Vulnerability Assessment Report for NightLider Pte Ltd

Chong Yun Long / Consultant @*Pwned Consulting*

Contents

1 Security Assessment Agreement

Lider Corp has authorized *Pwned Consulting* to carry out a Vulnerability Assessment of its internal network systems. An agreement between both parties has been arranged where the purpose is the discovery of security vulnerabilities in its network systems.

1.1 Fees & Timing

All testing and assessment work will be performed solely on Client's company premises, Monday – Friday, 8 a.m. – 8 p.m. local time. Work required outside of these normal business hours will incur an upcharge, to be approved by customer in advance. Automated testing may be performed outside of this window if testing can be scheduled in advance.

Any additional work required beyond our current estimate will be added to our invoices at the agreed daily billing rate.

1.2 Disclaimer

Pwned Consulting and the Client have agreed to the following terms and conditions with regards to the vulnerability assessment services provided by *Pwned Consulting.*

1. Client understands that *Pwned Consulting* may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities.

2. Client authorises *Pwned Consulting* to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services or otherwise approved by Client from time to time) on network resources with the IP Addresses identified by Client

3. Client represents that, if Client does not own such network resources, it will have obtained consent and authorisation from the applicable third party, in form and substance satisfactory to *Pwned Consulting*, to permit *Pwned Consulting* to provide the Security Services.

4. The services offered, such as penetration testing or vulnerability assessments, may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom coded applications but will exclude intentional and deliberate Denial of Service Attacks.

5. Client acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the Client's systems and accepts those risks and consequences.

6. Client hereby consents and authorises Consultant to provide any or all the Security Services with respect to the Client's systems.

7. Client acknowledges it is the Client's responsibility to restore network computer systems to a secure configuration after Consultant testing.

2 Methodology

2.1 Tools used

As part of this security assessment, we have made use of the following tools:

Nmap – a free and open source utility for network discovery and security auditing. It can be used for network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Zenmap – Zenmap is the official Nmap Security Scanner GUI

Nessus Vulnerability Scanner – Vulnerability scanner is developed by Tenable Network Security[1]. It is able to scan for:

1. Vulnerabilities on a computer system
2. System misconfiguration
3. Default passwords
4. Denials of service using malformed packets
5. PCI DSS audits

2.2 Approach

The security assessment will consist of two components, Reconnaissance and Vulnerability Scanning.

1. Reconnaissance – Zenmap/Nmap will be used to visualize network topology as well as to fingerprint the systems that are on the network.
2. Vulnerability Scan –Nessus scanner will be used to identify and rank vulnerabilities of a target machine. Remediation measures/solutions will then be proposed to help better secure the system.

3 Reconnaissance

3.1 Topology

Lider Corp has provided us their network topology, as shown in Figure 1. They have requested that we focus our effort on `192.168.134.131`, a machine which has been targeted for attacks multiple times.

3.2 Network Scan

We conduct a network scan by running `nmap -T4 -A -v 192.168.134.128/24` in Zenmap, as shown in Figure 2. The flags used were:

T4 Equivalent to –max-rtt-timeout 1250ms –min-rtt-timeout 100ms –initial-rtt-timeout 500ms –max-retries 6 and sets the maximum TCP scan delay to 10 milliseconds

