

**Christopher Hyde**

**Southern New Hampshire University**

**IT-320 – Network Security**

**Final Project**

**12/16/2018**



**Executive Summary**

I have been contracted by ABC Manufacturing as an information technology consultant to identify gaps in the security of the network and provide recommendations for improvement. The purpose of this report is to assess the current network infrastructure and vulnerabilities of the company, and then implement changes. In doing so, I will demonstrate evidence of the security risks such as firewall and virtual machine threats, identify security techniques like malicious software protection and intrusion detection, and implement critical changes. This is meant as a comprehensive guide of the network threats that exist, how they can be mitigated and what steps I took to do so. In short, the existing network for ABC Manufacturing is very poorly protected and therefore puts the whole financial stability of the company at risk; a situation more and more companies find themselves in.

*“Bombshell hacks were revealed one after another in 2017, from an Equifax breach that compromised almost half the country to global ransom campaigns that cost companies millions of dollars. More tools used by government hackers have become public, and it's easier than ever to create sophisticated ways to spread malware or ransomware or steal data from companies. Companies also frequently fail to patch security flaws in a timely manner.” (Larson, 2017)*

My methodology was based on taking on the persona of hacker trying to break into the system and what steps they would take to get in. Using various scans and tools such as Nmap and OpenVas, we can see which ports are open and determine vulnerabilities. NetworkMiner and Wireshark allow us to intercept and decipher network traffic. By knowing what routes an attacker might use we can then build defenses which allow us to be prepared for other potential attacks in the future.

**Network Assessment: Gathering Evidence of the Vulnerabilities**

The first step in assessing the basic security level of the network is to examine the traffic information using various tools. I examined the firewall status of both the Pfsense firewall (IP 203.0.113.100) as well as the Windows Server firewall (IP 192.168.1.10). Next, threats to the host machine were determined and the current malicious software protection level analyzed. Lastly, I executed intrusion detection techniques.

**Firewall**

A strong firewall is a must-have for any network. Basically, a firewall monitors traffic coming from external sources and validates compliance with pre-determined rules defined by the administrator.

*“Cyber security is certainly the most crucial part as all your system requires is important firewall protection system. Logically, the reasons behind network security are Trojans and key loggers; these threatening programs enter one’s system without your consent through illicit sites visited by users, thus creating the problems that follow. Failure to protect your computers may mean a failure to protect your business identity, which may ultimately hasten a person towards disaster.”(C9Soft, 2018)*

Firewalls can be easily violated through unencrypted HTTP connections and clients then exploited if they share the same network segment. There are access points that are vulnerable to breach; open ports that are related to unnecessary services.

Ideally all ports should be closed by default denying all access and then ports would be opened as needed. The only ports that should logically be open are port 80 for HTTP, 443 for HTTPS and ports 25, 465, and 587 for SMTP. However, testing showed several more were opened as well, which we will get to later in the report.

**Virtual Machine Threats**

As servers go from being protected behind a firewall to internet-accessible cloud-based virtualization environments, the threat from malicious attack becomes greater. To mitigate this, additional precautions should be taken. For starters, admin privileges should be limited to just a select few individuals in the company. Also, unnecessarily opened or unused ports present a security risk to the network and should be addressed whenever possible.

**Malicious Software Protection**

Malware comes in different forms such as trojans, logic bombs, worms, or viruses. They can pretty much cripple a computer network, compromising sensitive and critical data. While updating the anti-virus database is important, using multiple malware avoidance methods is too, since new and evolving malware is always being introduced. They can enter a network internally through 3rd party installed applications, infected USB thumb drives, or by destructive scripts hidden in document files deploying phishing attacks.

