**Assignment 4 – Network Security**

Nathan Ketterlinus

Fisher College of Science and Mathematics

Towson University

Towson, United States

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

**Assignment 4 – Network Security**

1. ‘Network security’ often used interchangeably with ‘cybersecurity’? Why? Do you agree? Why or why not – write a minimum 500 words.

Network Security is often used interchangeably with cybersecurity because it is a subcategory of cybersecurity. IBM defines cybersecurity as “any technology, measure or practice for preventing cyberattacks or mitigating their impact” [1]. Contrarily, Cisco defines network security as “the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft” [2]. Personally, I don’t mind the mix-up, if there is no fundamental changing of the meaning of a statement. For example, advertising oneself as a cybersecurity expert, while only having relevant experience in network security can be misleading to prospective employers, which may be deemed as unethical behavior.

As addressed above, the main reason network security and cybersecurity are used interchangeably is because of their parent-child relationship. An important part of this notion is the fact that, while anyone who practices network security is simultaneously practicing cybersecurity, one who practices cybersecurity is not necessarily practicing network security. Cybersecurity can be thought of as the protection of any digital asset, including but not limited to personal computers, mobile phones, critical infrastructure, files, applications, and networks [1]. Network security, however, specifically focuses on the protection of a network, being critical of incoming and outgoing traffic. It protects the environment personal computers and mobile phones operate in, not necessarily the devices themselves.

Network security specifically involves the implementation of security tools such as firewalls, proxy servers, network segmentation, and the concept of minimum permissions to prevent common attacks and threats, such as DoS attacks, DDoS attacks, insider threats, viruses, worms, and trojan horses, among others.

Cybersecurity addresses all the threats that network security does. In addition, cybersecurity also must worry about things like social engineering attacks and ransomware. While these threats can exist in very specific contexts in network security, the wider scope of cybersecurity allows for these attacks to manifest in much more complex and varying forms. This requires cybersecurity experts to be much more vigilant in their defensive practices, as the different contexts various attacks can come in requires a much broader set of knowledge to effectively detect, as well as a wider skill set to effectively handle. In addition, one could argue that network security is primarily focused on preventing or mitigating attacks, not necessarily handling the aftermath of a successful attack, unlike cybersecurity, which provides clear-cut standards on what best practices are for cleaning up any exploited system.

Another important thing to consider is the relative value and meaning behind various certifications in the industry. Certifications exist for network security, but they also exist for other subcategories of cybersecurity. By using cybersecurity interchangeably with network security, the relative value and meaning of these certificates may become less clear to those unfamiliar with them. Although not necessarily a very common scenario, there may be an uneducated hiring manager that sees a that a candidate has a certification for penetration testing or some other relevant cybersecurity skill, then hires them to be a network security engineer, where they are not as equipped to be effective as someone with a more network-focused certification.

1. List and describe each of the layers of the TCP/IP Model. Also list each layer in the table below.

The 4 layers of the TCP/IP Model are the:

1. Application Layer: handles “end-to-end communication and error-free delivery of data” through protocols like HTTP/S, SSH, and NTP [3]. It provides the end user their product, while hiding all the nitty-gritty parts of how their product got to them in the first place.
2. Transport Layer: “exchanges data receipt acknowledgments and retransmits missing packets to ensure packets arrive in order and without error” through the TCP and UDP protocols [3].
3. Internet Layer: “responsible for routing packets of data from one device to another across a network” using the IP (both IPv4 and IPv6), ICMP, and ARP protocols [3].
4. Network Access Layer: combines functionality of the OSI model’s data link layer and physical layer [3].
5. List and describe each of the layers of the OSI Model.

