CYBER SECURITY REPORT

By: Gary Bevans

Class: CSS 1005-0

Dated: December 3, 2018

Table of Contents:

Introduction

On November of the Fall 2018, I, Gary Bevans of *Students Security Solutions* (*SSS*) was hired to conduct a scan of the client's computer system. This test was performed with the use of different scanning tools, and was done both internally and externally, in order to facilitate the integrity of my results.

Based on the different tests performed and each with their unique results, the reader of this report can gain a basic understanding of different vulnerabilities that exist in a computer system. He/ she will also discover some things attackers can use to gain entry to a system (exploiting it for their malicious purposes), as well as some actions that can be taken to protect themselves or their organization from these threats.

As a result, this report will specifically identify weaknesses in the client's computer system, analyze the vulnerabilities, compare and contrast the internal scans with the external scans, and make recommendations to mitigate any risks found. Any personal information, such as the client's IP address, will be withheld as privilege data for this report.

Executive Summary

During November 2018, a comprehensive scan was performed on the client's computer system in order to detect and identify any weakness it had. The scope of the scan was to include a capture of the network traffic, identifying the availability of the system's ports, analyzing service running on the ports and to discover any other vulnerabilities that may exist.

Simply, WireShark was used to capture all network traffic and no unusual or unauthorized IPs or services were discovered when performing the tests. All authorized IPs and services were identified and no further testing were needed.

Nmap – Zenmap GUI was then activated and a thorough scan of the system's ports were performed. Each hosts and services were identified on the system and all ports were found to be appropriate to the system's usage. Results were recorded and no further testing was required.

However, the last test with the use of Nessus contained a few discrepancies. The internal and external scans held different results first of all. The internal Nessus scan was limiting, while the external scan contained what the internal had plus a few more risks. These risks were vulnerabilities in the system, which were recognized with possible reasons for why they existed.

Recommendations were then made of all risk found in the client's system and was concluded with a short security resolution.

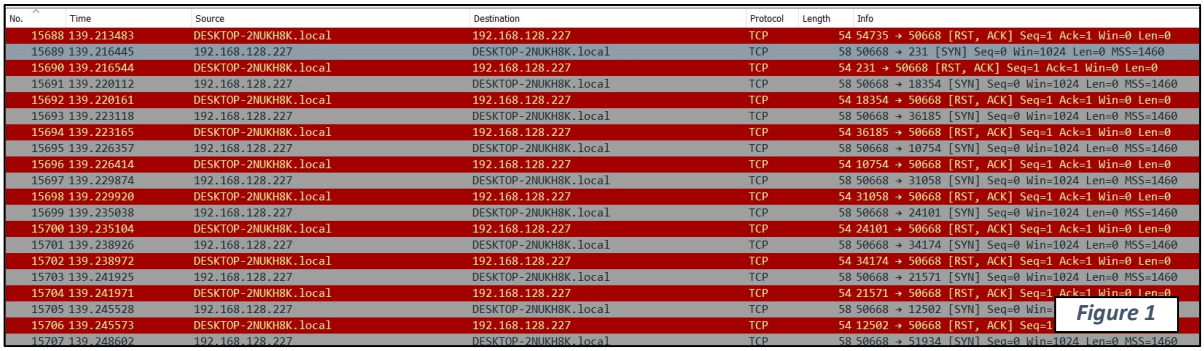
Tools Used

- WireShark
- Nmap – Zenmap GUI
- Nessus Professional

WireShark Analysis and Results

WireShark is a packet analyzer which is used to view and capture the network traffic of a system. It can illustrate the number of events, the time-base on the event, the source address of the packet, the destination address of the packet, what protocol it is using, the length of the packet (bytes) and more information regarding the activity of the processes.

As seen in *Figure 1* (below), is a brief illustration of a WireShark capture, which was used while conducting tests of the computer system. WireShark was used so that I could validate the source my external scan, that it was secured and being performed by one of my authorized



