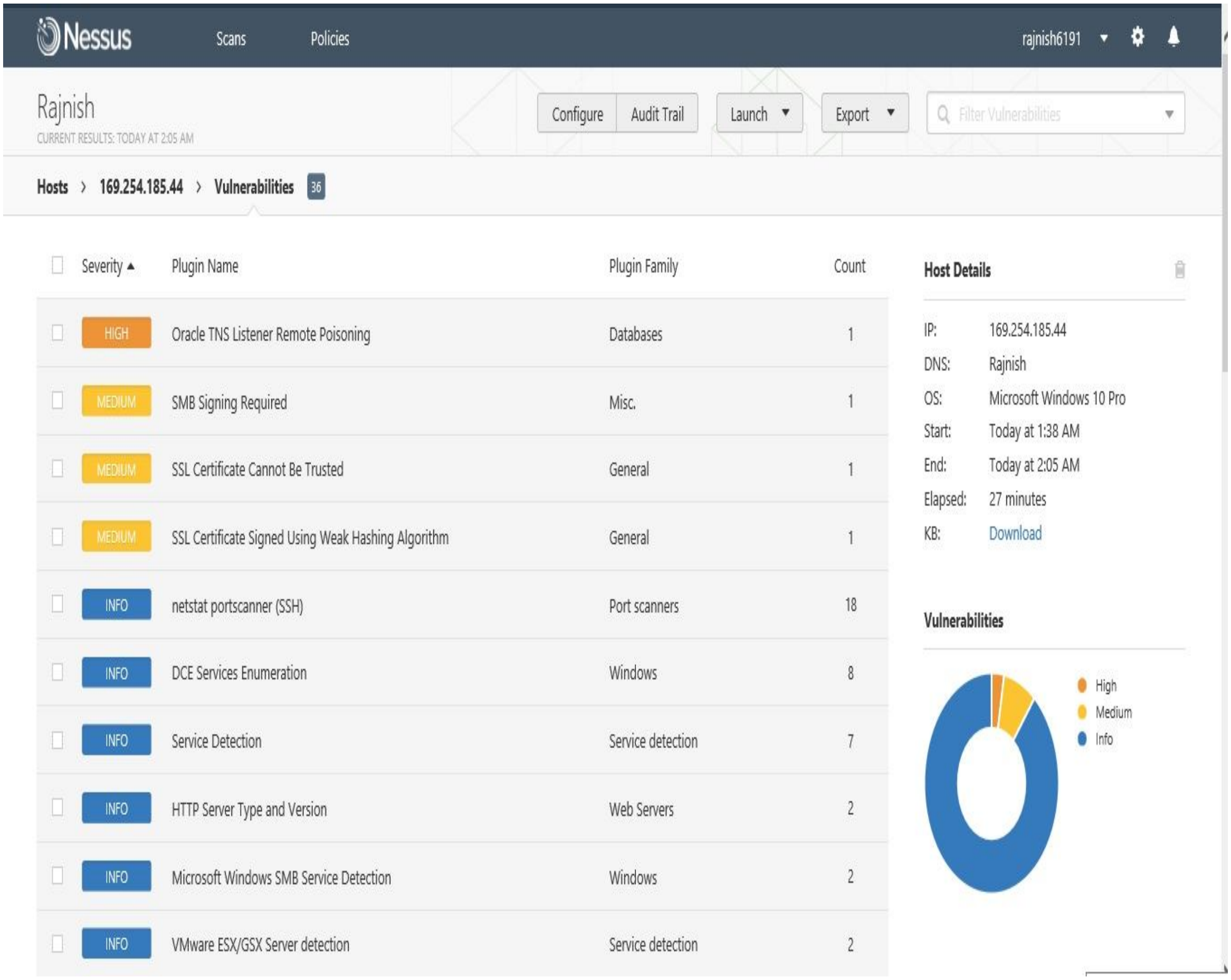
CURRENT RESULTS: TODAY AT 2:05 AM

Host	Vulnerabilities ▲
□ 169.254.185.44	3 65

Scan Details

Name:	Rajnish
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 1:38 AM
End:	Today at 2:05 AM
Elapsed:	27 minutes
Targets:	169.254.185.44