A Enable OS detection, version detection, script scanning, and traceroute

v Verbose output

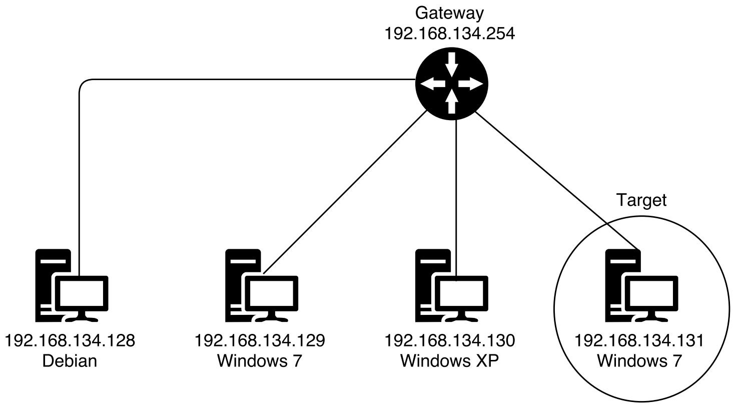
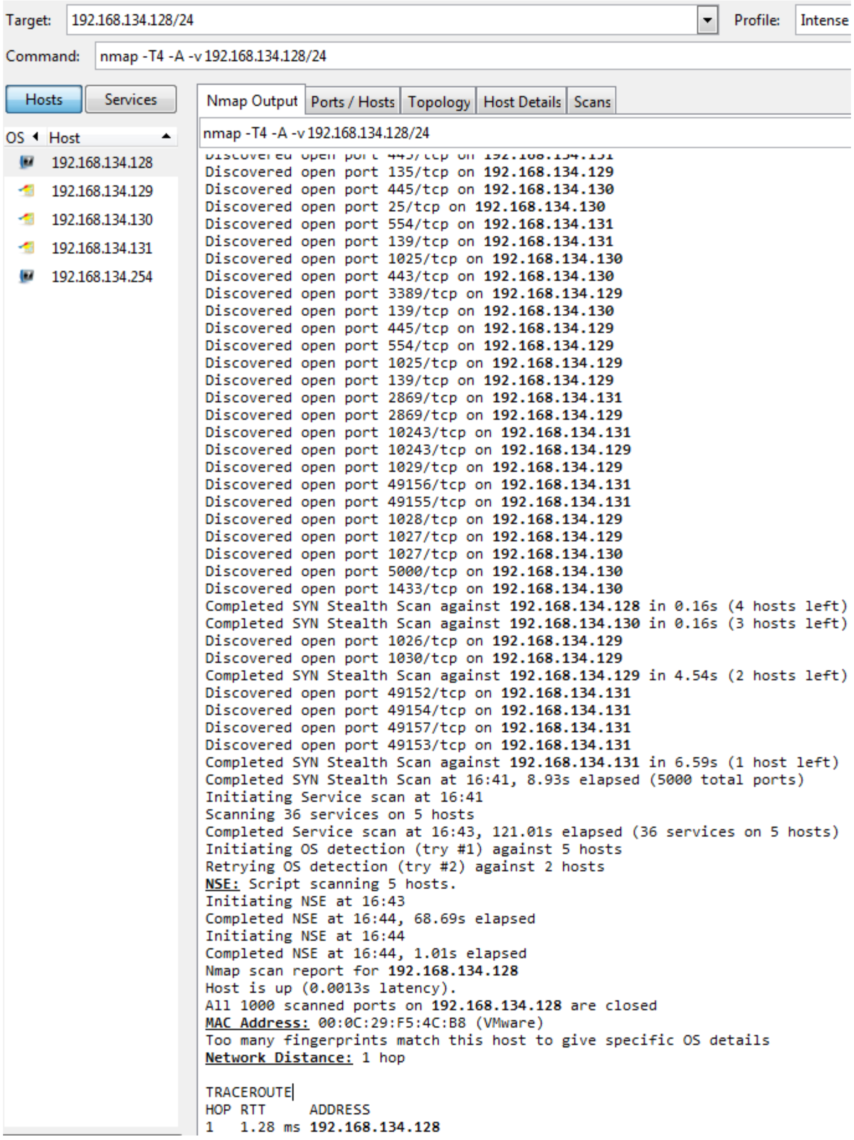


