

CNS Lab Assignment 7- Nessus and ARPWatch

111703013 Akshay Deodhar

27th October 2020

ARP Spoofing

- ARP (Address Resolution Protocol) is a protocol used by hosts for discovering the Link Layer Address (usually MAC) corresponding to a known IP address.
- ARP provides *hardware addresses* and is used on a LAN. A host on a LAN requires the hardware address of the host which it wants to send a frame to.
- Because the source host does not know the hardware address of the destination host, it **broadcasts** an ARP frame to all hosts within the LAN. For example, if the host's MAC is XYZ, and the destination IP address is ABC, it broadcasts a packet of form
"Who has ABC? tell XYZ"
- When someone resolves the IP address, the source host accepts the resolution *without authentication*, and begins to send frames meant for the destination IP address to the hardware address recorded in its tables.
- Furthermore, ARP is stateless, which means that the source host does not keep track of ARP requests which it sends. So if a host receives an ARP reply, it assumes its validity without authentication, and replaces the corresponding entry in its tables. This cached entry is then used by the host till it expires.
- The nature of ARP (described above) renders it vulnerable to an attack called ARP spoofing.
- ARP spoofing is a technique used by a malicious host in which it sends spoofed ARP replies onto a local area network, with an aim of associate its own hardware address with the IP address of some other host.
- If this succeeds, then the malicious host will be sent all the traffic which is meant for some other host.
- Using this, the malicious host may do any of the following:
 1. Denial of Service (traffic does not reach the intended host)
 2. Man-in-the-Middle (the malicious host modifies data before forwarding it)

TL;DR

1. What is ARP Spoofing?

- A technique used by a malicious host to associate its hardware address to the IP address of another host

2. How it happens?

- The malicious host sends spoofed ARP reply packets, which causes other hosts to update their IP:MAC tables without authentication.

3. In which network?

- Happens on a Local Area Network.

4. possible attacks with ARP Spoofing

- Denial of Service
- Session Hijacking
- Man in the Middle

Types of Vulnerabilities detected by Nessus

Nessus is a client server vulnerability scanner. It provides a number of plugins, each of which scans for a specific type of vulnerability. Nessus provides built-in templates of network scans which use subsets of these plugins, or allows custom scans where the user can choose plugins.

Vulnerability Types

1. Unauthorized access to sensitive data, or control over system
2. Misconfiguration vulnerabilities
3. Absence of passwords, or use of default passwords.
 - Nessus checks for default passwords for various types of web applications, and can also launch an attack using a dictionary.
4. Denial of Service
5. Vulnerabilities related to, updated to include recent exploits.
 - Operating Systems
 - Databases
 - Web Servers
 - Network devices
6. Patch levels.
 - Vendors release updates for their software from time to time for fixing newly published exploits. Nessus detects whether these patches have been applied.

What is ARPWatch tool and Nessus Tool?

Name of Tool	Open Source / Commercial	Supported OS	Features / Functionality	Drawbacks
arp-watch	Open Source, BSD	Linux, BSD	Track IP-MAC pairings, notify user via email when there is a change, uses <i>pcap</i> for tapping the ethernet traffic	Cannot detect that a particular change is due to spoofing or genuine- just reports the change
Nessus	Proprietary, Version 2 is GPL	Windows, Linux	Network Vulnerability Scanner, can scan a host, and the network associated with it, automated research generation	Is intrusive, may cause network errors, reports false positives, does not discover SQL injection attacks or business logic errors

Screenshots of ARPWatch Tools used to detect ARP Spoofing, or Nessus to find network vulnerabilities

ARPWatch

The screenshots are of the following scenario:

1. akshay-inspiron5423.aren.local or 192.168.51.221 has MAC 78:45:c4:a7:d2:c4
2. kali.aren.local or 192.168.51.230 has MAC b4:b5:2f:8d:d1:a5
3. The gateway ipcop.treknocom.local has MAC 0:50:8:3:87:93