Vulnerabilities



Rajnish

CURRENT RESULTS: TODAY AT 2:05 AM

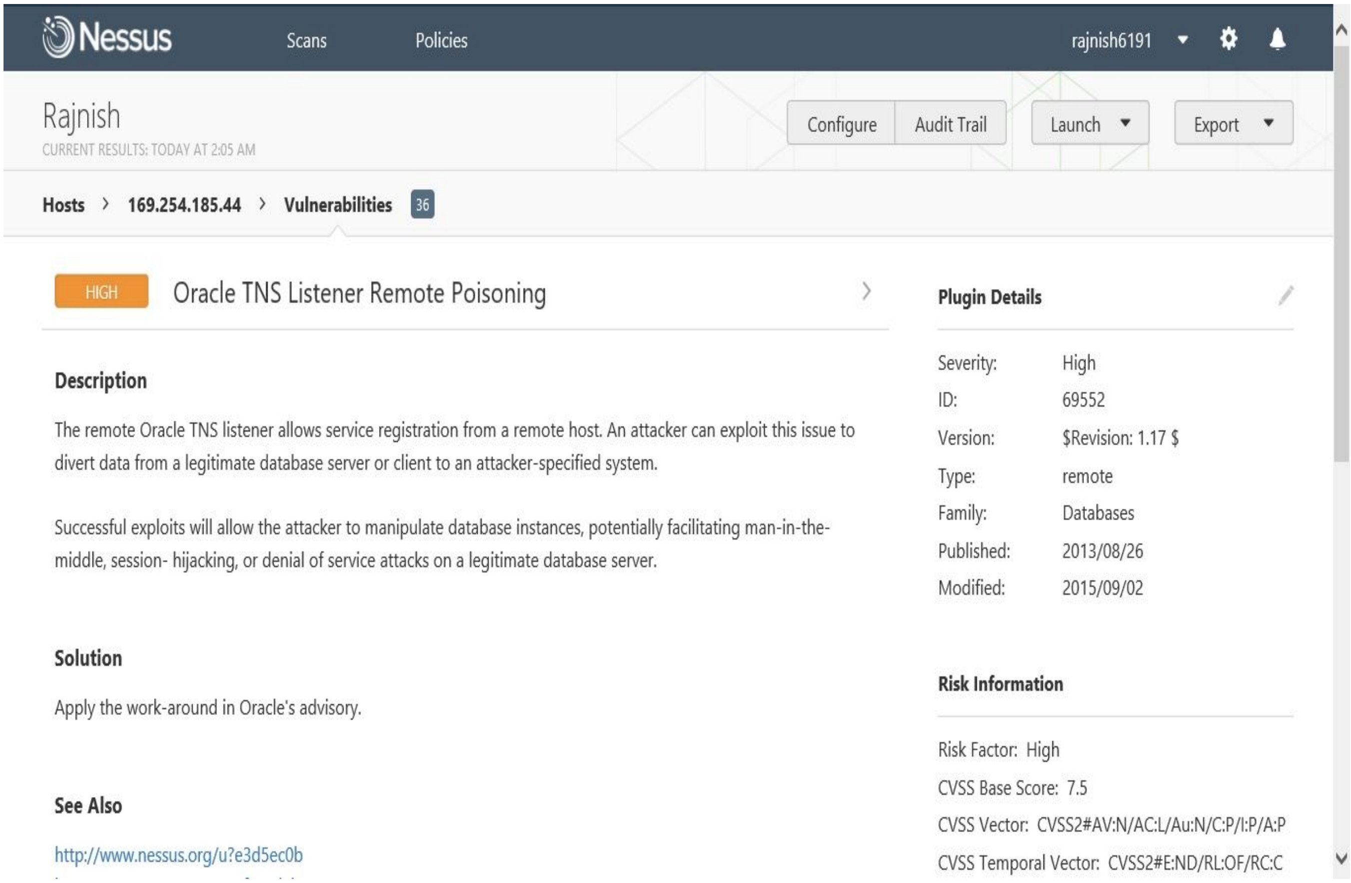
Hosts › 169.254.185.44 › Vulnerabilities 36