**Intrusion Detection**

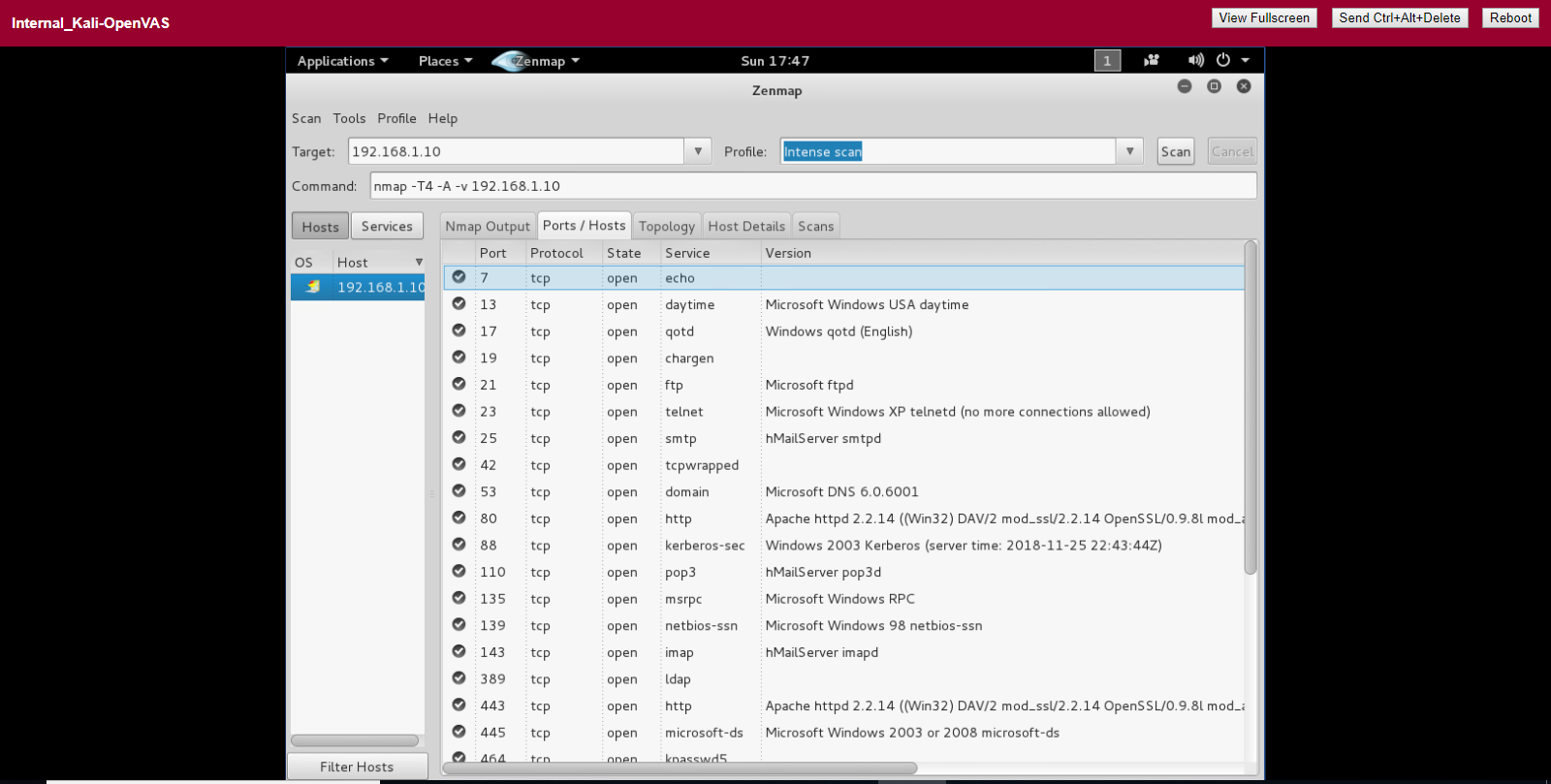
Intrusion detection systems (IDS) monitors network traffic, both inbound and outbound, and looks for suspicious activities. There are several different types of IDS. The two main ones are host-based (HIDS) and network-based (NIDS). Since firewalls can be circumvented through various means of attack, IDS is more complex and can find problems at an internal level. An IDS can map users’ activities and look for misuse at an individual level. They can also operate in a switched and encrypted environment.

**Vulnerability Assessment**

After gathering the evidence in the network assessment, I was able to interpret that information and develop a summary of the vulnerabilities with respect to network traffic, hardware, operating systems, and anti-malware software.

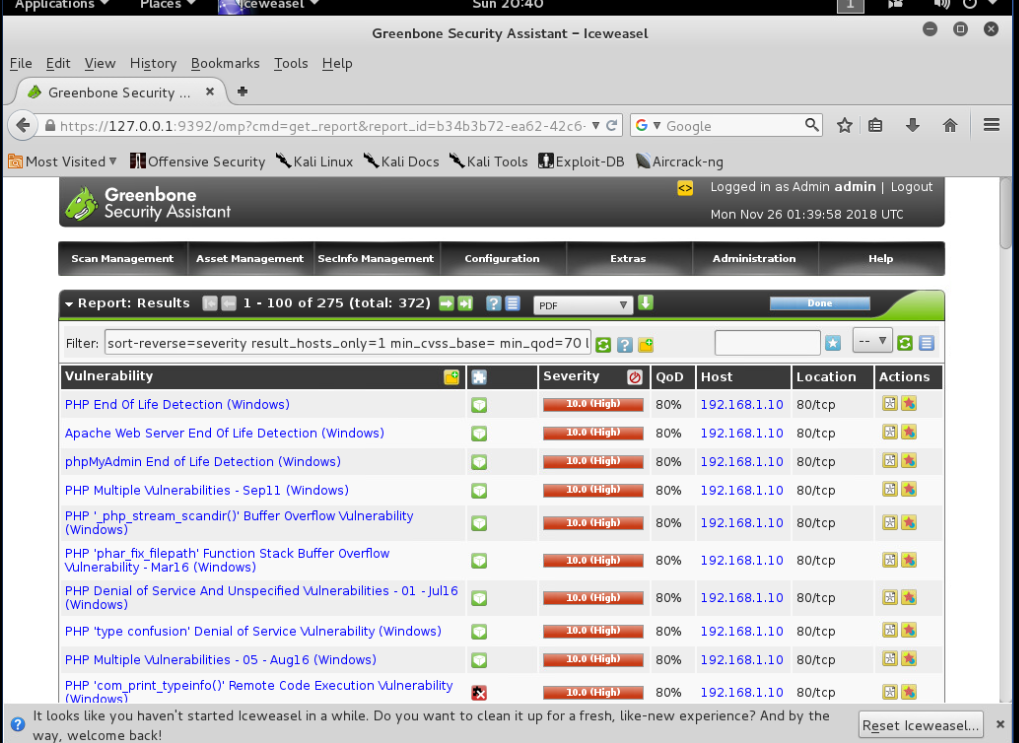
**Network Traffic**

The Nmap scan tool can perform network penetration testing by scanning TCP ports; mapping hosts and TCP services, revealing unnecessary open ports which could expose the system to the internet. It does this by sending packets to each port and listens for a response. Zenmap is a more detailed look at the open ports discovered by Nmap….