kali.aren.local now starts a man in the middle attack using ARP spoofing (with ettercap), triggering flip-flop messages by arpwatch.

```
Terminal -
File Edit View Terminal Tabs Help

Untitled x Untitled x Untitled x

valid_lft forever preferred_lft forever
2: enp9s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 78:45:c4:a7:d2:c4 brd ff:ff:ff:ff:ff:ff
   inet 192.168.51.221/24 brd 192.168.51.255 scope global dynamic noprefixroute enp9s0
       valid_lft 3248sec preferred_lft 3248sec
   inet6 fe80::ec64:b44f:2ea5:f316/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlp7s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
   link/ether d6:67:26:79:af:d9 brd ff:ff:ff:ff:ff:ff permaddr 08:ed:b9:61:71:a7
akshay@akshay-inspiron5423 ~/.../lab_assignments/7_security_tools sudo systemctl status arpwatch@enp9s0
● arpwatch@enp9s0.service - Watch ARP on interface enp9s0
   Loaded: loaded (/usr/lib/systemd/system/arpwatch@.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
* akshay@akshay-inspiron5423 ~/.../lab_assignments/7_security_tools sudo systemctl restart arpwatch@enp9s0
akshay@akshay-inspiron5423 ~/.../lab_assignments/7_security_tools sudo systemctl status arpwatch@enp9s0
● arpwatch@enp9s0.service - Watch ARP on interface enp9s0
   Loaded: loaded (/usr/lib/systemd/system/arpwatch@.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-10-27 14:41:59 IST; 2s ago
     Process: 2799 ExecStartPre=/usr/bin/touch /var/lib/arpwatch/enp9s0.dat (code=exited, status=0/SUCCESS)
     Process: 2800 ExecStart=/usr/bin/arpwatch -f /var/lib/arpwatch/enp9s0.dat -i enp9s0 (code=exited, status=0/SUCCESS)
    Main PID: 2801 (arpwatch)
      Tasks: 1 (limit: 4554)
     Memory: 1.1M
       CGroup: /system.slice/system-arpwatch.slice/arpwatch@enp9s0.service
               └─2801 /usr/bin/arpwatch -f /var/lib/arpwatch/enp9s0.dat -i enp9s0

Oct 27 14:41:59 akshay-inspiron5423 systemd[1]: Starting Watch ARP on interface enp9s0...
Oct 27 14:41:59 akshay-inspiron5423 arpwatc[2801]: chdir(/usr/arpwatch): No such file or directory
Oct 27 14:41:59 akshay-inspiron5423 arpwatc[2801]: (using current working directory)
Oct 27 14:41:59 akshay-inspiron5423 systemd[1]: Started Watch ARP on interface enp9s0.
Oct 27 14:41:59 akshay-inspiron5423 arpwatc[2801]: listening on enp9s0
akshay@akshay-inspiron5423 ~/.../lab_assignments/7_security_tools man ettercap
akshay@akshay-inspiron5423 ~/.../lab_assignments/7_security_tools
```

Figure 1: The arpwatch service is started, it is listening on the LAN interface **enp9s0**

```
Terminal -
File Edit View Terminal Tabs Help

Untitled x Untitled x Untitled x

From: arpwatch
To: arpwatch
Subject: new station (kali.aren.local)

        hostname: kali.aren.local
        ip address: 192.168.51.230
        ethernet address: b4:b5:2f:8d:d1:a5
        ethernet vendor: <unknown>
        timestamp: Tuesday, October 27, 2020 14:55:37 +0530

From: arpwatch
To: arpwatch
Subject: new station (akshay-inspiron5423.aren.local)

        hostname: akshay-inspiron5423.aren.local
        ip address: 192.168.51.221
        ethernet address: 78:45:c4:a7:d2:c4
        ethernet vendor: <unknown>
        timestamp: Tuesday, October 27, 2020 14:55:37 +0530
arpwatch: ethernet mismatch 192.168.51.1 b4:b5:2f:8d:d1:a5 (0:50:8:3:87:93)
arpwatch: ethernet mismatch 192.168.51.1 b4:b5:2f:8d:d1:a5 (0:50:8:3:87:93)
arpwatch: ethernet mismatch 192.168.51.1 b4:b5:2f:8d:d1:a5 (0:50:8:3:87:93)

From: arpwatch
To: arpwatch
Subject: changed ethernet address (ipcop.treknocom.local)

        hostname: ipcop.treknocom.local
        ip address: 192.168.51.1
        ethernet address: 0:50:8:3:87:93
        ethernet vendor: <unknown>
old ethernet address: b4:b5:2f:8d:d1:a5
old ethernet vendor: <unknown>
        timestamp: Tuesday, October 27, 2020 15:09:07 +0530
previous timestamp: Tuesday, October 27, 2020 15:08:15 +0530
        delta: 52 seconds
```

