Is my Network Secure?

ITCN 6823

Vinay Sawant

Abstract

Is my network secure? This would be the most common and important question every Network and Information Security administrator, Network and Information Security Manager, and Chief Information Security Officer (CISO) will have. This research paper discusses about various Computers and Networking related security threats and vulnerabilities in enterprise network. We also discuss about traditional security threats, latest security threats and makes a list of all the security related threats and discuss suggested mitigation methods. A detailed analysis of network security appliances, software, and management products will be presented so that reader can choose best solution for their network. Some common security implementation mistakes are also analyzed in this paper. Finally, we are discussing about network security audits and importance of up to date security patches.

Introduction

With increasing cyber-attacks happening everyday all over the world, information security department plays key role in protecting company's data. Attackers are using advanced techniques every time they come up with cyber-attack or virus attack or try to steal company data or disrupt company using open vulnerabilities. With advancement of technologies, web-based applications and cloud computing, every enterprise will have to interact more and more on the public internet and that increases the risk of external attacks. With that said, Network Security department's job becomes more critical and they need to keep themselves up-to date with latest security threats, vulnerabilities, malware and viruses. As we go more and more towards digitization, and with the new upcoming Internet of things (IoT) model, network traffic, web traffic is growing at very rapid speed which effectively increases the chances of cyber-attacks and security related threats. Advanced persistent threats are more concerning to Security Managers. Attackers get access to our systems or network via malware or social engineering. Attackers then try to get access to shell prompt of our system and verify and access the network mapped drive, then they initiate port scan of victim system. After that attackers will identify available open ports running on other systems and get information about the network segments. There are various ways we can protect our information security. It is very important to choose the solution that best suits your network.

Traditional Security Threats

Following is the list of more traditional security threats to hosts (Servers, pc/laptops) and network appliances. In general, when you are thinking about is my network secure, you need to address following traditional threats and attacks to begin with.

1. Malware: Malware is a type of Malicious software which can has following different types. [Admin, 2018]

a. Viruses: There are special programs that can run on your computer and affect performance of other applications of operating system and make your memory and CPU utilization high and make system behave unexpectedly.

b. Adware: There are the advertisement pop up which we see on our computers. These software tracks out internet browsing and will show us advertises.

c. Spyware: These types of malicious software will get install in our computers and will spy on out internet activities.

d. Worms: These software codes can delete our files.

e. Trojan: These software code can pretend they are safe to run and can steal important data on our computers.

2. Denial of Service (DOS) attacks: In this type of attacks, the attacker makes the end system busy by utilizing the resources on that host and ultimately the host stops responding to legit requests.
3. Malicious HTML email: In this type of attack am email will be sent to users and it may contain some fancy heading or some fake interesting news which may trigger user to click on it and that link will be linked to some malicious website.
4. Attacking the networking appliances, or servers using known vulnerabilities. Attackers uses known vulnerabilities to access or exploit the network devices or servers. One example vulnerability is HP Server access over ILO connection. Some of the old Firmware on HP ILO server were vulnerable attackers could use that vulnerability to access the server. HP has released patches for that vulnerability. [HPE Support Center, 2017]

5. Phishing: Phishing are programs or emails that trick users to provide sensitive information by sending some mails or anything similar methods which looks legitimate. Once the attacker gets required info they can gain access to computers network.
6. Rootkit: It is basically set of software that allows hacker to gain access to system application and then it can modify it. They can go undetected. First the attacker will get access to our system and then use the rootkit to modify/alter applications.
7. Keylogger: These are programs that once got installed on our pc, it basically capture the keystrokes. These are mainly used for stealing credentials.
8. Spoofing: As the name suggest the man in middle can hack the emails and alter it in such a way that it may look like it is coming from a person known to you.
9. Man-In-Middle Attack: In this type of attacks the hacker will intercept the flow/communication/data along the path and modify it. This includes email hijacking, Wi-Fi Eavesdropping, session hacking.
10. Dropper: It's a type of program that gets install in our system and then install virus in our system. Dropper itself is not a virus. It is something that install virus in
11. Spams: We know these are the unwanted email we get. They pose a high risk if they are not handled carefully.

Latest Security Threads

WPA2: Wi-Fi Protected Accesses, which was so for known as most secure wireless security protocol was found as vulnerable to directory attack. [Agbeboaye, Akpojedje, Okoekhian, 2018]. For now, security patches are available for AP vendors to make it secure.

Ransomware: These are latest type of malwares. In this type of attack the attacker will take control of our system and will lock it and they will ask ransom money to release the control. In some cases, they even don't give the control back even after paying the money. As per the report from Kaspersky lab, the people who paid ransom to get their files, 20% of them did not get their files decrypted. [Furnell, Emm, 2017] Example of Ransomware: Wanna Cry which we saw in 2017.