(Infosec,2018)

While the company’s firewall was active, there were found to be many exceptions that were allowed through that shouldn’t be. Those exceptions represent a risk to the network. The browser-based OpenVas scanner, Greenbone Security Assistant, is a powerful scanning tool that scans the IP addresses of hosts on the network and tests their vulnerability levels.



(Infosec,2018)

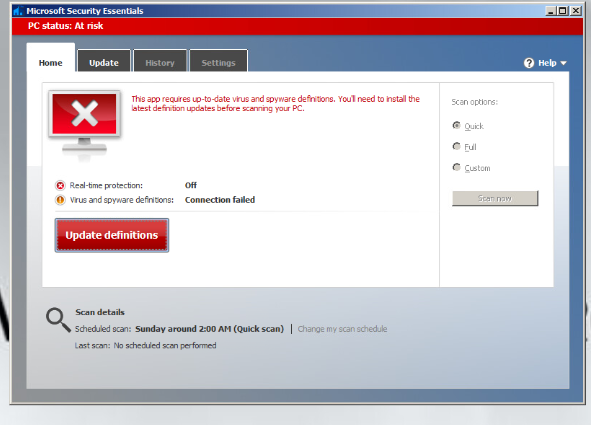
The intense scan of those hosts in addition to the firewall itself revealed a high severity of risk, particularly on the Windows Server machine.

**Operating Systems / Workstations**

Keeping up-to-date with Windows security patches can go a long way in protecting the operating system at a users’ workstation. Out-of-date productivity and server software also pose a security risk. It was discovered that the Windows Server had only been updated to Service Pack 1 rather than the newer Service Pack 2 which includes security improvements over the first.

**Anti-Malware Systems**

A Microsoft Security Essentials scan revealed that the Windows Server PC was at risk for potential malware infection. This is because virus definitions were found to be not updated and regular scans not performed.

(Infosec,2018)

**Network Hardware**

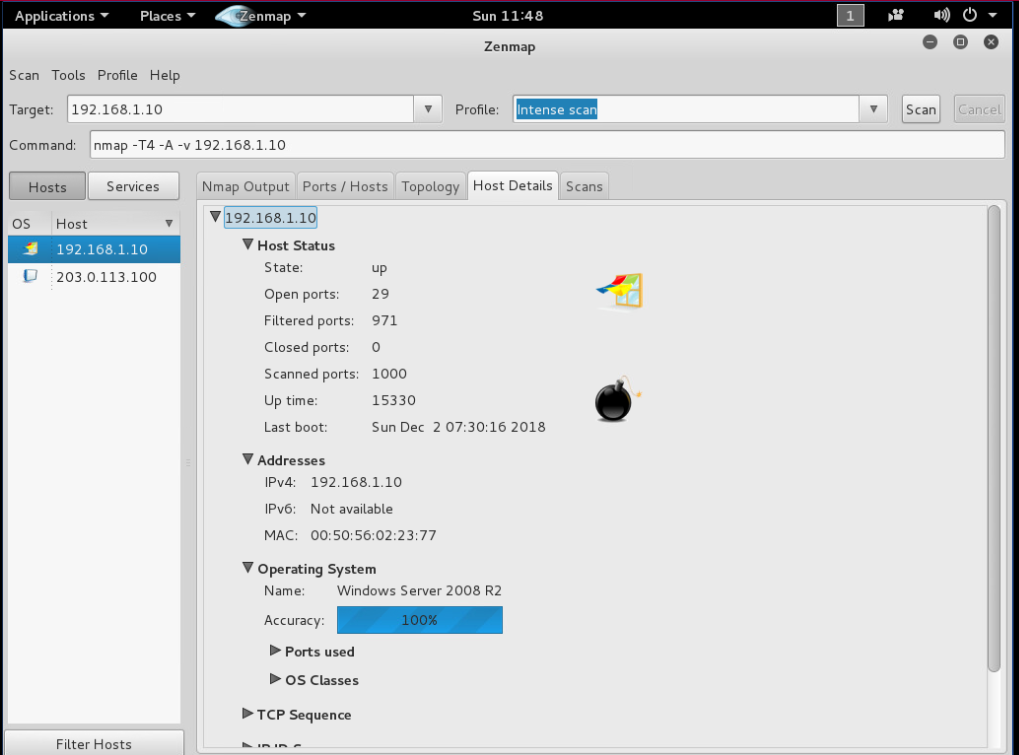
Older PC’s and laptops lack the built-in security features of new ones. Likewise, hardware such as firewall appliances, routers, and WiFi access points if not updated can represent a risk to the network.

**Network Security Posture Recommendations**

In this segment, I have identified the specific aspects of the network that require addressing and assigned risk criteria to those areas. I have put together mitigation strategies, established a priority to each strategy, and explain the reasoning behind them. Finally, I implemented those changes on the network.

