**Assignment 5 – Network Security**

Nathan Ketterlinus

Fisher College of Science and Mathematics

Towson University

Towson, United States

[nketter1@students.towson.edu](mailto:nketter1@students.towson.edu)

CIS377\_Fall 2023 Dr. Atul Rawal

**Assignment 5**

Viruses, Policy, Reconnaissance

1. **Warm up:** Download and install the AVG Free antivirus software on your machine. It is a lightweight software install that you can remove after the assignment, if you have other protection already.
2. Carefully study the application, noting features you like and **dislike**.

I appreciate the app’s overall UI, it is very easy to navigate and make changes. I like that users can add a password to AVG to prevent unwanted users from making changes. I am not a huge fan of how little they explain what some features are, like what the differences between low, medium, and high sensitivity are for their detection feature. In addition, a lot of the wording seems to make everything seem either more dangerous as a threat, or more protective as a defense. As a consumer educated enough to see this going on, I don’t appreciate how their wording can scare uneducated users into getting the premium version.

1. Compare the application to its paid version. Comment on which features in the paid version are worth paying for given the cybersecurity risks you face as a student.

A screenshot of a computer security system

Description automatically generated

I believe the premium features “Protects your private documents” and “provides safer online shopping” are the most relevant to me as a student. Protecting private documents is important because if a malicious actor can steal an assignment of mine, I could be falsely punished for academic dishonesty. In addition, safer online shopping is important for students because of the number of things they have to buy for school, such as tuition, textbooks, school supplies, and licensed software. There is also something to say about the importance of another premium feature “keeping me safe from fake websites”. Apart from the obvious cybersecurity threats of fake websites, like their ability to spread malware or install backdoors, they could also present false information, jeopardizing the quality of research students can accomplish.

1. Which version would you recommend to a non-student population (say your parents), and why?

To demographics that aren’t as tech savvy, I would recommend the premium version, as it takes care of a bunch of threats that they may not think to cover, such as fake websites or unwanted remote desktop access. However, in groups that are more tech-savvy, I believe they could get away with the free version, as I not only trust their ability to safely navigate the web in a careful and responsible manner, but also to effectively mitigate any unwanted consequences of their risky actions.

* 1. **Security Policy:** Consider what you have learned from the book, and discussions in class till date, write a small antivirus policy for the IT infrastructure and users in a
  2. **a.** small business

This policy is designed to protect the company’s digital assets by enforcing appropriate anti-malware and antivirus measures on all devices connected to the company’s network. As a starting point, all machines must:

* Have appropriate antivirus software, such as AVG installed.
  + It should be configured in such a way that does not limit the effectiveness of the program.
  + It should be enabled on boot, and never disabled unless there is an approved, compelling reason to do so.
* Have their operating systems regularly patched with current updates from trusted vendors.
* Have their software regularly patched with current updates from trusted vendors.
* Only connect to company-approved Wi-Fi networks
* Route all traffic through the company’s proxy server.
  + This prevents machines from establishing themselves as a server, such as for email or sharing files.
  + This ensures that all traffic passes through the company’s firewall.

In addition, there are some behaviors employees must follow to protect not only company data, but also any relevant personal data. These include (but are not limited to):

* Only accessing approved websites.
  + In addition, verifying that the site is the intended site, and not an impostor site, like [www.mikrosoft.com](http://www.mikrosoft.com), and checking that every site is HTTPS encrypted, instead of just HTTP (check for the padlock in the address bar), will go a long way in ensuring general privacy and safety online.
* Not downloading any unapproved software
  + This includes copying software from USB drives or other means that may not explicitly be considered “downloading”.
* Not tampering with any settings on software that may cause a security vulnerability.
  + This is designed to prevent changes to antivirus software and other important safeguards, while still allowing for changes to things like mouse scroll speed, font size, and other personalization/accessibility settings.
* Double checking all incoming email, being especially wary of any attachments.
  + If not explicitly asked for, it’s best practice to not open any attachments at all.
* Reporting any users who you suspect to be in violation of these policies to appropriate authorities, such as the IT department, HR department, or police (if necessary).