Figure 1: *Lider Corp*'s network topology



Target: 192.168.134.128/24

Profile: Intense

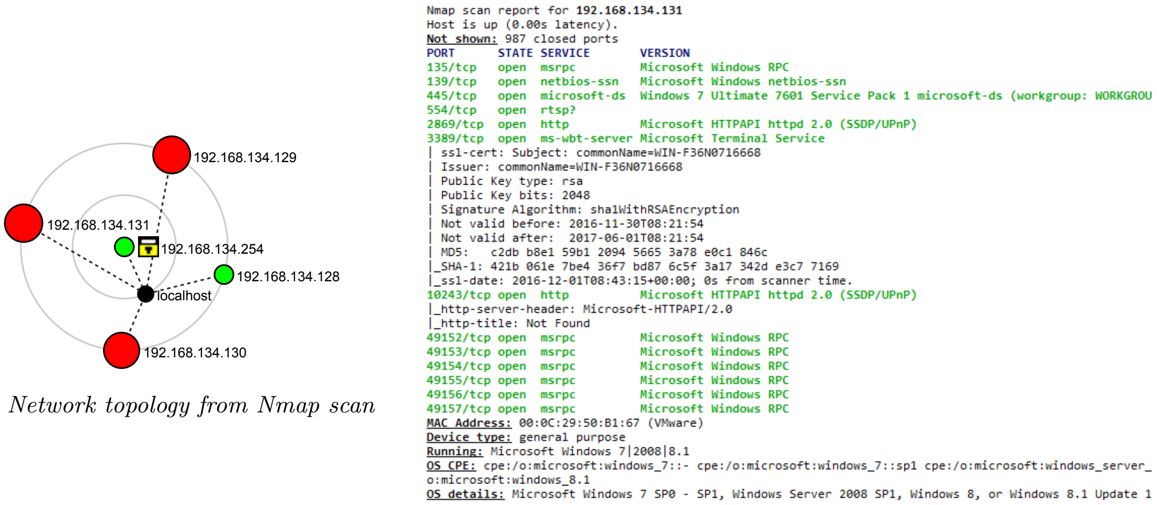
Command: nmap -T4 -A -v 192.168.134.128/24

192.168.134.128
192.168.134.129
192.168.134.130
192.168.134.131
192.168.134.254

```
nmap -T4 -A -v 192.168.134.128/24
Discovered open port 443/tcp on 192.168.134.131
Discovered open port 135/tcp on 192.168.134.129
Discovered open port 445/tcp on 192.168.134.130
Discovered open port 25/tcp on 192.168.134.130
Discovered open port 554/tcp on 192.168.134.131
Discovered open port 139/tcp on 192.168.134.131
Discovered open port 1025/tcp on 192.168.134.130
Discovered open port 443/tcp on 192.168.134.130
Discovered open port 3389/tcp on 192.168.134.129
Discovered open port 139/tcp on 192.168.134.130
Discovered open port 445/tcp on 192.168.134.129
Discovered open port 554/tcp on 192.168.134.129
Discovered open port 1025/tcp on 192.168.134.129
Discovered open port 139/tcp on 192.168.134.129
Discovered open port 2869/tcp on 192.168.134.131
Discovered open port 2869/tcp on 192.168.134.129
Discovered open port 10243/tcp on 192.168.134.131
Discovered open port 10243/tcp on 192.168.134.129
Discovered open port 1029/tcp on 192.168.134.129
Discovered open port 49156/tcp on 192.168.134.131
Discovered open port 49155/tcp on 192.168.134.131
Discovered open port 1028/tcp on 192.168.134.129
Discovered open port 1027/tcp on 192.168.134.129
Discovered open port 1027/tcp on 192.168.134.130
Discovered open port 5000/tcp on 192.168.134.130
Discovered open port 1433/tcp on 192.168.134.130
Completed SYN Stealth Scan against 192.168.134.128 in 0.16s (4 hosts left)
Completed SYN Stealth Scan against 192.168.134.130 in 0.16s (3 hosts left)
Discovered open port 1026/tcp on 192.168.134.129
Discovered open port 1030/tcp on 192.168.134.129
Completed SYN Stealth Scan against 192.168.134.129 in 4.54s (2 hosts left)
Discovered open port 49152/tcp on 192.168.134.131
Discovered open port 49154/tcp on 192.168.134.131
Discovered open port 49157/tcp on 192.168.134.131
Discovered open port 49153/tcp on 192.168.134.131
Completed SYN Stealth Scan against 192.168.134.131 in 6.59s (1 host left)
Completed SYN Stealth Scan at 16:41, 8.93s elapsed (5000 total ports)
Initiating Service scan at 16:41
Scanning 36 services on 5 hosts
Completed Service scan at 16:43, 121.01s elapsed (36 services on 5 hosts)
Initiating OS detection (try #1) against 5 hosts
Retrying OS detection (try #2) against 2 hosts
NSE: Script scanning 5 hosts.
Initiating NSE at 16:43
Completed NSE at 16:44, 68.69s elapsed
Initiating NSE at 16:44
Completed NSE at 16:44, 1.01s elapsed
Nmap scan report for 192.168.134.128
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.134.128 are closed
MAC Address: 00:0C:29:F5:4C:B8 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.28 ms 192.168.134.128
```