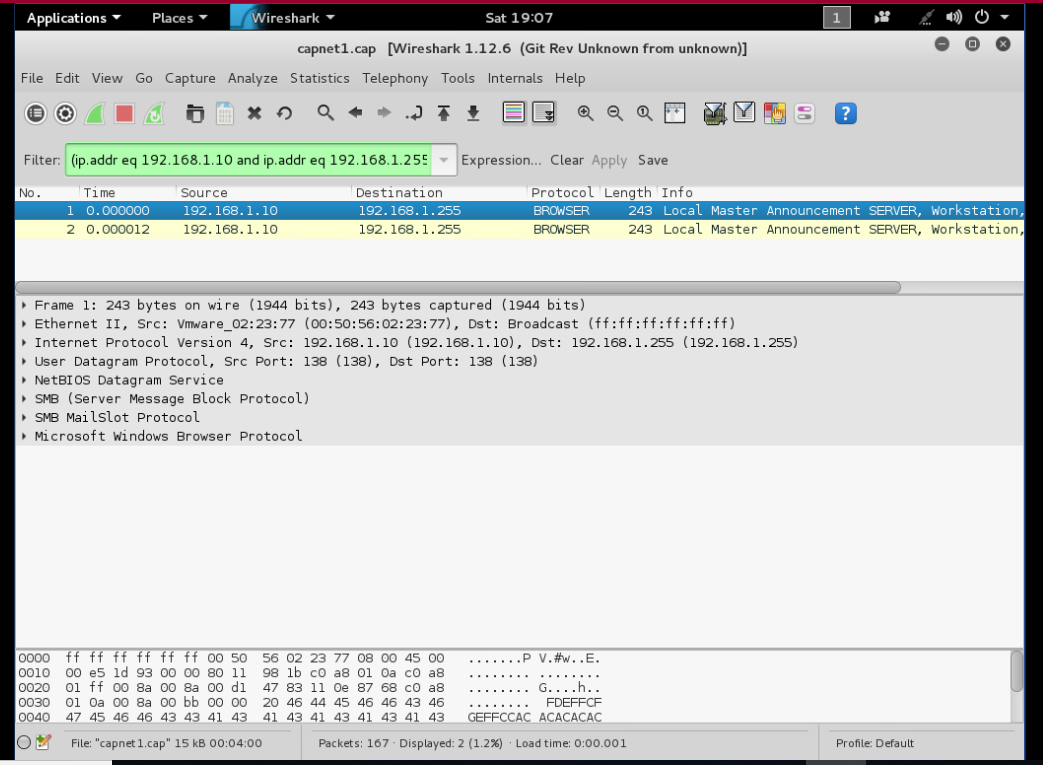
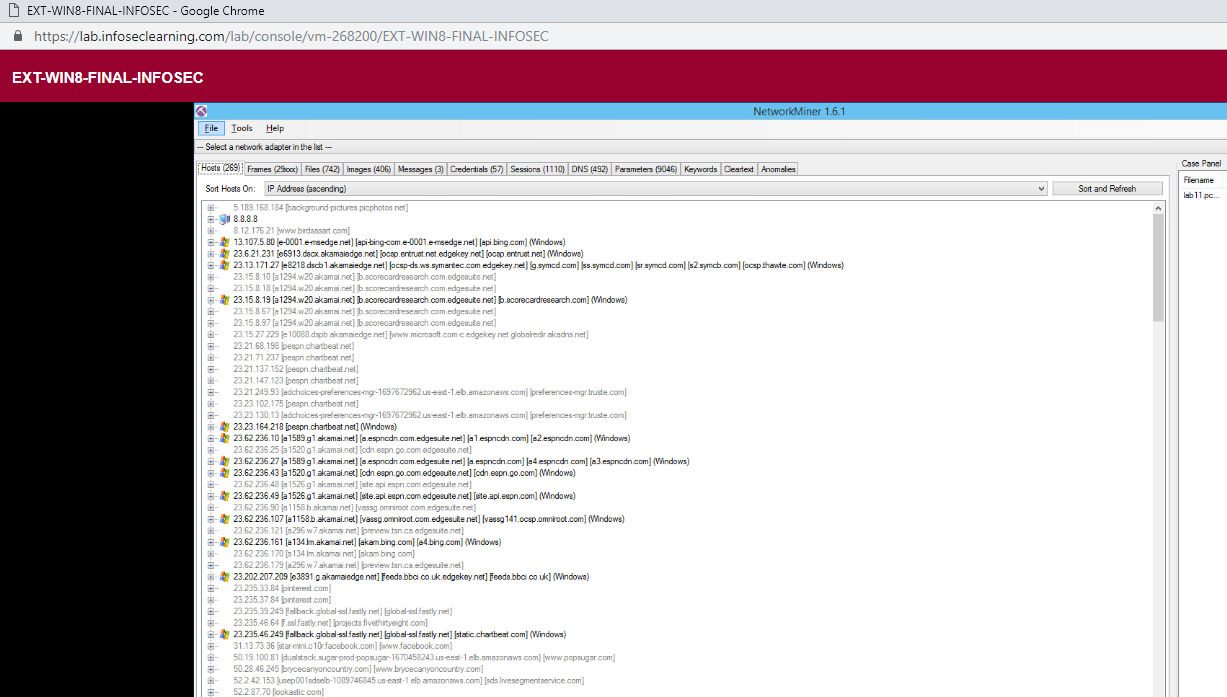
*Server-Related issues*

The firewall server has the most significant issues in the entire network. Telnet on port 23, for example, uses un-encrypted clear text protocol and should definitely be blocked, however, it was not. Since it is a legacy protocol, it is not widely used anyway. Other unnecessary ports were also open allowing traffic to come in. A scan of the network using Zenmap showed a total of 29 ports were open and 0 were closed

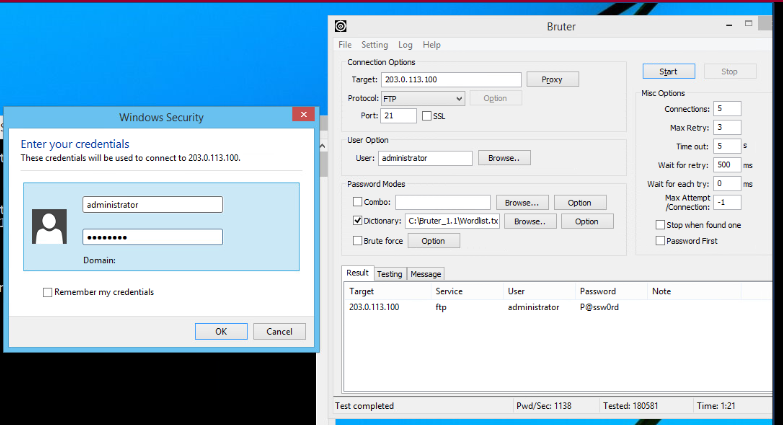
 Infosec (2018)

For security’s sake, it’s best to implement a NAT rule on all addresses and ports which effectively blocks all traffic by default, allowing only the appropriate traffic in such as HTTP (Port 80) and Server-to-client (Port 3389). The default username and password are also in place for the pfSense firewall making it easy for someone to hack in to the network. The login credentials should be changed as soon as possible.