Figure 2: The initial status of the system show by arpwatch

```
Terminal -
File Edit View Terminal Tabs Help

Untitled x Untitled x Untitled x

From: arpwatch
To: arpwatch
Subject: flip flop (ipcop.treknocom.local)

    hostname: ipcop.treknocom.local
    ip address: 192.168.51.1
    ethernet address: b4:b5:2f:8d:d1:a5
    ethernet vendor: <unknown>
old ethernet address: 0:50:8:3:87:93
old ethernet vendor: <unknown>
    timestamp: Tuesday, October 27, 2020 15:09:46 +0530
    previous timestamp: Tuesday, October 27, 2020 15:09:07 +0530
    delta: 39 seconds

From: arpwatch
To: arpwatch
Subject: flip flop (ipcop.treknocom.local)

    hostname: ipcop.treknocom.local
    ip address: 192.168.51.1
    ethernet address: 0:50:8:3:87:93
    ethernet vendor: <unknown>
old ethernet address: b4:b5:2f:8d:d1:a5
old ethernet vendor: <unknown>
    timestamp: Tuesday, October 27, 2020 15:09:52 +0530
    previous timestamp: Tuesday, October 27, 2020 15:09:50 +0530
    delta: 2 seconds

From: arpwatch
To: arpwatch
Subject: flip flop (ipcop.treknocom.local)

    hostname: ipcop.treknocom.local
    ip address: 192.168.51.1
```

Figure 3: Flip flop messages from arpwatch showing a change in the MAC-IP tables (the messages are shown on stderr, when run in -d or debug mode), The old MAC for 192.168.51.1 was 0:50:8:3:87:93. The flip flop message shows that it changed to b4:b5:2f:8d:d1:a5

There is a change in MAC address corresponding to 192.168.51.1 from 0:50:8:3:87:93 to b4:b5:2f:8d:d1:a5.

There are further flip flops back to the correct MAC, and again to the spoofed MAC, as both the gateway and the intruder send ARP replies

```
Terminal -
File Edit View Terminal Tabs Help
Untitled x Untitled x Untitled x
Oct 27 15:09:44 akshay-inspiron5423 NetworkManager[565]: <info> [1603791584.9994] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:09:46 akshay-inspiron5423 arpwatch[2801]: flip flop 192.168.51.1 b4:b5:2f:8d:d1:a5 (0:50:8:3:87:93)
Oct 27 15:09:46 akshay-inspiron5423 arpwatch[2801]: reaper: pid 5767, exit status 78
Oct 27 15:09:48 akshay-inspiron5423 NetworkManager[565]: <info> [1603791588.9413] device (wlp7s0): supplicant interface state: inacti>
Oct 27 15:09:48 akshay-inspiron5423 NetworkManager[565]: <info> [1603791588.9414] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:09:49 akshay-inspiron5423 NetworkManager[565]: <info> [1603791589.9827] device (wlp7s0): supplicant interface state: scanni>
Oct 27 15:09:49 akshay-inspiron5423 NetworkManager[565]: <info> [1603791589.9828] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:09:51 akshay-inspiron5423 NetworkManager[565]: <info> [1603791591.9405] device (wlp7s0): supplicant interface state: inacti>
Oct 27 15:09:51 akshay-inspiron5423 NetworkManager[565]: <info> [1603791591.9405] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:09:52 akshay-inspiron5423 NetworkManager[565]: <info> [1603791592.9867] device (wlp7s0): supplicant interface state: scanni>
Oct 27 15:09:52 akshay-inspiron5423 NetworkManager[565]: <info> [1603791592.9867] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:09:53 akshay-inspiron5423 arpwatch[2801]: flip flop 192.168.51.1 0:50:8:3:87:93 (b4:b5:2f:8d:d1:a5)
Oct 27 15:09:53 akshay-inspiron5423 arpwatch[2801]: reaper: pid 5768, exit status 78
Oct 27 15:09:55 akshay-inspiron5423 NetworkManager[565]: <info> [1603791595.9399] device (wlp7s0): supplicant interface state: inacti>
Oct 27 15:09:55 akshay-inspiron5423 NetworkManager[565]: <info> [1603791595.9400] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:09:56 akshay-inspiron5423 NetworkManager[565]: <info> [1603791596.9911] device (wlp7s0): supplicant interface state: scanni>
Oct 27 15:09:56 akshay-inspiron5423 NetworkManager[565]: <info> [1603791596.9911] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:00 akshay-inspiron5423 arpwatch[2801]: flip flop 192.168.51.1 b4:b5:2f:8d:d1:a5 (0:50:8:3:87:93)
Oct 27 15:10:00 akshay-inspiron5423 arpwatch[2801]: reaper: pid 5771, exit status 78
Oct 27 15:10:01 akshay-inspiron5423 NetworkManager[565]: <info> [1603791601.9404] device (wlp7s0): supplicant interface state: inacti>
Oct 27 15:10:01 akshay-inspiron5423 NetworkManager[565]: <info> [1603791601.9404] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:02 akshay-inspiron5423 NetworkManager[565]: <info> [1603791602.9895] device (wlp7s0): supplicant interface state: scanni>
Oct 27 15:10:02 akshay-inspiron5423 NetworkManager[565]: <info> [1603791602.9896] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:05 akshay-inspiron5423 NetworkManager[565]: <info> [1603791605.9392] device (wlp7s0): supplicant interface state: inacti>
Oct 27 15:10:05 akshay-inspiron5423 NetworkManager[565]: <info> [1603791605.9392] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:06 akshay-inspiron5423 NetworkManager[565]: <info> [1603791606.9885] device (wlp7s0): supplicant interface state: scanni>
Oct 27 15:10:06 akshay-inspiron5423 NetworkManager[565]: <info> [1603791606.9885] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:11 akshay-inspiron5423 NetworkManager[565]: <info> [1603791611.9419] device (wlp7s0): supplicant interface state: inacti>
Oct 27 15:10:11 akshay-inspiron5423 NetworkManager[565]: <info> [1603791611.9419] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:12 akshay-inspiron5423 NetworkManager[565]: <info> [1603791612.9929] device (wlp7s0): supplicant interface state: scanni>
Oct 27 15:10:12 akshay-inspiron5423 NetworkManager[565]: <info> [1603791612.9930] device (p2p-dev-wlp7s0): supplicant management inte>
Oct 27 15:10:19 akshay-inspiron5423 NetworkManager[565]: <info> [1603791619.9417] device (wlp7s0): supplicant interface state: inacti>
lines 3082-3113
Add/Remov... Limit the siz... General (CB... CNS Lab Ass... 7_security_t... Fw: Garrett ... Terminal -
```