Figure 2: Zenmap/Nmap interface and command used

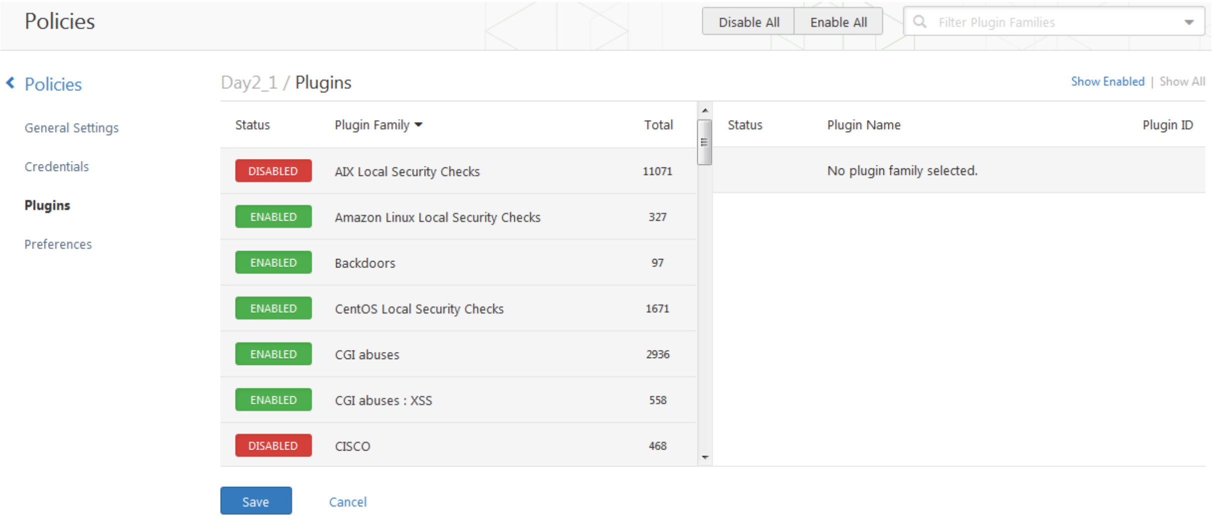


(a) *Network topology from Nmap scan*

```
Nmap scan report for 192.168.134.131
Host is up (0.00s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROU
554/tcp   open  rtsp?
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=WIN-F36N0716668
| Issuer: commonName=WIN-F36N0716668
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-11-30T08:21:54
| Not valid after:  2017-06-01T08:21:54
| MD5:   c2db b8e1 59b1 2094 5665 3a78 e0c1 846c
|_SHA-1: 421b 061e 7be4 36f7 bd87 6c5f 3a17 342d e3c7 7169
|_ssl-date: 2016-12-01T08:43:15+00:00; 0s from scanner time.
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:50:B1:67 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_
o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
```

(b) OS fingerprinting

Figure 3: Nmap results



Day2_1 / Plugins

Status	Plugin Family	Total
DISABLED	AIX Local Security Checks	11071
ENABLED	Amazon Linux Local Security Checks	327
ENABLED	Backdoors	97
ENABLED	CentOS Local Security Checks	1671
ENABLED	CGI abuses	2936
ENABLED	CGI abuses : XSS	558
DISABLED	CISCO	468

Status	Plugin Name	Plugin ID
	No plugin family selected.	