A packet sniffer known as Snort is software which captures incoming and outgoing network traffic. It can then be viewed with programs such as Wireshark and NetworkMiner. A test performed as part of the network security assessment verified that a substantial amount of traffic was moving through the network and that no Intrusion Prevention System (IPS) was present.

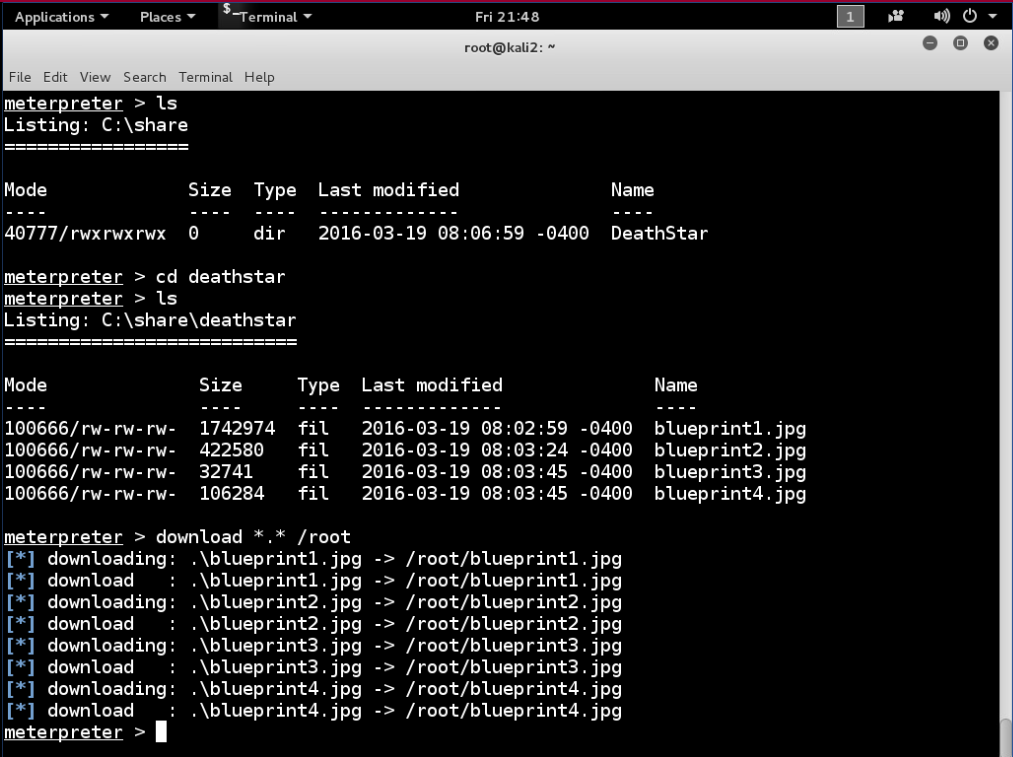
  Infosec (2018) Infosec (2018)

Because of this, a vulnerability was exploited using a program known as Metasploit that allowed me to then use a program called Bruter to scan the IP address to capture login credentials.



Infosec (2018)

From that point I could gain access to the server, view files on the victim machine’s shared drive. and then download them. (See Below)

Infosec (2018)

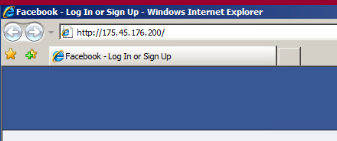
As a manufacturer, this vulnerability could cause proprietary information to fall into the wrong hands and expose them to a Ransomware attack. The other possibility is embedding the files with trojans or keyloggers so the unsuspecting user opens them exposing the company to further issues.

*Client-Related Issues*

Further investigation showed that the Windows 7 2008 Server was not updated to the latest Service pack. It was also lacking many security patches. The Windows 10 client machine lacked patches as well. Even though it had Windows Defender installed, its virus definitions were not up-to-date. Both machines did not have any means of malicious software removal such as Microsoft Security Essentials either. This is a free piece of software and should be installed on the system for at least a minimum level of protection. Anti-Virus software such as Windows Defender would add another layer of real-time protection for the client machines.

Through what’s known as Privilege escalation, users in the organization with less permissions and rights can access administrative level areas of the network that they should not be allowed to. There appear to be no controls in place to prevent this.

Social Engineering represents another big problem. Links to these malicious sites are usually embedded in phishing emails tricking the user to click on them and enter their personal information. In the example below the user is sent an email, supposedly from the founder of Facebook luring them to join the social media site. In actuality, the URL is not [www.facebook.com](http://www.facebook.com) but through the Metasploit browser Autopwn, a redirect link to the attacking machine (IP 175.45.176.200).

