Mengxue Ni, Mengqi He
MIS 5211.001
Analysis Report 2: Scanning Exercise
10/26/2016

Nessus Vulnerability Scanning

Overview

For this assignment, we conducted Nessus vulnerability scans on two computers: a Macbook Air and a HP laptop. The Macbook Air was bought in 2012 and was not used often. Its OS was OS X 10.9.1 and not updated for a long time. On the other hand, the HP was bought half year ago for daily use. Its OS was Windows 10. To find out what differences are between the vulnerabilities of these two computers with different systems in different conditions, we compared the scan results, and found that there are 88 vulnerabilities in the Macbook Air, only two in the HP.

Macbook Air

Scan Results

We had an advanced scan with default setting on the Macbook Air. The scan took five minutes to complete and uncovered 88 vulnerabilities: 13 critical, 64 high, 10 medium and 1 low (see details in chart below).

Level of vulnerabilities	Descriptions	Number of vulnerabilities
Critical	Vulnerabilities due to low version of OS	9
	Vulnerabilities due to low version of Adobe Photoshop	2
	Mozilla foundation unsupported application detection	1
	GNU bash local environment variable handling command injection	1
High	Vulnerabilities due to low version of OS	1
	Vulnerabilities due to low version of FireFox	26
	Vulnerabilities due to low version of Apple Safari	16
	Vulnerabilities in Microsoft Office allow remote code execution (lack security updates)	20
	NTP security update	1
Medium	Vulnerabilities due to low version of Apple Safari	4
	Vulnerabilities due to low version of Firefox	4
	Vulnerabilities due to low version of iTunes	1
	SSL Certificate Cannot Be Trusted	1
Low	Vulnerabilities due to low version of iTunes	1

From the chart above, we found out that most of vulnerabilities are due to low version of operating system and applications. Among them, 10 vulnerabilities are due to low version of OS, 30 for Firefox, 20 for Safari, 20 for Microsoft Office and 2 for Adobe and iTunes. The latest version of Mac OS is Mac OS X 10.11, but the running version is 10.9.1 released at the end of 2013. The system updates contain several security-related fixes for components such as OpenSSL, bluetooth, IOKit and CoreGraphics. Without the updates, the OS will be vulnerable to "new" virus or malware developed after the last system update. In addition, the latest available version of Firefox is 44.0.2, but the version on the host is 28.0 which was launched back to early 2014. The low version will lead to a security bypass vulnerability due to improper restriction of interaction between service workers and plugins. Therefore, an authenticated, remote attacker can exploit this. Flaws, overflow and underflow conditions, and use-after-free errors also exist due to lack of updates containing patches and fixes. More than that, the latest available version of Apple Safari is 7.1.8, while the running version is 7.0.1 released in December 2013. Therefore, it may cause multiple memory corruption flaws, and security policy bypass and information disclosure vulnerabilities existing in Webkit. Moreover, current version of Microsoft Office is 2011 14.3.9, but the lack of necessary patches may result in a remote code execution vulnerability due to improper handling of RTF files. An unauthenticated, remote attacker can exploit this by convincing a user to open a specially crafted Office file, resulting in the execution of arbitrary code in the context of the current user. Like other applications, current Adobe Photoshop version is 14.0 released in June 2013, while the newest version is CC2015 16.0. This would lead to unspecified memory corruption laws and integer overflow flaws, and thus an attacker can exploit that to execute arbitrary code. iTunes version is also outdated. The newest version is 12.5.1, while the running version is 11.1 released in January 2014. Due to this, an insecure permission vulnerability may exist and this could allow a local attacker to manipulate the contents or gain escalated privileges. Another important medium-risky vulnerability except the results of low versions is that SSL certificate cannot be trusted. The server's X.509 certificate does not have a signature from a known public certificate authority.

According to the analysis, we found that the last upgrades and updates of most applications are at the end of 2013 or in early 2014. This is because the pre-owner rarely used the Mac since 2014, and it was given to the current owner as a gift at the end of 2015. The current owner started frequently using it from the beginning of this year, but she didn't upgrade the system and applications, and not realize that there are so many vulnerabilities existing on the computer.

Suggested Solutions

- Upgrade OS to Mac OS X 10.11
- Upgrade Firefox to version 44.0.2
- Upgrade Apple Safari to version 7.1.8
- Update and install patches for Microsoft Office 2011
- Upgrade Adobe Photoshop to version CC 2015 16.0
- Upgrade iTunes to version 12.5.1
- Install the vendor-supplied security patch to APPLE-SA-2014-12-22-1
- Purchase or generate a proper certificate for the service

Re-scan Results

Since most the vulnerabilities can be solved easily through upgrading or installing patches, we suggested the owner to follow the suggested solutions to avoid potential risks related to those vulnerabilities. After doing as we suggested, the owner allowed us to have another scan to check if the computer was optimized through upgrading and if vulnerabilities above are solved. The re-scan result was that the vulnerabilities reduced to only 1! The only remaining vulnerability is that SSL certificate cannot be trusted in medium level.

HP Windows 10

Scan Result:

Level of vulnerabilities	Descriptions	Number of vulnerabilities
Medium	SMB Signing Disabled	1
	SSL Certificate Cannot Be Trusted	1
Info	Netstat portscanner (SSH)	182
	MSRPC Service Detection	6
	Microsoft Windows SMB Service detection	5
	VMware ESX/GSX Server detection	2

Suggested Solutions

SMB Signing Disabled: signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. SMB signing is a security mechanism in the SMB protocol and is also known as security signatures. SMB signing is designed to help improve the security of the SMB protocol. SMB signing was first available in Microsoft Windows NT 4.0 Service Pack 3 (SP3) and Microsoft Windows 98.

Suggested 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'

SSL Certificate Cannot Be Trusted : The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This

can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

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.

Suggested solution: Purchase or generate a proper certificate for this service

I didn't list out all the info that Nessus scanned because info can be consider as very low risks. Also, there are 218 info that Nessus wanted me to check. But I do look into the first info-Netstat portscanner (SSH). This plugin runs 'netstat' on the remote machine to enumerate open ports. There are 182 ports are found to be open on the HP Windows 10 computer. Netstat is a command-line network utility tool that displays network connections for the Transmission Control Protocol, routing tables and a number of network interface and network protocol statistics. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

Conclusion

For the Macbook Air which was bought in 2012 and was not used frequently. It contains 13 critical, 64 high, 10 medium and 1 low vulnerabilities. It indicates that computers that are used before but abandoned years later are exposed to high risks. If a hacker want to get your personal information, this kind of computers are the best targets. Updating softwares and systems is very important in order to protect your own information. Or you can delete all the information once you decide not to use the computer anymore. On the other hand, the HP Windows 10 computer was bought only half year and used daily. Nessus showed it only contained 2 median vulnerabilities. One requires to enable SMB signing, another requires to purchases or generate a proper certificate. Daily used computers are not easy to be hacked, but still they have vulnerabilities. Scanning should be conducted regularly. Keep updating systems and softwares is necessary as well.