In general, just use common sense. If something looks suspicious, it’s probably for the best that you don’t use it, and let others know not to do it too.

Finally, there are some activities that are strictly banned to prevent insider threats. These are not designed for one person, but rather are in place to adhere to best practices. Employees are not allowed to deliberately engage in behaviors which would compromise the company’s integrity. This includes behaviors such as:

* Port scanning devices on the network.
* Sniffing packets sent over the network.
* Allowing someone else to access your computer in an unauthorized manner.
* Accessing someone else’s computer in an unauthorized manner.
  + This includes employees using anyone else’s computer but leaves room for approved IT staff in the event they need to troubleshoot or enforce company policy.
  1. b. an elementary school

This policy is designed to protect the school’s digital assets, as well as the privacy of all employees and students by enforcing appropriate anti-malware and antivirus measures on all devices connected to the school’s network. As a starting point, all machines must:

* Have appropriate antivirus software, such as AVG installed.
  + It should be configured in such a way that does not limit the effectiveness of the program.
  + It should be enabled on boot, and never disabled unless there is an approved, compelling reason to do so.
* Have their operating systems regularly patched with current updates from trusted vendors.
* Have their software regularly patched with current updates from trusted vendors.
* Only connect to school-approved Wi-Fi networks
* Route all traffic through the school’s proxy server.
  + This prevents machines from establishing themselves as a server, such as for email or sharing files.
  + This ensures that all traffic passes through the school’s firewall.

Students, teachers and other staff should take care to adhere to the following behavior guidelines:

* Only access approved websites, or those believed to be both safe and necessary to instruction.
  + In addition, verifying that the site is the intended site, and not an impostor site, like [www.mikrosoft.com](http://www.mikrosoft.com), and checking that every site is HTTPS encrypted, instead of just HTTP (check for the padlock in the address bar), will go a long way in ensuring general privacy and safety online.
  + As an extension of this, teachers and staff should diligently ensure that students are only on whitelisted websites and software.
* Do not download any unapproved software.
  + This includes copying software from USB drives or other means that may not explicitly be considered “downloading”.
  + While visiting unapproved websites can be done, much more care should be taken regarding software. As such, all software must be whitelisted by IT staff before being used.
* Do not tamper with any settings on software that may cause a security vulnerability.
  + This is designed to prevent changes to antivirus software and other important safeguards, while still allowing for changes to things like mouse scroll speed, font size, and other personalization/accessibility settings.
* Double check all incoming email, being especially wary of any attachments.
  + If not explicitly asked for, it’s best practice to not open any attachments at all.
* Report any users who you suspect to be in violation of these policies to appropriate authorities, such as the IT department, HR department, or police (if necessary).

Finally, there are some activities that are strictly banned to prevent insider threats. These are not designed for one person, but rather are in place to adhere to best practices. Students, teachers, and staff are not allowed to deliberately engage in behaviors which would compromise the school’s integrity. This includes behaviors such as:

* Port scanning devices on the network.
* Sniffing packets sent over the network.
* Allowing someone else to access your computer in an unauthorized manner.
* Accessing someone else’s computer in an unauthorized manner.
  + This includes employees using anyone else’s computer but leaves room for approved IT staff in the event they need to troubleshoot or enforce company policy.

You may research anti-virus policies of organizations on the web, please use and cite responsibly. (Minimum one-full page for each)

**Security Recommendation:** Rose Shumba manages the IT security for a school. Given the wide range of people who use the school’s computers, it is challenging for Rose to prevent virus infections. She has installed an anti-virus on each machine and has a policy prohibiting software downloads. Comment on:

* 1. a. How secure is the network from viruses?

Rose has done a good job at blocking the more common attack vectors. However, there are still some vulnerabilities in which a dedicated attacker can sneak a virus onto the network.