Figure 4: Disabling unnecessary Nessus plugins

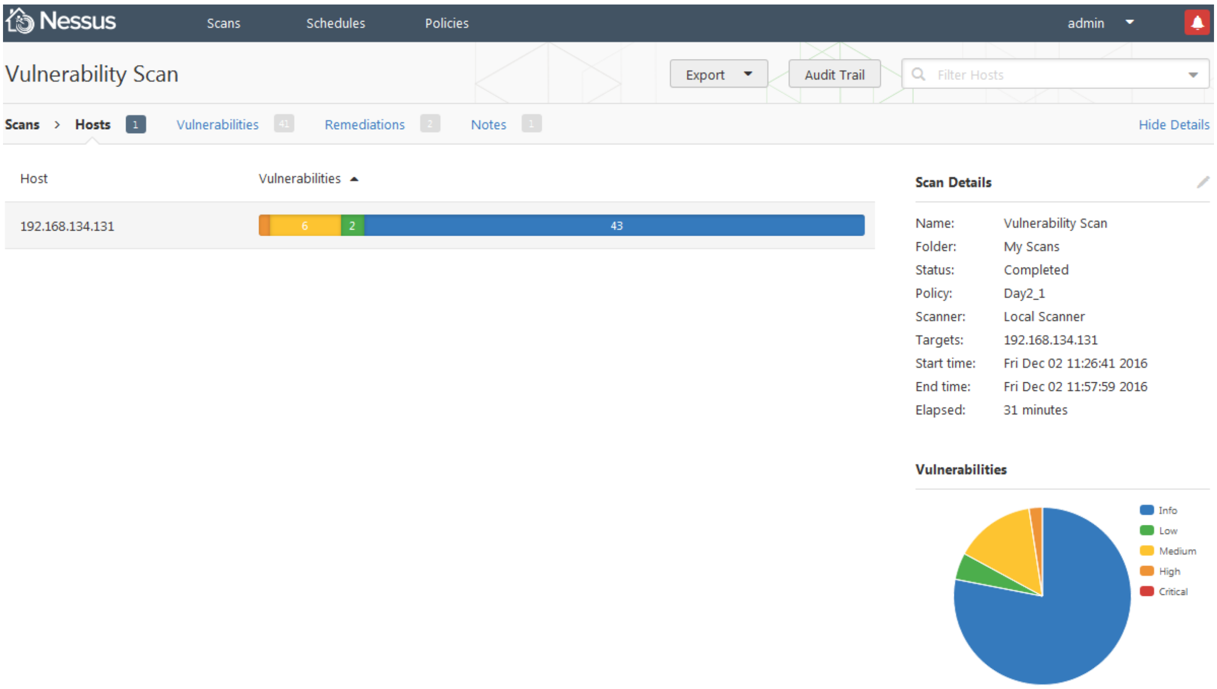
The results of our scan revealed a network topology (Figure 3a) that is similar to what was described to us by *Lider Corp*. We also know that the target (`192.168.134.131`) is likely Windows 7 machine from the Nmap results (Figure 3b)

4 Vulnerability Scan

With information about the network, the next step would be to make use of Nessus to scan our target for system vulnerabilities. Since the target machine is running Windows, we can decrease the scanning duration by disabling plugins which are not applicable for Windows. In Figure 4, AIX local security checks and CISCO plugins were disabled. There are many other unrelated plugins that we are able to disable to speed up the scanning process.

The Nessus scan on our target revealed 1 high, 6 medium and 2 low vulnerabilities (Figure 5). The

[1] http://www.tenable.com/



Host	Vulnerabilities
192.168.134.131	6 2 43

Scan Details

Name:	Vulnerability Scan
Folder:	My Scans
Status:	Completed
Policy:	Day2_1
Scanner:	Local Scanner
Targets:	192.168.134.131
Start time:	Fri Dec 02 11:26:41 2016
End time:	Fri Dec 02 11:57:59 2016
Elapsed:	31 minutes