Figure 4: Flip flop message in the system message log

```
Terminal -
File Edit View Terminal Tabs Help
Untitled x Untitled x
old ethernet vendor: <unknown>
timestamp: Tuesday, October 27, 2020 15:13:10 +0530
previous timestamp: Tuesday, October 27, 2020 15:13:06 +0530
delta: 4 seconds

From: arpwatch
To: arpwatch
Subject: flip flop (ipcop.treknocom.local)

hostname: ipcop.treknocom.local
ip address: 192.168.51.1
ethernet address: 0:50:8:3:87:93
ethernet vendor: <unknown>
old ethernet address: b4:b5:2f:8d:d1:a5
old ethernet vendor: <unknown>
timestamp: Tuesday, October 27, 2020 15:13:51 +0530
previous timestamp: Tuesday, October 27, 2020 15:13:50 +0530
delta: 1 second

From: arpwatch
To: arpwatch
Subject: flip flop (ipcop.treknocom.local)

hostname: ipcop.treknocom.local
ip address: 192.168.51.1
ethernet address: b4:b5:2f:8d:d1:a5
ethernet vendor: <unknown>
old ethernet address: 0:50:8:3:87:93
old ethernet vendor: <unknown>
timestamp: Tuesday, October 27, 2020 15:14:00 +0530
previous timestamp: Tuesday, October 27, 2020 15:13:51 +0530
delta: 9 seconds
Add/Remov... Limit the ... General (... CNS Lab ... 7_securit... Fw: Garre... Terminal - Screenshot
```

Figure 5: More flip flop messages on stderr (these are email messages, printed on stderr due to -d option). One ARP broadcast answered by the true gateway, resulting in a flip flop to the true MAC address. However, the intruder keeps broadcasting ARP replies, and the next flip flop again shows the MAC for the gateway changing to the spoofed MAC address