□	Severity ▲	Plugin Name	Plugin Family	Count
□	HIGH	Oracle TNS Listener Remote Poisoning	Databases	1
□	MEDIUM	SMB Signing Required	Misc.	1
□	MEDIUM	SSL Certificate Cannot Be Trusted	General	1
□	MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
□	INFO	netstat portscanner (SSH)	Port scanners	18
□	INFO	DCE Services Enumeration	Windows	8
□	INFO	Service Detection	Service detection	7
□	INFO	HTTP Server Type and Version	Web Servers	2
□	INFO	Microsoft Windows SMB Service Detection	Windows	2
□	INFO	VMware ESX/GSX Server detection	Service detection	2

Host Details

IP:	169.254.185.44
DNS:	Rajnish
OS:	Microsoft Windows 10 Pro
Start:	Today at 1:38 AM
End:	Today at 2:05 AM
Elapsed:	27 minutes
KB:	Download

Vulnerabilities



Rajnish

CURRENT RESULTS: TODAY AT 2:05 AM

Hosts › 169.254.185.44 › Vulnerabilities 36

HIGH Oracle TNS Listener Remote Poisoning

Description

The remote Oracle TNS listener allows service registration from a remote host. An attacker can exploit this issue to divert data from a legitimate database server or client to an attacker-specified system.

Successful exploits will allow the attacker to manipulate database instances, potentially facilitating man-in-the-middle, session- hijacking, or denial of service attacks on a legitimate database server.

Solution

Apply the work-around in Oracle's advisory.

See Also

http://www.nessus.org/u?e3d5ec0b

Plugin Details

Severity:	High
ID:	69552
Version:	$Revision: 1.17 $
Type:	remote
Family:	Databases
Published:	2013/08/26
Modified:	2015/09/02