* 1. b. What areas has Rose not secured?

Web attacks, such as buffer overflows and cross-site scripting, remain as possibilities for arbitrary code execution. Obviously 0-day attacks will always be an attack vector. Finally, the threat of social engineering network members into either disabling the anti-virus or otherwise adding vulnerabilities to the network should not be overlooked.

* 1. c. What recommendations would you make to Rose to increase the security?

To limit the efficacy of these attack vectors, Rose can block all web traffic to unapproved websites, and only whitelist servers where buffer overflows and XSS cannot occur, although this seems to be a heavy-handed approach. While 0-day threats cannot ever be truly completely accounted for, best practice would be to have all machines automatically patch their operating systems and software anytime important security updates come out. Finally, Rose can instate mandatory cyber training exercises for all network users. While this won’t stop deliberate insider threats, it can go a long way in stopping behaviors which might accidentally introduce viruses into networks, like using uncleared USB drives.

* 1. **Reconnaissance**: Download and install the Nmap port scanner. Find tutorials for Nmap on their site, your book, and other resources on the web and keep them handy. **Understand what you are about to do first!** Run at least three different scans on your computer (set **localhost** as target). Please be aware of the Towson University policy if you are on campus: https://www.towson.edu/technology/about/policies/resnet.html. Use localhost as target only.
  2. A screenshot of a computer program

     Description automatically generated
  3. Run a scan on scanme.nmap.org as target. What key differences do you see in the results on your machine vs nmap.org? Research and explain the differences.
  4. A white screen with text

     Description automatically generated

My Windows 10 VM had 2 ports open: 135 and 445. Scanme.nmap.org had 4 ports open, 22, 80, 9929, and 31337.

Port 135 “enables other systems to identify what services are available on a machine and on which port they can be found. Essentially it allows a system unfettered access to a target system” [1]. Port 445 “is used by newer versions of SMB (the Server Message Block Protocol) (after Windows 2000) on top of a TCP stack, allowing SMB to communicate over the Internet. This also means you can use IP addresses to use SMB like file sharing” [2]. Seeing as how I created this VM specifically for this assignment, and the only software on it is AVG (with its firewall up) and Nmap, it makes sense that there would be so few ports open, and that the ones that are open are related to VMs.

Port 22 is used for the SSH protocol. Port 80 is used for the HTTP protocol. Port 9929 is unique to Nmap, it is used to show users how packets change in transit [3]. Finally, port 31337, which translates to ELITE if you squint really hard, is used for 2 main purposes. Firstly, there was a trojan horse called Back Orifice that allowed attackers remote access to a system through that port [4]. Secondly, Sky, an ISP, uses that port to perform remote maintenance for clients [4]. The fact that these ports are open makes sense for scanme.nmap.org as well. Ports 22 and 80 are standard for receiving web traffic, while 9929 is proprietary. Finally, my best guess is that the server is managed by Sky, who requires customers to leave 31337 open. I doubt that the port is open because of a trojan that was relevant decades ago.

As a quick side note, I appreciate how many different OS’s Nmap thought scanme.nmap.org could have been hosted on, while they were completely confident in my own OS.

* 1. **Reconnaissance**: Jane has an intent to penetrate the network in an organization. She has used passive reconnaissance to gather extensive information on the company. She finds out the model numbers of routers and other devices by reading discussions between system administrators in forums. She also has a list of all the IT staff and their phone numbers. She also has the services running on ports on some machines she ran a network scanner on. What reasonable steps should the company have taken to prevent Jane from finding this information? (One full page minimum)

The company has a lot of things they could have done better to prevent Jane from gathering so much passive information. Passive information is information that’s publicly available and that doesn’t need to be gathered in a compromising manner. In general, the company can do a much better job at limiting the amount of information that they make available to the public. A good rule of thumb would be to only share what is necessary: nothing more, nothing less.