The 7 layers of the OSI Model are the:

1. Application Layer: allow various applications to access a network and displays received info to an end user [4].
2. Presentation Layer: “The data from the application layer is extracted here and manipulated as per the required format to transmit over the network” [4].
3. Session Layer: “responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security” [4].
4. Transport Layer: “responsible for end-to-end delivery of the complete message” as well as providing acknowledgement for successful delivery and retransmitting data with an error [4].
5. Network Layer: handles packet routing and transmission between networks [4].
6. Data Link Layer: “responsible for the node-to-node delivery of the message”, while keeping the data error-free [4].
7. Physical Layer: “responsible for the actual physical connection between the devices” [4].
8. What is the difference between TCP/IP and OSI models?

The TCP/IP model combines the OSI model’s application, presentation, and session layers into the application layer, and combines the data link layer and physical layer into the network access layer [3].

For each of the terms below – describe it and write it at the correct place on the table (see examples below). User your book and/or web for resources.

1. Ethernet Cable
   1. A type of cable that connects devices to each other or to a larger network of devices.
2. Optical fiber
   1. Another type of cable which transmits binary data through beams of light, which is much faster than other kinds of cables.
3. WIFI

Utilizes radio waves to enable high-speed communication between devices over long distances.

1. Radio waves

A type of low frequency wave which can be transmitted across long distances without much signal degradation.

1. Packet

A unit of information communicated between two systems. Contains relevant information about source, destination, protocol, packet number, etc. that the end system can use to interpret the packet. Useful for breaking down large objects, like HD videos or large images, into smaller, more manageable chunks for a network.

1. MAC

Short for Media Access Control, uniquely identifies a device on a network, allowing traffic within a network to be properly routed [5].

1. ARP

Short for Address Resolution Protocol, ties a device’s volatile IP address to its stable MAC address for consistent communication within a network [6].

1. IP address
   1. A unique number assigned to every device which allows traffic to be properly directed to the correct device across different networks. Similar to how every building has a unique street address for mail.
2. IP spoofing

An attack in which packets are sent with a modified source IP address, impersonating a target machine.

1. ARP Cache poisoning

“a type of malicious attack in which a cybercriminal sends fake ARP messages to a target LAN with the intention of linking their MAC address with the IP address of a legitimate device or server within the network. The link allows for data from the victim's computer to be sent to the attacker's computer instead of the original destination” [6].

1. Router

A device which decides the best way to forward packets between networks so that they reach their target destination quickly while also balancing traffic.

1. UDP

“User Datagram Protocol (UDP) is a communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet. [7].

1. SYN flood
   1. A form of DoS attack where a server is flooded with packets containing a SYN(chromize) flag, but never a SYN/ACK(knowledge) flag, causing the server to idle.
2. Port scanning
   1. A form of reconnaissance in which all possible ports on a machine are scanned to gain information about which ports are open and which are inaccessible due to firewall configuration settings.
3. Port

“A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection” [8].

1. NMAP

NMAP is a piece of software noted for its ability to scan the ports of a target system.

1. Ping

A basic message is sent to a target machine, which sends a message in return. Often used to test if a machine is reachable and able to respond to requests.

1. Ping of Death
   1. A DoS attack in which a target system is flooded with too many ping requests for it to handle, rendering it useless while pings continue to be sent.
2. Firewall
   1. Controls incoming and outgoing network information by limiting port access to certain protocol types (or no traffic at all).
3. Session hijacking
   1. Taking over a user’s connection with a server by tricking the server into thinking a malicious actor is the user.
4. SSL

Short for Secure Sockets Layer, is a protocol which protects information shared between a user and a server.

1. TLS

An updated, more secure version of SSL.

1. SSH

Short for Secure Shell, allows users secure, remote access to devices over a network.

1. HTTP
   * 1. Short for Hyper Text Transfer Protocol, allows websites to display stylized content to users.
2. HTTPS

Short for Hyper Text Transfer Protocol Secure, is a more secure form of HTTP.

1. Digital key

Assuming this is the same as an encryption key, allows encrypted data to be returned to plaintext.

1. FTP

Short for File Transfer Protocol, is a protocol which describes how to transfer files from one computer to another across a network.

1. IDS

Short for Intrusion Detection System, is a preventative measure designed to analyze network traffic and flag any suspicious behavior.