Meltdown and Spectre: In these two vulnerabilities, attacker can get access to processor and get access to critical data which currently being processes on the computer. According to Nigel Houlden, head of technology policy at the Information Commissioner's office, “"In essence, the vulnerabilities provide ways that an attacker could extract information from privileged memory locations that should be inaccessible and secure." [Treharne, 2018]. Meltdown basically eliminate the wall between operating system and application software. This allows the attacker to access the memory and which can give access to secrets or passwords. [Lipp, Schwarz, Gruss, Prescher, Haas , Mangard , Kocher , Genkin , Yarom , Hamburg (2018). Spectre breaks the wall between two different applications. It tricks the application software to leak the secrets. [Kocher, Genkin, Gruss, Haas, Hamburg, Lipp, Mangard, Prescher, Schwarz, Yarom 2018]

Protecting your network

Network Security Monitoring

Colin Tankard in his Journal article (Advanced Persistent threat [APT] and how to monitor and deter them) mentioned how to deal with Advanced Persistent Threat. As per him to control APT, organizations should understand and study their data and data pattern. They suggest, for in detailed multiple network monitoring, measure are required like proper log configuration and log analysis from firewall, Intrusion Prehension System (IPS), Network Intrusion Detection System (NIDS), file integrity checking, rootkit detection and registry monitoring. He suggested organization should mark baseline and then compare them periodically. He mentioned many vendors offers logs monitoring and can generate ticket based on those logs and can make it automated. This will make detecting abnormal behavior and take automated corrective action like shutting down port and open network security incidents. [Tankard, 2011]. Another important factor which plays important role in monitoring network security for cyberattacks is how quickly you identify the alerts, and how much time you take act on it and address it. There are various factors which play role in this, such as how many alerts are received each day and how many security analysts are available to analyze them. [Shah, Ganesan, Jagodia, Cam, 2017]. If you are using Software Defined Networking (SDN) technology in your network then that technology programmable features which brings new challenges. For those type of technology Machine Learning approach is used in the SDN based Network Intrusion Prevention Systems [NPIS] (Sultana, Chilamkurti, Rabei Alhadad, 2018)

Antivirus Software

As we all know antivirus software plays important role in protecting our laptops, servers, and any other internal hosts machines. Keeping antivirus software definition updated is very important task and it is now a day an automated process. The antivirus client machines can either directly reach out to web-based antivirus server or in case of some company they download the latest update file every day and then they distribute to local client machines. Since every day new viruses are discovered, the antivirus software company should be efficient enough to keep adding fix for all known virus. One important precaution we need to take is how we configure Virus security scan. There is incident reported about virus security scan consuming heavy network resources and utilizing network bandwidth and leaving very limited bandwidth for other critical data and voice application causing big network outages and huge impact. Antivirus software generally use behavior-based detection and signature-based detection. In signature-based detection the antivirus software will already know the virus, it will scan for known code signature to detect the virus. Behavior based detection will dynamically analyze how a particular code is executed and behaving and then will mark that peace of code as suspected anomaly. [Sukwong, Kim, Jame, Joe 2011]

Firewalls

Firewall act as first level of protection for our network so it becomes very important to make sure the firewall is configured properly, no error made with policy. Since firewalls are at the edge of the network, it is highly possible that they can become victim of DoS attack. There are many tools available in the market to detect such misconfiguration and report them to security managers or security administrator. One of such model was studied by Salah, Elbadawi and Boutaba. They presented an analytical model to study and analyze the performance of firewall which are rule based. For their study they derived performance measure and key feature. These features include packet loss, throughput, CPU utilization and delay. Their module can be used to evaluate the performance of the firewall during normal packet flow and during any type of DoS attack. As per their analysis, if the rule set are too large, then the rules at the bottom of the list shows decremental performance. As a performance measure and counter measure from DoS, it is recommended to reduce down the rule or rearrange them. [Salah, Elbadawi and Boutaba, 2012]

Network Security Monitoring Centers

Various modern tools are available which can provide centralized management of Firewalls, Security applications, URL filtering, Advanced Malware protection, and IPS (Intrusion Prevention System). Cisco's Solution for this is Firepower. Cisco Firepower solution can centrally manage Firewalls, IPS, Advanced Malware protection. It has total visibility to our network including users, hosts, files, applications, Virtual environment threats, mobile devices, vulnerabilities that present in our network. It can perform real time threat management. It can defend against known threats, controls network access. One of the most important question every network security manager will have is how to effectively manage from unknown viruses. Firepower uses sandboxing and advanced Malware (AMP) to take care if this problem.