Infosec (2018)

In order to resolve these issues, I have put together a table which summarizes the findings and the recommended actions based on risk criteria such as impact, likelihood and priority. Aspects that play a role and need to be considered when determining resolution are cost vs. benefit, operational impact and feasibility.

The *Risk levels* range from Very Low to Very High. Threats in the lower range are not as critical but should be addressed at some point. By contrast, threats in the higher range represent the greatest risk to the company and need to be acted upon immediately. The *Impact* identifies the level that the company will be impacted by this threat on an operational or financial basis. The *Likelihood* rating designates how possible the threat is to present itself. *Prioritization* is the order in which the corrective actions should executed based on the level of threat.

The Risk Ratings Matrix below illustrates these criteria.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Likelihood | 5 | Medium | High | High | Very High | Very High |
| 4 | Medium | Medium | Medium | High | Very High |
| 3 | Low | Medium | Medium | Medium | High |
| 2 | Very Low | Low | Medium | Medium | Medium |
| 1 | Very Low | Very Low | Low | Low | Medium |
|  |  | 1 | 2 | 3 | 4 | 5 |
|  |  | Impact | | | | |

For a detailed breakdown of the threat indicators, see the findings table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability | Impact (1-5) | Likelihood (1-5) | Priority (1-5) | Mitigation Strategy |
| Phishing Attack | 4 | 2 | 3 | Schedule user training sessions |
| Failure of aging equipment | 2 | 1 | 2 | Upgrade servers and clients |
| Out-of-Date Software or Operating System | 2 | 2 | 4 | Install Updates and Patches |
| Malware or Virus attack | 5 | 3 | 4 | Install anti-virus software on all clients and create a VPN. |
| Password Policy | 4 | 3 | 5 | Establish a minimum password requirement |
| Firewall Hardening | 5 | 4 | 5 | Close unnecessary ports |
| Privilege escalation | 3 | 2 | 3 | Implement a Group Policy |
| Human Error | 2 | 2 | 2 | Schedule user training sessions |

**Rationale**

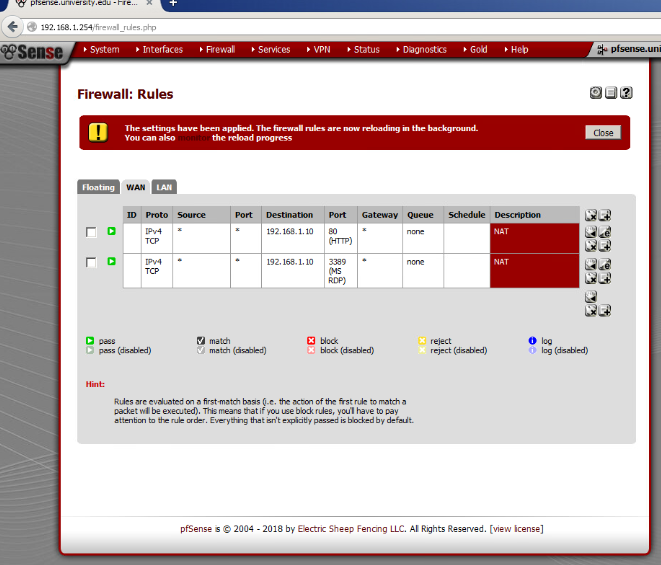
The mitigation strategy was prioritized in such a way to take care of the more critical issues first. Since the firewall is the first line of defense, it makes sense to address those issues first followed by the client-related problems.

**Implementation Solutions**

**Execution**

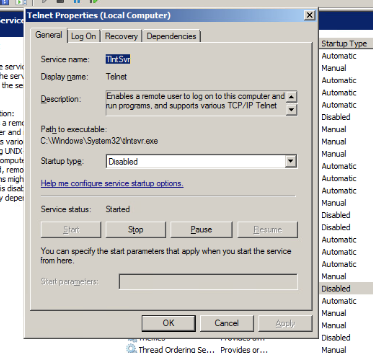
As mentioned earlier, the firewall has quite a few unnecessary ports that are open. Logging into the pfSense firewall shows the NAT rules for the WAN are very liberal.

To fix this, I eliminated all rules with the exception of those governing HTTP (Port 80) and Server-to-client traffic (Port 3389).

 Infosec (2018)