Nessus

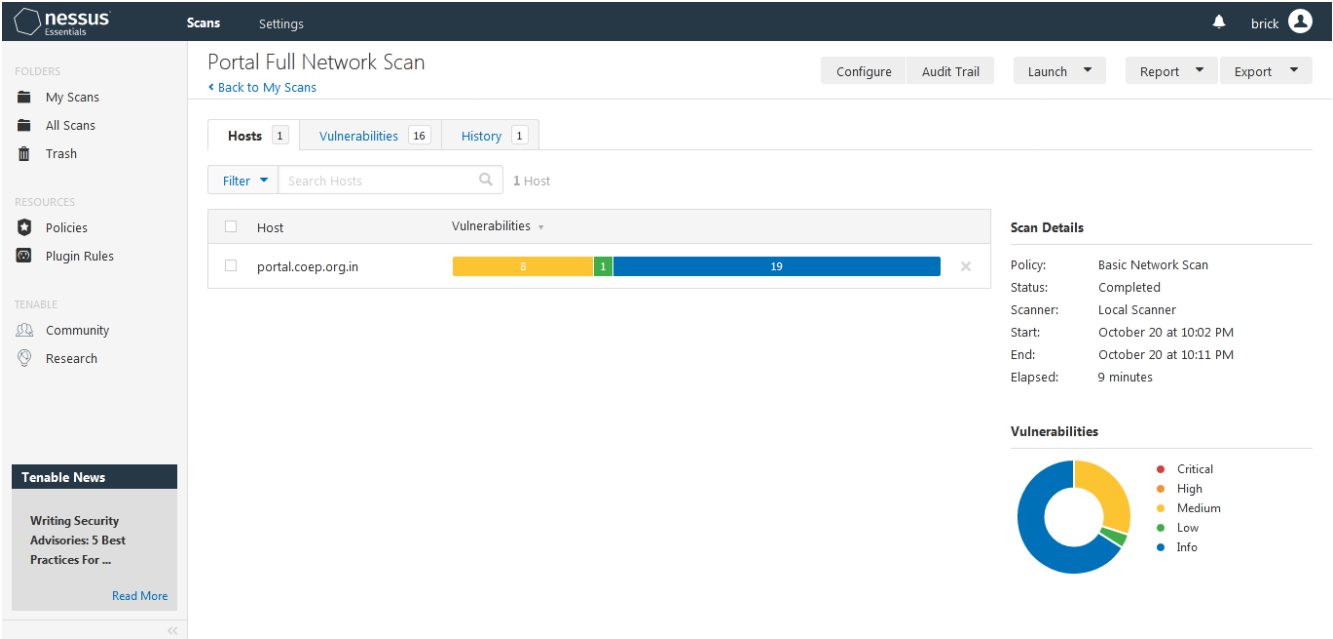


Figure 6: Overview of full network scan of portal.coep.org.in

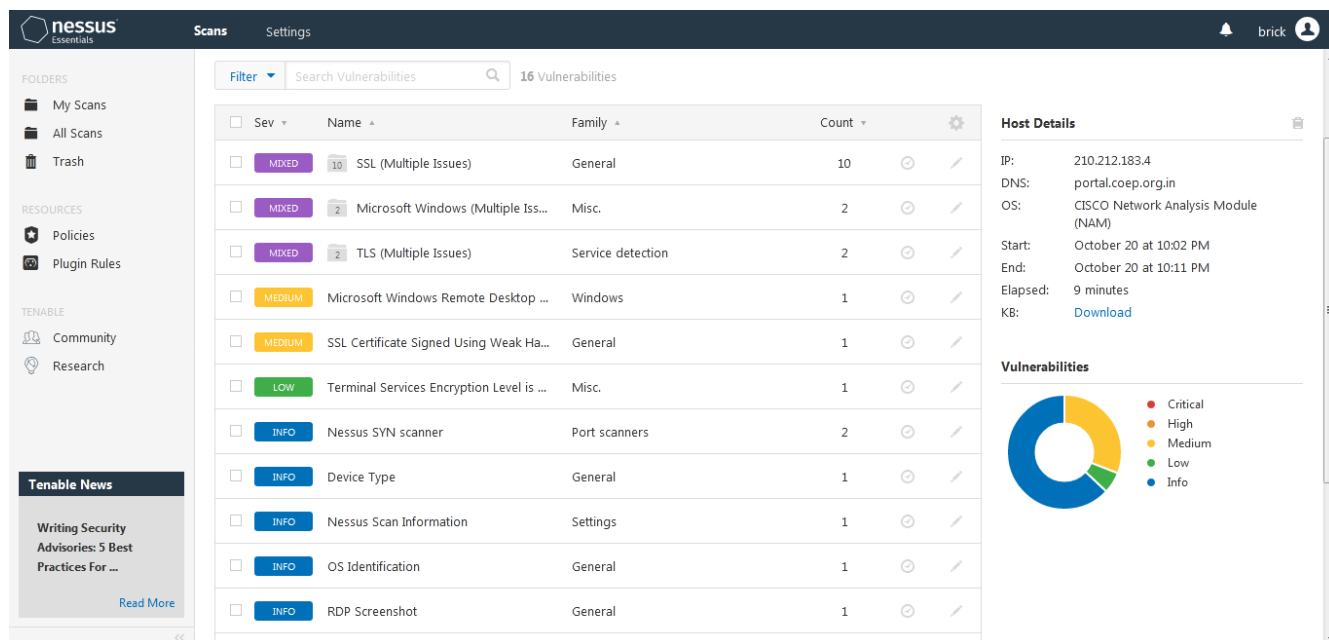


Figure 7: List of vulnerabilities found by Nessus in the IP which it scanned

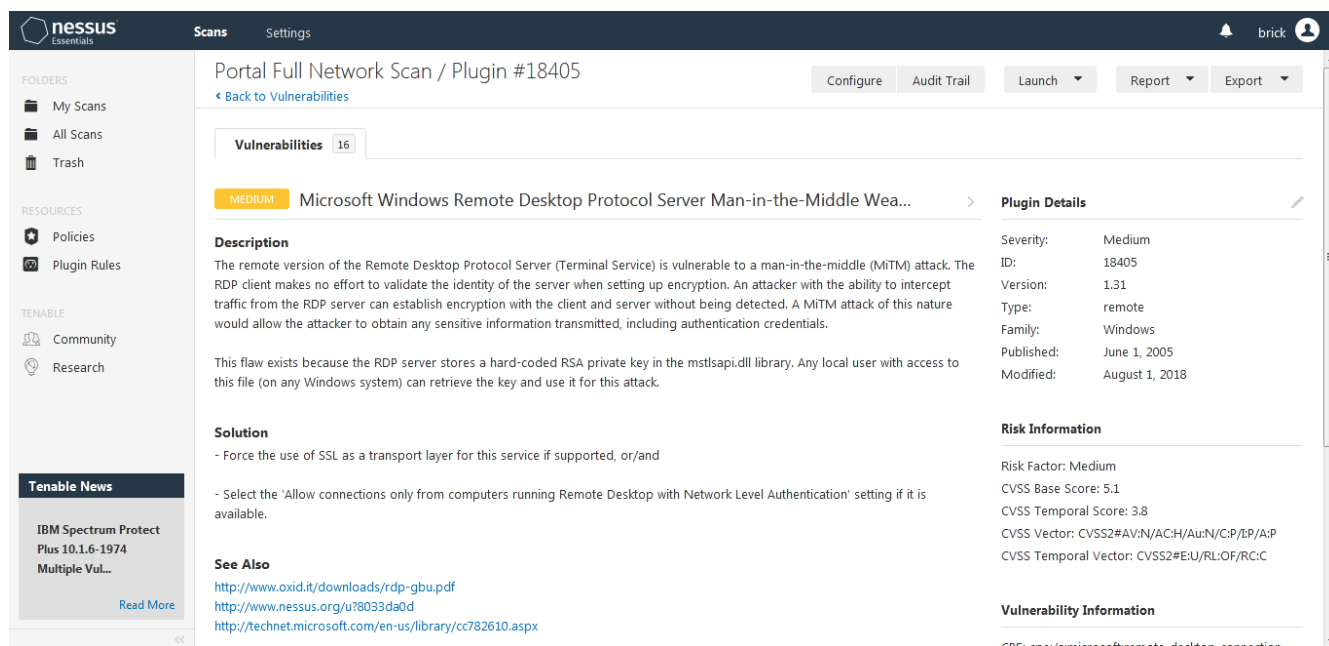


Figure 8: A microsoft remote desktop protocol man-in-the-middle vulnerability found by Nessus

Portal Full Network Scan

Tue, 20 Oct 2020 22:02:34 India Standard Time

TABLE OF CONTENTS

Hosts Executive Summary

- portal.coep.org.in

Hosts Executive Summary

[Collapse All](#) | [Expand All](#)

portal.coep.org.in

0	0	8	1	18
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	54615	Device Type
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	66173	RDP Screenshot
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	51891	SSL Session Resume Supported
INFO	N/A	22964	Service Detection
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	10940	Windows Terminal Services Enabled

[Hide](#)

Figure 9: The full executive summary report generated by Nessus