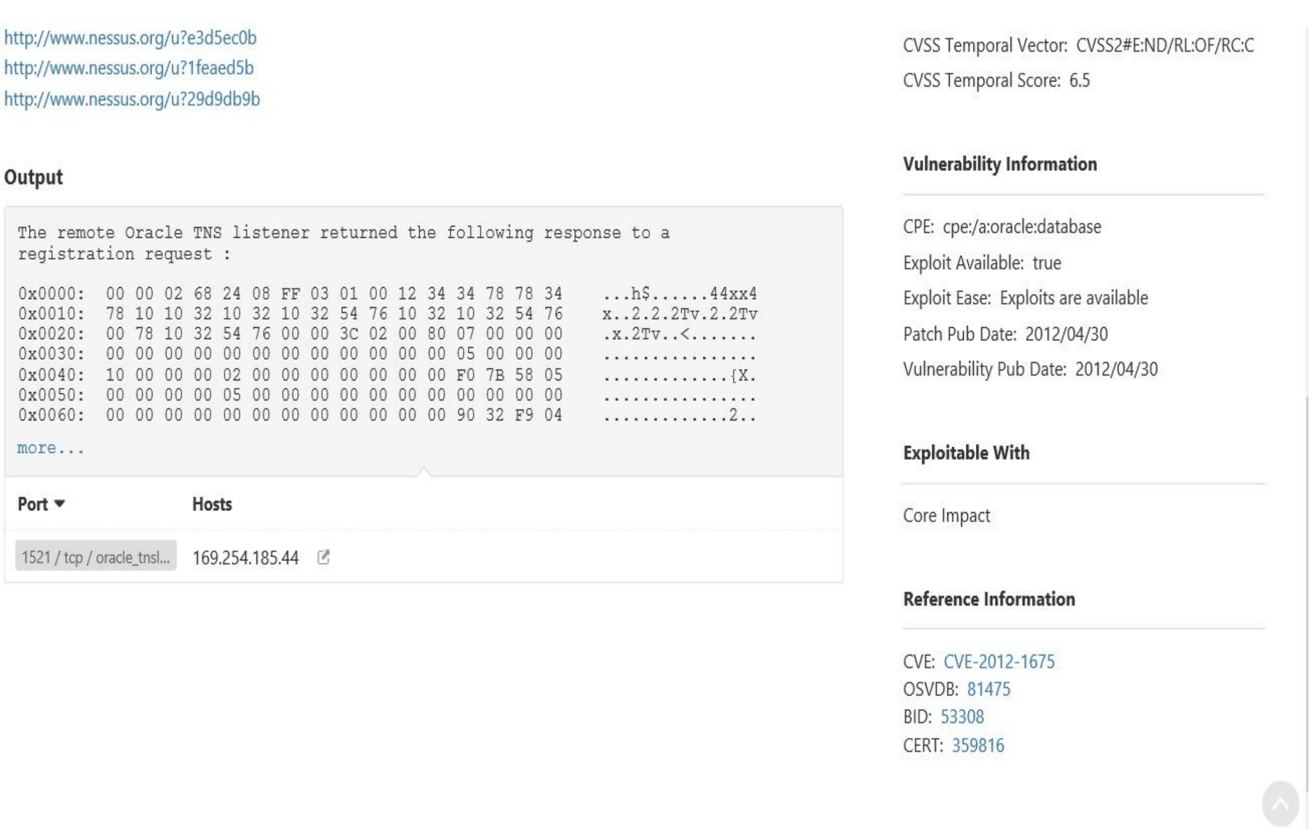
Risk Information

Risk Factor: High

CVSS Base Score: 7.5

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C



http://www.nessus.org/u?e3d5ec0b

http://www.nessus.org/u?1feaed5b

http://www.nessus.org/u?29d9db9b

Output

```
The remote Oracle TNS listener returned the following response to a
registration request :

0x0000:  00 00 02 68 24 08 FF 03 01 00 12 34 34 78 78 34    ...h$......44xx4
0x0010:  78 10 10 32 10 32 10 32 54 76 10 32 10 32 54 76    x..2.2.2Tv.2.2Tv
0x0020:  00 78 10 32 54 76 00 00 3C 02 00 80 07 00 00 00    .x.2Tv..<.......
0x0030:  00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00    ................
0x0040:  10 00 00 00 02 00 00 00 00 00 00 00 F0 7B 58 05    ............{X.
0x0050:  00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00    ................
0x0060:  00 00 00 00 00 00 00 00 00 00 00 00 90 32 F9 04    ............2..
more...
```