A good first step would be to either encrypt or otherwise hide the information on the system administrator’s forums. If internal communications are not taking place strictly inside the company’s network, then that should be changed to prevent sensitive info being sniffed out by any malicious actors listening in. In addition, educating system administers to not share sensitive info so freely would also probably help. Although slightly impractical, and could change the burden of security from digital to physical, IT staff can share necessary sensitive information through physical mediums, such as sticky notes.

Not much can be done to completely hide the IT staff’s information and their phone numbers, unless phonebooks and social media like LinkedIn are completely reworked. However, removing contact information off any company websites or other company-managed contact lists couldn’t hurt. Since this may be impractical in a business setting, an IT page could be set up with a phone number for their front desk, operating on similar principles to a proxy server.

Finally, although a port scan can be difficult to completely prevent, the company can port scan their own devices, and block any unnecessarily open ports they find on their own devices, limiting not only the data that Jane can find but also the possible attack vectors she can use. A good rule of thumb is to only have the bare minimum number of ports open to operate properly. Supplementarily to this, the company could also implement a firewall and IPS in a way that would attempt to block Jane’s port scan once it was detected. While this would mean that some information would be gleaned, it can be an effective mitigation tool for the company across various circumstances, not just in dealing with Jane’s port scan. For instance, brute force attacks and DoS attacks can be easily prevented by a properly configured IPS.

* 1. What steps should the company take to prevent or reduce the efficacy of port scans? (One full page minimum)

Although a port scan can be difficult to completely prevent, there are steps the company can take to limit the efficiency of such scans. For instance, the company can port scan their own devices, and block any unnecessarily open ports they find on their own devices, limiting not only the data that Jane can find but also the possible attack vectors she can use. A good rule of thumb is to only have the bare minimum number of ports open to operate properly. In addition, the implementation of a strict firewall across the entire network can be used in conjunction with manually closing ports on a per-device basis.

Supplementarily to this, the company could also implement an aggressive IPS in a way that would attempt to block Jane’s port scan once it was detected. While this would mean that some information could be gleaned, it can be an effective mitigation tool for the company across various circumstances, not just in dealing with Jane’s port scan. For instance, brute force attacks and DoS attacks can be easily prevented by a properly configured IPS. An IPS combined with honeypots, or ports/machines designed to trick attackers into focusing on them, can be an extremely useful combination in catching amateur attackers or those that don’t think to account for fake ports.

Network segmentation can also be implemented to mitigate any damage Jane may be able to cause with information she gets from a port scan. If one segment is found with a vulnerability, then all other segments can be saved from attacks if configured properly.

Finally, as is best practice in many other aspects of cybersecurity, all machines on the company’s network should be regularly updated to receive relevant security patches from the developers of their operating system. These patches regularly fix security vulnerabilities. Applying them to the company’s machines prevents patched attacks from being effective.

While the company may only be able to implement a few of these measures, they are designed to work in tandem with each other to prevent attackers from taking advantage of the more common attack vectors and methods of port scanning. The more of these features that the company can implement, the better coverage they will have in not only preventing port scans, but also other common cyberattacks.

References

[1] H. York, “What is TCP Port 135 [HelpWire blog],” HelpWire Blog, https://www.helpwire.app/blog/tcp-port-135/ (accessed Oct. 6, 2023).

[2] A. T. Tunggal, “What is an SMB port? A detailed description of ports 445 + 139: Upguard,” RSS, https://www.upguard.com/blog/smb-port (accessed Oct. 6, 2023).

[3] L. M. Garcia, “Chapter 18. NPING reference guide,” Chapter 18. Nping Reference Guide | Nmap Network Scanning, https://nmap.org/book/nping-man.html#nping-man-echo-mode (accessed Oct. 6, 2023).

[4] hotpatatata, “31337/TCP open elite o\_o,” Reddit, https://www.reddit.com/r/cybersecurity\_help/comments/12oycc2/31337tcp\_open\_elite\_o\_o/ (accessed Oct. 6, 2023).