Intrusion Detection System (IDS)

The main function of Intrusion Detection System (IDS) is to monitor the traffic which is passing through and detect malicious activities and generate alert. Some advanced IDS can take action on the detected anomaly. It is very important to configure the IDS properly fine tune it to detect malicious traffic or else it can generate false alarm. There are different types of IDS based on where they are placed in the network and based on how they function. The IDS which are placed close to network entry point for external traffic are called as Network IDS(NDIS). They are strategically placed at network boundary to monitor thread coming from external sources. The IDS which run on every host inside the network are called as Host IDS (HIDS) and their main function is to detect malicious activity generated by internal hosts. Another type is signature-based IDS they mainly look for known signatures to detect the abnormal traffic pattern. They are more like Antivirus Software. The fourth category is abnormally based. These types of IDS detect abnormal traffic behavior based on established baseline. [Margaret 2018]

Intrusion Prevention System (IPS)

The unction is Intrusion Prevention (IPS) is they not only monitor the traffic for abnormal behavior but also, they can take action to stop that traffic and block the potential problematic flow. Proper care must be taken otherwise it can block legitimate traffic.

Network Security Audit

Network security audit are as important as Network security monitoring tools, appliances and antivirus software. Network security auditor will verify your network against all known vulnerabilities, virus, and security threats and will generate a report indicting which of your network devices and computer systems not meeting security criteria and suggested actions.

Here is the list of check for network and computers security Audits

1. Operating System Software: Choose the best operating system that will suit your environment requirement. Know that none of the Operating system available at any given point if time will be bug free and threat free. But knowing our operating system is vulnerable to what type of threats is also one type of precaution.
2. Vulnerability Patches: Regular check for known vulnerabilities and newly published vulnerabilities and install the patches
3. Update Firmware and BIOS: Old firmware and BIOS create security risk.

4. Username: Delete username and account related information once an employee leaves the organization
5. Password: Password must be regularly updated, should not be any directory word and should be alpha numeric.
6. No sharing of user accounts
7. Review roles, membership of the user account
8. Verify if proper policies are setup for Guest access, internet access, Mobile devices, Remote access, VPN access, email policy, data encryption policy, and network security policy.
9. Verify antivirus is setup properly and signature update mechanism in place.
10. Verify Firewall rules and polices, Router access control-lists (ACL), IPS/IDS setups
11. Use SNMP (Simple Network Management Protocol) version 3 is used and proper read only and ready right access-list are configured.
12. Verify is Cisco Discovery Protocol (CDP) or Link Level Discovery Protocol (LLDP) are not enable. Some people enable it depending on their setup security policies.
13. Verify daily backup and restore process is in place.
14. Vulnerability Scan: There are some tools available in the market which can do vulnerability check and generate report.

Common Mistakes

1. Sending sensitive information/data without encryption.
2. Using password security question whose answer can be easily guesses.
3. Using dictionary words as passwords.

4. Writing down password in text files.
5. Imposing not so strict password restrictions.
6. Letting vendor consultant define security.
7. Not knowing which services are important or not know how the data flows.
8. Not testing security.
9. Not having plan of action in case of cyberattack.
10. Neglecting security awareness trainings
11. Not staying up to date with latest in information security.
12. Not having qualified information security staff in the team.

[Perrin, 2008]

Best Practices

While implementing Network security best practices includes we need to think about:- LAN (Local Area Network) security best practices, Wireless security best practices, cyber security best practices, email security best practices, DNS and DHCP best practices, should be taken into consideration.

LAN /WAN Security best practices:

1. Apply port security, MACsec where ever needed.
2. Broadcast traffic rate controls, multicast traffic rate control to broadcast and multicast storms.
3. Remove VLAN 1 from trunks, prune unwanted VLANs from the trunk
4. Use Private VLAN (PVLAN) Configuration wherever needed
5. Use Access-control list (ACL) and Vlan access control lists (ACL) to filter traffic.
6. If you are using service provider link to connect your remote sites then you can IPsec tunnels to securely move your traffic along the link.

7. Implement Dynamic ARP inspection, password encryption, authentication for routing protocols, SNMP version 3 secured SNMP access.
8. Implement AAA (Authentication, Authorization, and accounting) using Radius or TACACS+

Wireless security Best Practices

1. Separate Internal user wireless network from external guest wireless network
2. Use WPA2 (Wi-Fi protected access 2) as wireless security protocol
3. Secure you access point physically.
4. Limit Wireless access point
5. Limit WIFI signal
6. Implement mechanism to detect Rogue AP.
7. Implement Wireless Intrusion Protection System
8. Implement Mobile devices and personal devices management
9. Make separate Wireless LAN (WLAN) for legacy wireless devices who does not support latest wireless security standards.

   [Froehlich, 2016]

Cybersecurity Best Practices:

1. Make a list of control system devices in your network make sure these systems are not externally connected without proper safety measures.
2. Setup Firewalls properly and segment your network to reduce the impact.
3. Setup secure Remote access methods like VPN.
4. Configure system event logging and configure role-based access.