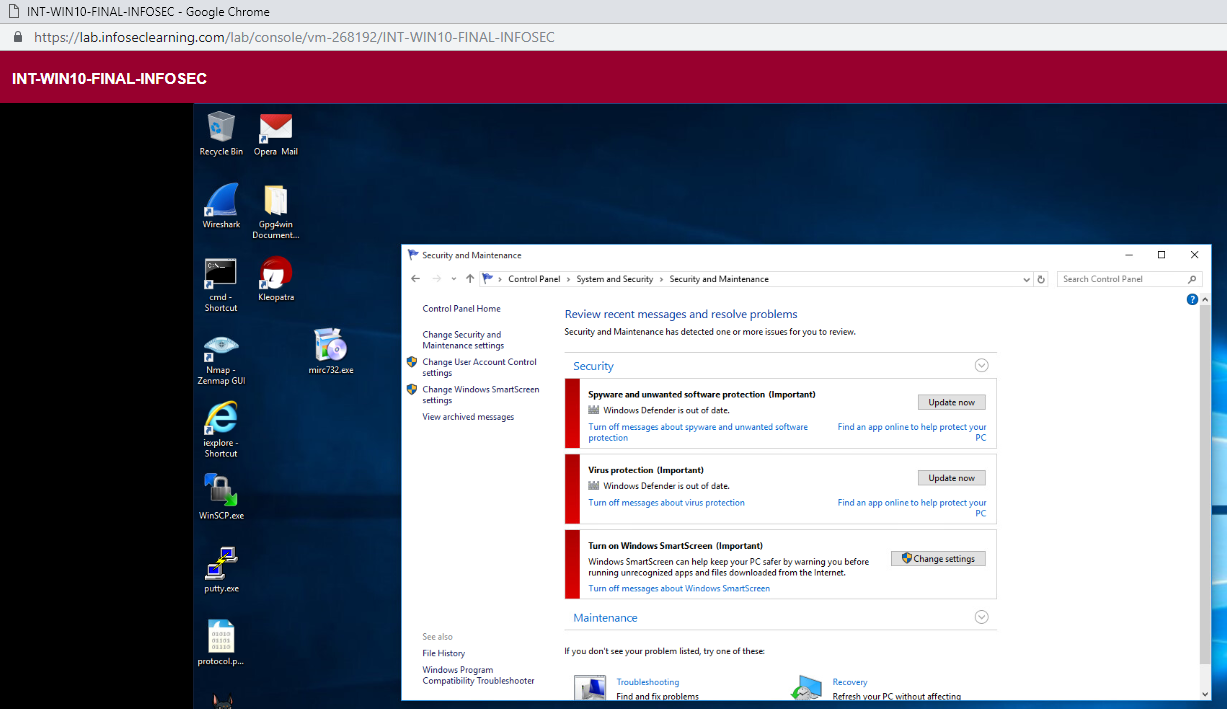
By either deleting or disabling certain services in the port exceptions tab, we can minimize the exposure to threats.

As we see below, I have disabled several serves including Chargen, Daytime, Echo, FTP Server, QOTD, and Telnet. This greatly reduces the risk of exposure.

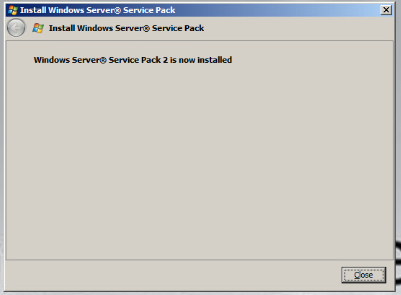
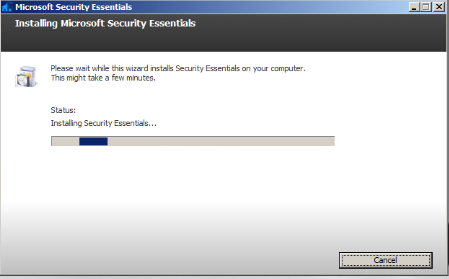
Infosec (2018)

**Hardening the Server**

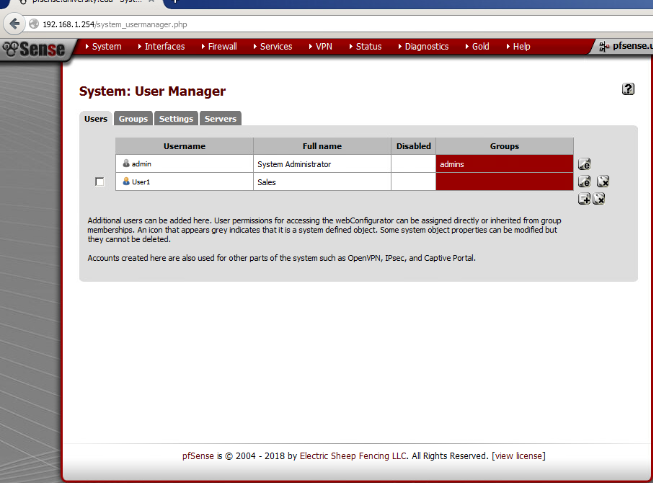
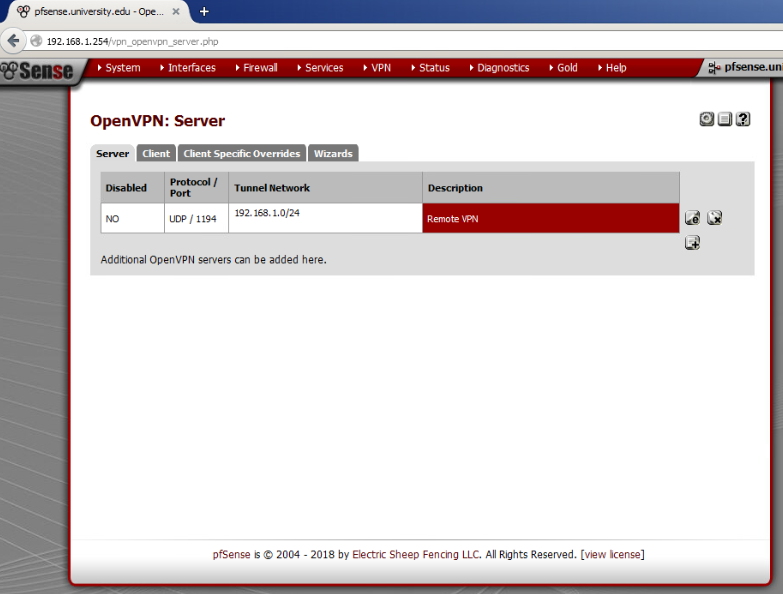
To harden the security of the network, I enacted several solutions. While the Windows 10 machine has Windows Defender, it is not up-to-date. It is not protecting against spyware, viruses, or dangerous apps.

Infosec (2018)

I therefore installed Service Pack 2 to institute all the latest definitions, as well as Microsoft Security Essentials.