Port ▾	Hosts
1521 / tcp / oracle_tnsl...	169.254.185.44

CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C

CVSS Temporal Score: 6.5

Vulnerability Information

CPE: cpe:/a:oracle:database

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: 2012/04/30

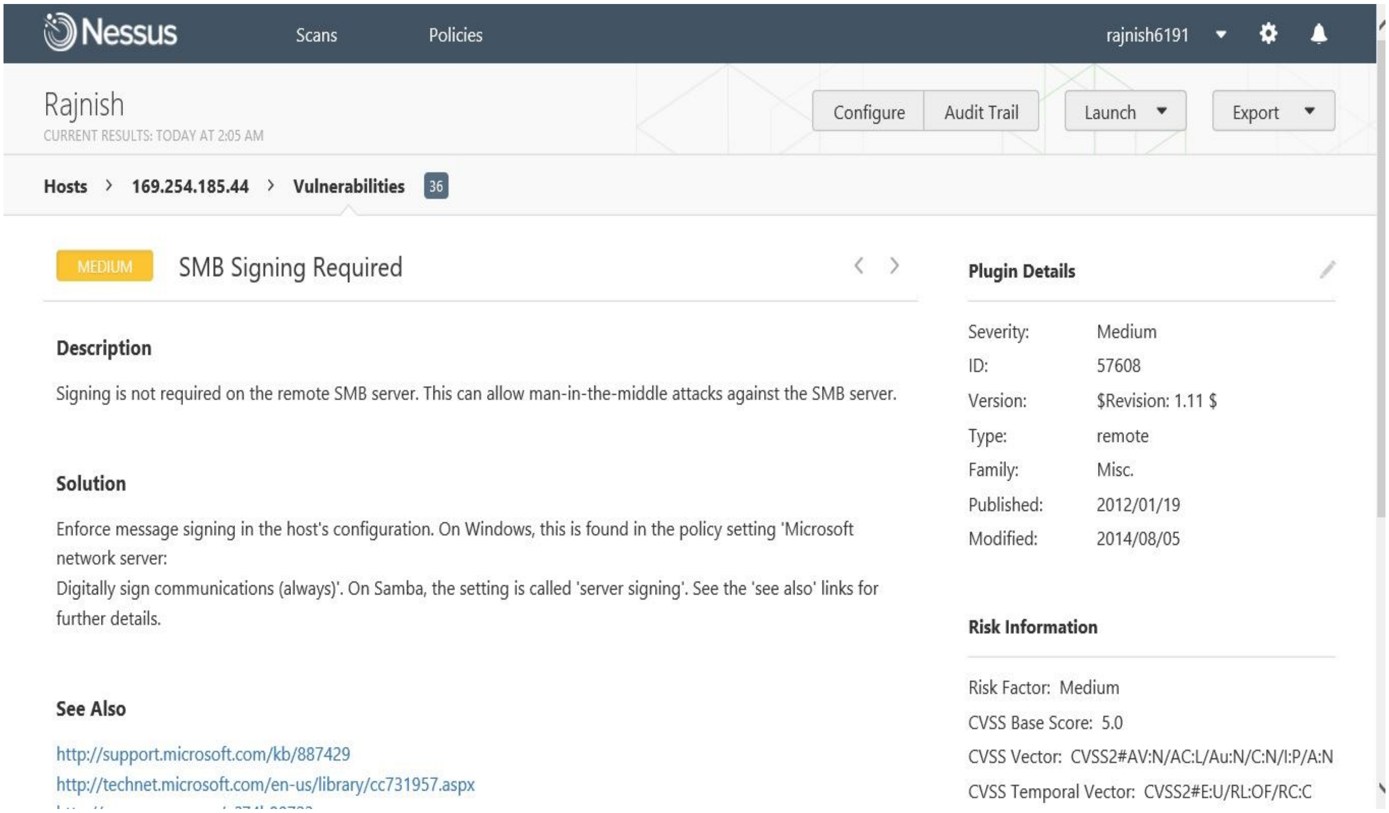
Vulnerability Pub Date: 2012/04/30

Exploitable With

Core Impact

Reference Information

CVE: CVE-2012-1675
OSVDB: 81475
BID: 53308
CERT: 359816



Rajnish

CURRENT RESULTS: TODAY AT 2:05 AM

Hosts > 169.254.185.44 > Vulnerabilities 36

MEDIUM SMB Signing Required

Description

Signing is not required on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server:
Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