No.	Time	Source	Destination	Protocol	Length	Info
15688	139.213483	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	54735 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15689	139.216445	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 231 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15690	139.216544	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	231 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15691	139.220112	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 18354 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15692	139.220161	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	18354 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15693	139.223118	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 36185 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15694	139.223165	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	36185 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15695	139.226357	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 10754 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15696	139.226414	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	10754 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15697	139.229874	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 31058 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15698	139.229920	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	31058 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15699	139.235038	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 24101 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15700	139.235104	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	24101 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15701	139.238926	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 34174 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15702	139.238972	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	34174 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15703	139.241925	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 21571 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15704	139.241971	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	21571 → 50668 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15705	139.245528	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 12502 [SYN] Seq=0 Win=
15706	139.245573	DESKTOP-2NUKH8K.local	192.168.128.227	TCP	54	12502 → 50668 [RST, ACK] Seq=1
15707	139.248602	192.168.128.227	DESKTOP-2NUKH8K.local	TCP	58	50668 → 51934 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 1

computers, and not being compromised in any way. WireShark was also used to monitor all traffic on the system from any suspicious sources and activities.

During the tests, authorized IPs were recognized and no discrepancies were identified during the the length of my work. Network traffic was secure and safe and coincides with the external capture; no further testing needed.

Nmap – Zenmap GUI Analysis and Results

Zenmap is a GUI for Nmap, which is a tool used for security scanning. The Zenmap's scans are concentrated to discover the hosts and services on a computer network. Essentially, with all this information, Nmap builds a map of the network.

The objective of using Nmap in the tests was to validate the services as well as to identify TCP and UDP ports opened in the system. With certain services and ports open, hackers and other attackers can gain entry into the system, perform randomwares, violate security protocols (such as seeing and attaining confidential data), or just being desturctive and perform denial of service (DOS) or distributed denial of service (DDOS) attacks on the client's system or with the use of the system.

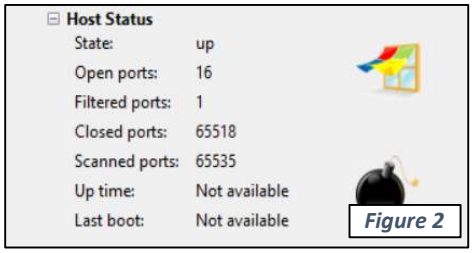


Figure 2

As seen in *Figure 2* (on the left), Nmap scanned the ports on the computer system (65535 in total) and identified their status, which were either open, closed or filtered (firewall, filter or network obstacle that blocks the port exists).

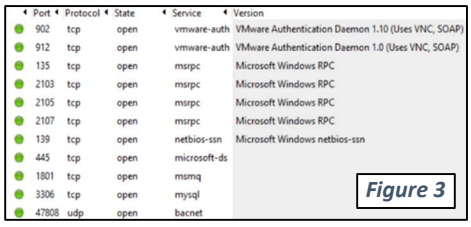


Figure 3

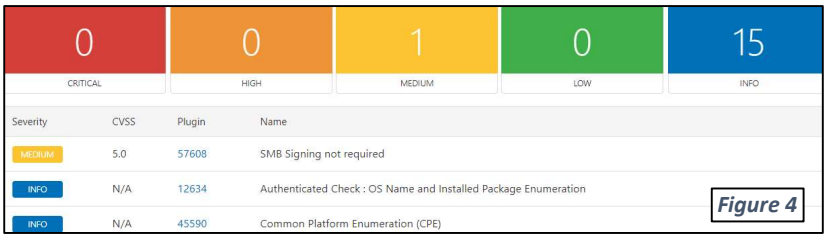
Navigating through the tabs, Nmap breaks down the details of the results, illustrating what ports was found, what protocol it is using, what is the state of the port, what services is using that port, as well as details of what specific programs might be using it; *Figure 3* (on the left) is a good representation of this.

Results were cross-referenced between the internal and external scans, with no descrepancies identified. No irregular ports were identified to be opened, or any suspicioius service identified for using any ports. However, this does not mean that an attack cannot happen. If a program becomes outdated and has not been updated to the latest patch, vulnerabilites can exist in them for attackers to exploit by gaining backdoor entry to the system (through these cracks), in which to conduct their malicious activities. Subsequently, new patches can also retain vulerabilities (such as bugs, glitches, or backdoors) which can also be used by attackers, which exist due to the product being new and not tested sufficiently or throughroughly to anticipate every scenarios.