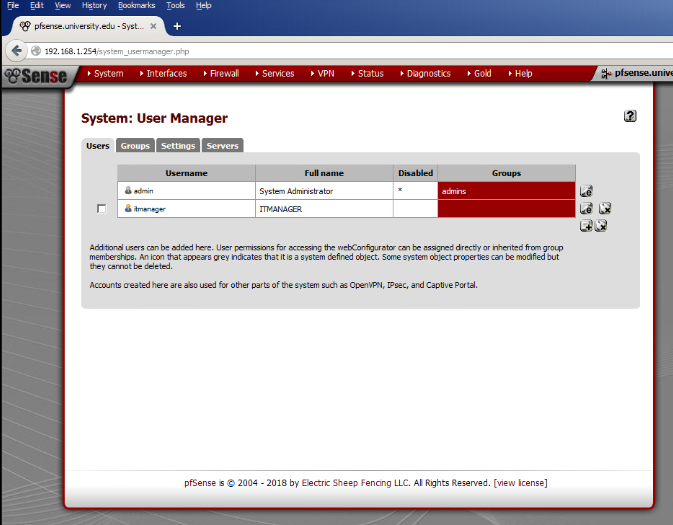
  Infosec (2018)

A virtual private network (VPN) is an encrypted connection over the internet between the server and the client. Since clients can now include mobile devices which carry a risk of intrusion themselves by hackers, it extends the risk that much further. To reduce that vulnerability, I installed a VPN in the current network that all traffic must connect through. Here, I create a user account, “Sales” with their own username and password rather than the admin’s. I also assigned a certificate-based user authentication for the SSL VPN for added security.



Infosec (2018) Infosec (2018)

Lastly, to correct the default user and password issue in the PfSense firewall, I created a “new” administrator and disabled the existing “admin” user effectively giving them admin rights. The new credentials are: Username: itmanager, Password:C0rp0rate23!

 Infosec (2018)

**The Human Element**

Ultimately the human element plays a very large role. Educating employees about the dangerous of potential threats and viruses through end-user training should be initiated in the coming months. Also, instituting an Acceptable Use Policy that stipulates what their workstation should and should not be used for, and distributing a training manual to new hires can go a long way in protecting company data.

**Conclusion**

Companies such as Walmart, Home Depot, Target, and TJ Maxx in recent years have fallen victim to massive data breaches that cost them millions. While companies that size may be able to recover financially, a breach to a smaller company as ABC could have devasting consequences.

*"We continue to see sizable gaps in how organizations defend themselves," said Mike Denning, vice president of global security for Verizon Enterprise Solutions. "While there is no guarantee against being breached, organizations can greatly manage their risk by becoming more vigilant in covering their bases."(Violino,2015)*

Hopefully, this report has demonstrated how vital it is that ABC Manufacturing vigilantly maintain the security of their network on a regular basis to ensure the continued success of the company.

**References**

Stewart, M (2010). Fundamentals of Network Security. *Network Security, Firewalls, and VPN’s.* Retrieved from <https://www.safaribooksonline.com/library/view/network-security-firewalls/9780763791308/ch02.html>

Eldorado Printing (2018). Network Security. [title image] received from <https://www.eldoradoprinting.com/network-security>

Larson, S (2017, Dec 20). The Hacks that left us exposed in 2017. *CNN Business*. Retrieved from https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

C9Soft (2018). Importance of Firewall in Network Security. Retrieved from <http://c9soft.com/blog/2015/11/20/importance-of-firewall-in-network-security/>

Infosec (2018). Zenmap output [Image]Retrieved from <https://lab.infoseclearning.com/lab/console/vm-250789/Internal_Kali-OpenVAS>

Infosec (2018). Wireshark output [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-268200/EXT-WIN8-FINAL-INFOSEC>

Infosec (2018). Greenbone Scan Detail [Image]Retrieved from <https://lab.infoseclearning.com/lab/console/vm-250789/Internal_Kali-OpenVAS>

Infosec (2018). NetworkMiner output [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-268200/EXT-WIN8-FINAL-INFOSEC>

Infosec (2018). Bruter menu [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-268200/EXT-WIN8-FINAL-INFOSEC>

Lepofsky R. (2011, Feb 23). Intrusion Detection: Why do I need IDS, IPS, or HIDS. *Networkworld.* Retrieved from <https://www.networkworld.com/article-/2228598/security/intrusion-detection--why-do-i-need-ids--ips--or-hids-.html>

Infosec (2018). Microsoft Security Essentials install screen [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-250790/WIN-2K8SP1-INFOSEC>

Infosec (2018). Microsoft Security Essentials virus scan [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-250790/WIN-2K8SP1-INFOSEC>

Infosec (2018). Opera Mail [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-250790/WIN-2K8SP1-INFOSEC>

Infosec (2018). pfSense Port Rules [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-250790/WIN-2K8SP1-INFOSEC>

Infosec (2018). pfSense User Manager [Image]. Retrieved from https://lab.infoseclearning.com/lab/console/vm-302016/WIN-2K8SP1-INFOSEC

Infosec (2018). Windows Security Center [Image]. Retrieved from <https://lab.infoseclearning.com/lab/console/vm-268192/INT-WIN10-FINAL-INFOSEC>

Kaspersky (2018). What is Malware and how to defend against it. *Kaspersky.* Retrieved from <https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it>

Violino B. (2015, Apr 22). Organizations Are Not Doing Enough To Secure Data. *Baseline Mag.* Retrieved from http://www.baselinemag.com/security/organizations-are-not-doing-enough-to-secure-data.html