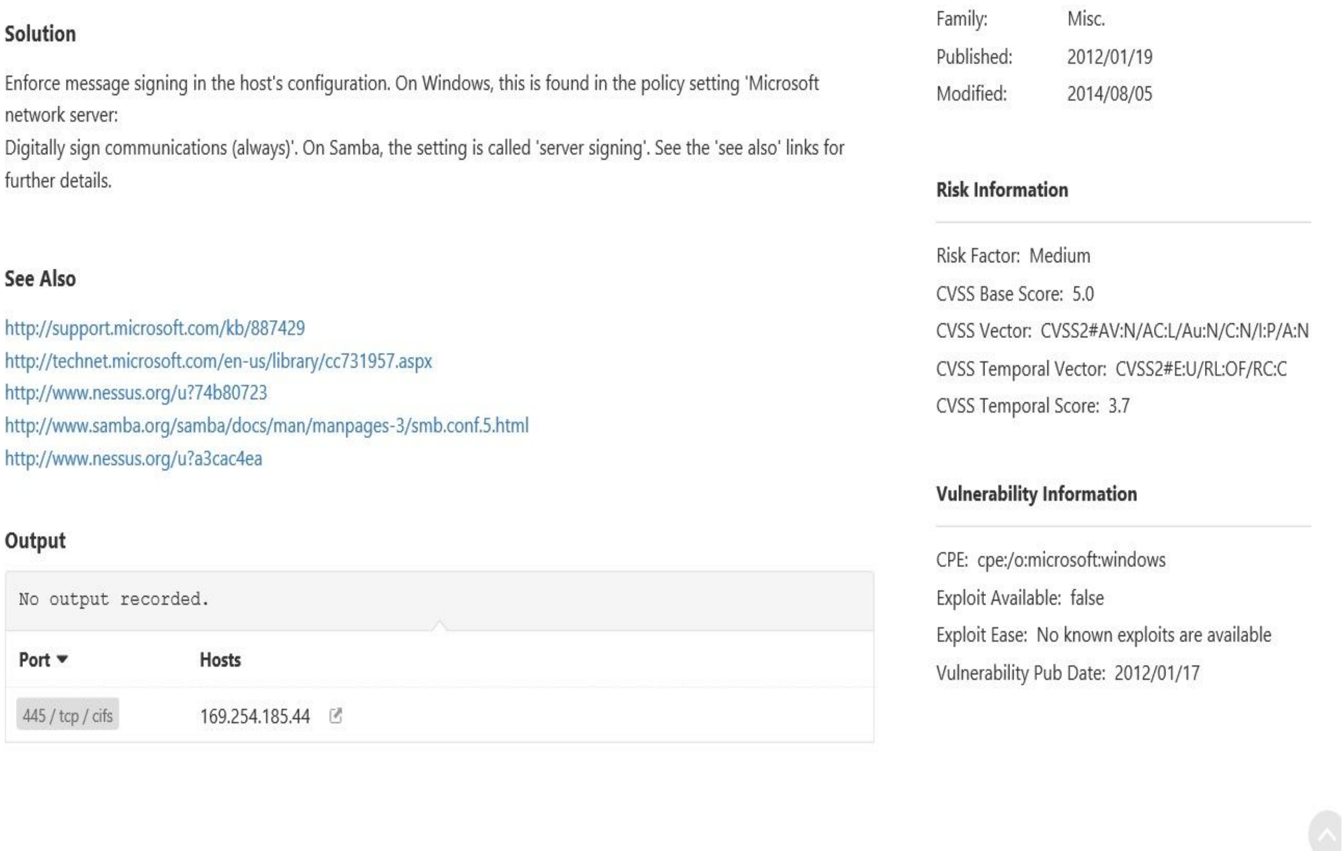
http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx

Plugin Details

Severity:	Medium
ID:	57608
Version:	$Revision: 1.11 $
Type:	remote
Family:	Misc.
Published:	2012/01/19
Modified:	2014/08/05

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C



Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server:
Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

Port	Hosts
445 / tcp / cifs	169.254.185.44

Family:	Misc.
Published:	2012/01/19
Modified:	2014/08/05

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C
CVSS Temporal Score: 3.7

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 2012/01/17