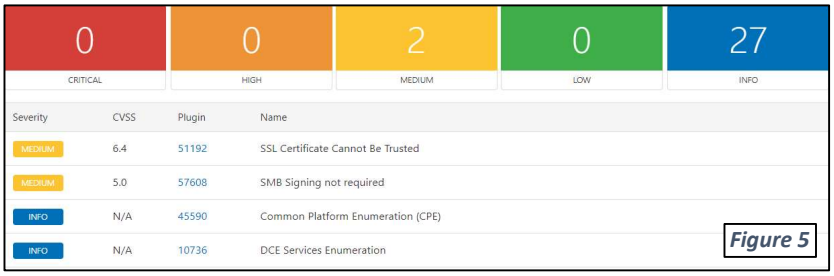
Nessus Analysis and Results

Nessus Professional is a version of the Nessus software product developed by Tenable, which is used for scanning vulnerabilities in a system. Vulnerabilities are classified into five different categories, ranking from worst to least as : Critical (red), High (orange), Medium (yellow), Low (green) and Info (Blue). After a scan is selected and performed, the results can be accessed, saved on the cloud or even exported to generate a report. Although the report generates a qualitative measurement for the severity of any vulnerabilities, it is also quantified based on the CVSS or Common Vulnerability Scoring System in order to measure the risk appropriately.

After I conducted my Nessus testing, I identified some differences between the external and internal scans. The internal scan, as seen in *Figure 4* (below), identified a set number of risks; 1 Medium and 15 Info based level risks.



The external scan, as seen in *Figure 5* (below), found the exact same risks as the internal, but also found a few more additional risks; making it now 2 Medium and 27 Info based level risks.



This is exactly, why both an internal and external scan of the system is performed in these tests. Whether each computer could be the same or different, they each have a different outlook on things or you can say computers have differences in perspective internally and externally. Internally is what we see as users. Externally is what attackers possibly see. This is why it is important to see results from all perspectives.

As a result, after comparing the results, *Figure 5* – the external scan contains all results from the internal (*Figure 4*), plus it has a few additional risks; therefore, the external scan will be used to assess the system we are working with. As seen in the illustrations above, the 2 main issues in the system is the SSL Certificate and the SMB Signing Issues.

The ‘SSL Certificate Cannot Be Trusted’ refers to the server's X.509 certificate, which cannot be trusted. That issue exists because the chain of trust was broken due to one of the three ways. The first way is when the top of the certificate chain sent by the server might not be descended from a known public certificate authority. The second way is because the certificate chain may contain a certificate that is not valid at the time of the scan. Thirdly, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. “*If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host*” – (Plugins.” Tenable™. 2018).

The ‘SMB Signing not required’ issue is simply as the name states, which is that no signing is required for the remote SMB server. This is bad because with no signing-in required, if an attacker finds out this vulnerability then can exploit it to perform a man-on-the-middle attack against the SMB server.

Recommendations

The following is based on the vulnerabilities that were identified through the various scanning and tests.

- SSL Certificate cannot trusted – in order to resolve this issue a proper certificate for the service must be generated. If this cannot occur, then one must be purchased.

- SMB Signing not required – to address this, a message signing in must be enforced in the host configuration. For Windows, this can be found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. For Samba, the setting is called 'server signing’.

Conclusion

On November 2018 tests were conducted on the client’s computer system. Testing were done both internally and externally to validate and ensure integrity of our results. Through thorough scanning, data was gathered from identified risks in the system, and an assessment was made. After analyzing the data, a risk mitigation plan was made to provide recommendations to the client on what was needed in order to resolve the issues. As a result, this report identified weaknesses in the client’s computer system, analyzed the vulnerabilities, compared and contrasted internal and external scans, and made recommendations to mitigate the risks.

Although recommendations were made, always remember to ensure safe usage of the system. Update applications as needed, report any bugs or glitches, ensure proper network security at times and ensure signing in to the system and services, whether local or online.

References

"Plugins." Tenable™. 2018. Retrieved from https://www.tenable.com/plugins.

Additional Images

- **Image of a PORT SCAN, via Nmap, illistrating what services utilizing the ports:**

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912	tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306	tcp	open	mysql	
137	tcp	filtered	netbios-ns	
5040	tcp	open	unknown	
8834	tcp	open	http	NessusWWW 6.7 - 6.9
33060	tcp	open	mysqlx	
38068	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664	tcp	open	msrpc	Microsoft Windows RPC
49665	tcp	open	msrpc	Microsoft Windows RPC
49666	tcp	open	msrpc	Microsoft Windows RPC
49667	tcp	open	msrpc	Microsoft Windows RPC
49669	tcp	open	msrpc	Microsoft Windows RPC
49673	tcp	open	msrpc	Microsoft Windows RPC