5. Regularly check for vulnerabilities at https://www.cvedetails.com/ and apply updates and patches to your firmware, BIOS, and OS.
6. Apply proper security for mobile devices.
7. Educate all employees for cybersecurity related topics.
8. Update senior security management in the process of cyber security.
9. Develop a plan of action for situations like cyber attacks.

[WaterISAC 2012]

Best practices for Email Security

1. Do not open email attachments from unknown and or unexpected sender
2. Pay attention to phishing emails
3. Use Strong password
4. Instruct employees not to use email for private use.
5. Scan all the email and attachments for viruses
6. Use Span filter
7. Never click on unsubscribe link in spam emails.

   [Dobran 2018]

Conclusion

Our main topic of discussion in this paper is "Is my network secure?". The answer to that question would be it depends on how you setup computer and network security in your network. If we properly take all measures described in this research paper and design our network security, then you network is mostly secure. But we need to keep in mind that maintaining network security is a continuous process and not one-time thing. Since network security team is responsible for maintaining the network security, it is important that, this team is well funded, and they keep themselves aware of latest security threats in the market.

Reference:

Agbeboaye, C., Akpojedje, F. O., & Okoekhian, J. (2018). SECURITY THREATS ANALYSIS OF WIRELESS LOCAL AREA NETWORK. Compusoft, 7(6), 2773-2779. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/2064332169?accountid=10639

Khan, R., & Hasan, M. (2017). NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW. International Journal of Advanced Research in Computer Science, 8(8) Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1953785415?accountid=10639

Steven Furnell, David Emm, The ABC of ransomware protection, Computer Fraud & Security, Volume 2017, Issue 10, 2017, Pages 5-11, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(17)30089-1. (http://www.sciencedirect.com/science/article/pii/S1361372317300891)

Treharne, T. (2018). Spectre of doom: Channel reacts to security meltdown. Computer Reseller News, 10-11. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1987676296?accountid=10639

Colin Tankard, Advanced Persistent threats and how to monitor and deter them, Network Security, Volume 2011, Issue 8, 2011, Pages 16-19, ISSN 1353-4858, https://doi.org/10.1016/S1353-4858(11)70086-1. (http://www.sciencedirect.com/science/article/pii/S1353485811700861)

Hewlett Packard Enterprise, HP. "HPESBHF03769 Rev.1 - HPE Integrated Lights-out 4 (ILO 4) Multiple Remote Vulnerabilities." HPE Support Document - HPE Support Center, 2017, Retrieved from www.support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en_us.

Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard , Paul Kocher , Daniel Genkin , Yuval Yarom , Mike Hamburg (2018). Meltdown. Retrieved from https://meltdownattack.com/meltdown.pdf

Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher,
Michael Schwarz, Yuval Yarom (2018). Spectre. Retrieved from https://spectreattack.com/spectre.pdf

Admin (2018) Malware vs Virus. Retrieved from https://antivirus.comodo.com/blog/computer-safety/malware-vs-viruses-whats-difference/

K. Salah, K. Elbadawi and R. Boutaba, "Performance Modeling and Analysis of Network Firewalls," in IEEE Transactions on Network and Service Management, vol. 9, no. 1, pp. 12-21, March 2012.doi: 10.1109/TNSM.2011.122011.110151

Sultana, N., Chilamkurti, N., Peng, W. et al. Peer-to-Peer Netw. Appl. (2018). https://doi-org.jproxy.lib.ecu.edu/10.1007/s12083-017-0630-0

Shaikh, S.A. & Kalutarage, H.K. Telecommun Syst (2016) 62: 167. https://doi-org.jproxy.lib.ecu.edu/10.1007/s11235-015-0071-0

Orathai Sukwong, Hyong Kim, James Joe (March 2011) Commercial Antivirus Software Effectiveness: An Empirical Study. Retrieved from https://ieeexplore-ieee-org.jproxy.lib.ecu.edu/stamp/stamp.jsp?tp=&arnumber=5506074

Rouse Margaret (Jan 2018) Intrusion Detection System [IDS] Retrieved from https://searchsecurity.techtarget.com/definition/intrusion-detection-system

Froehlich Andrew (April 2016) .8 WLAN Security Best Practices. Retrieved from https://www.networkcomputing.com/network-security/8-wlan-security-best-practices/1977586091

WaterISAC (2012)10 Basic Cybersecuirty Measures. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

Dobran Bojana [2018] 9 Email Security Best Practices For 2018. Retrieved from https://phoenixnap.com/blog/email-security-best-practices

Perin Chad (2008) 10 common security mistakes that should never be made. Retrieved from https://www.techrepublic.com/blog/10-things/10-common-security-mistakes-that-should-never-be-made/