Figure 5: Nessus scan results

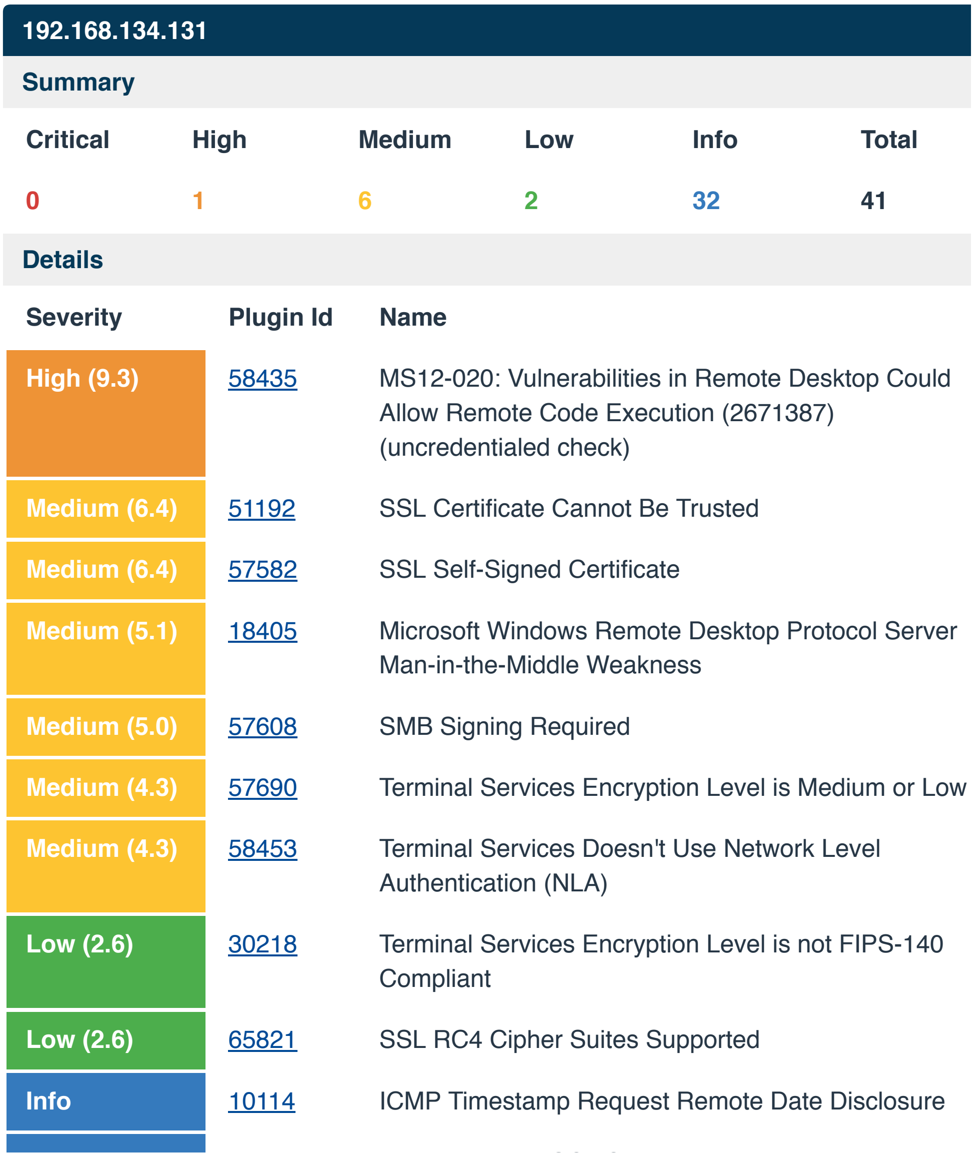
detailed Nessus report (Figure 6) revealed that the vulnerability lies in the implementation of Remote Desktop Protocol (RDP) on the Windows host (MS12-020). Attackers are able to send crafted RDP packets to the host and execute code remotely

4.1 Remediation

Microsoft has released a patch on its security bulletin(MS12-020) site[2].

This security update resolves two privately reported vulnerabilities in the Remote Desktop Protocol. The more severe of these vulnerabilities could allow remote code execution if an attacker sends a sequence of specially crafted RDP packets to an affected system. By default, the Remote Desktop Protocol (RDP) is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk. This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the subsection, Affected and Non-Affected Software, in this section. The security update addresses the vulnerabilities by modifying the way that the Remote Desktop Protocol processes packets in memory and the way that the RDP service processes packets. For more information about the vulnerabilities, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, Vulnerability Information. Recommendation. The majority of customers have automatic updating enabled and will not need to take any action because this security update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates and install this update manually. For information about specific configuration options in automatic updating, see Microsoft Knowledge Base Article 294871. For administrators and enterprise installations, or end users who want to install this security update manually, Microsoft recommends that customers apply the update immediately using update management software, or by checking for updates using the Microsoft Update service. See also the section, Detection and Deployment Tools and Guidance, later in this bulletin. Known Issues. Microsoft Knowledge Base Article 2671387 documents

[2] `https://technet.microsoft.com/en-us/library/security/ms12-020.aspx`



192.168.134.131

Summary

Critical	High	Medium	Low	Info	Total
0	1	6	2	32	41

Details

Severity	Plugin Id	Name
High (9.3)	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA)
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10114	ICMP Timestamp Request Remote Date Disclosure

Figure 6: Nessus indepth report

the currently known issues that customers may experience when installing this security update. The article also documents recommended solutions for these issues. Affected and Non-Affected Software The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

We recommend LiderCorp to apply the patch immediately to the affected system.

Remote Desktop is a huge attack surface for the Windows operating system. It is highly recommended to disable Remote Desktop on all Windows systems which do not require Remote Desktop functionalities.