1. IPS

Short for Intrusion Protection System, is like an IDS but is also able to prevent access to suspicious actors automatically.

1. Trojan horse
   1. A form of malware that is disguised as beneficial software to entice users to download and run, activating a malicious payload.
2. Physical security
   1. The act of securing any physical data and devices, especially those that contain sensitive information, or allow access to sensitive information, like printed health records or a notebook of login information.
3. Eavesdropping
   1. Synonymous with sniffing, refers to intercepting packets and learning/ stealing/ modifying information on the packet, before either sending the packet to its original target or any malicious actor.
4. Switch

Connects various computers to a network, and sends received packets only to their destination.

1. Flooding attacks

A type of DDoS attack in which a server sent too many packets for it to handle, rendering the server unavailable.

1. ARP spoofing

“a type of malicious attack in which a cybercriminal sends fake ARP messages to a target LAN with the intention of linking their MAC address with the IP address of a legitimate device or server within the network. The link allows for data from the victim's computer to be sent to the attacker's computer instead of the original destination” [5].

1. WPA2

“Wi-Fi Protected Access 2 is an encrypted security protocol that protects internet traffic on wireless networks. The second-generation of the Wi-Fi Protected Access security protocol, WPA2 addresses earlier flaws and offers more powerful encryption. Since its introduction in 2004, it has become the standard for Wi-Fi network security” [9].

1. VLAN

Short for Virtual Local Area Network, “A virtual local area network (VLAN) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network” [10].

1. Encryption

The act of preventing unwanted access to data by passing it through a typically mathematical process that (hopefully) only authorized users can reverse.

1. IPv4

Short for Internet Protocol version 4, can handle 2^32 addresses.

1. IPv6

Short for Internet Protocol version 6, can handle 2^128 addresses, while also including security features not found in IPv4.

1. IPSec

Short for Internet Protocol Security, addresses security concerns of IPv4, like IP spoofing.

1. VPN
   1. Short for Virtual Private Network, allows remote systems access to a network by encrypting traffic between the two over the internet.
2. Access control list

“Made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access” [11].

1. Segments

A segment is used as a unit of information sent over the transport layer.

1. DNS
   1. Short for Domain Name System, converts IP addresses into readable names, like [www.google.com](http://www.google.com)
2. DNS Spoofing
   1. An attack in which a DNS server is tricked into redirecting end users to a malicious site instead of the intended website.
3. DoS
   1. Short for Denial of Service, a form of attack where a single computer floods a server with requests to prevent authorized users from legitimate access.
4. ICMP

Short for Internet Control Message Protocol, is a protocol which allows network devices to send error messages and operational info to each other.

1. Malware
   1. short for malicious software, any piece of software designed to cause damage, harm, or otherwise cause any unintended behaviors.
2. DDoS
   1. Short for Distributed Denial of Service, a form of DoS attack where several computers flood a server with requests to prevent authorized users from legitimate access.
3. Zombie

A computer controlled by a 3rd party for malicious intents, like DDoS attacks.

1. Botnet
   1. A network of zombies, controlled by a 3rd party.
2. Onion routing
   1. a method of transmitting data by bouncing it between various intermediary hosts, all of which only know the host before and after them, thus hiding the end user’s identity.

Not quite sure how to fill out this table, the instructions were a bit vague. I tried my best, sorry if its not what you were looking for!

|  |  |  |  |
| --- | --- | --- | --- |
| TCP/IP Model | Components (tangible) /protocols | Vulnerabilities | Attacks |
| Data Link | Optical fiber | Port Scanning | IP Spoofing |
| Network | Ethernet Cable | NMAP | ARP Cache Poisoning |
| Transport | ARP | Firewall | SYN Flood |
| Session | Router | Physical security | Ping of Death |
| Physical | UDP | Zombie | Session hijacking |
| Presentation | TLS | Botnet | Trojan horse |
| Application | SSH | Encryption | Eavesdropping |
| Packet | HTTP | IPv4 | Flooding attacks |
| Ping? | HTTPS | IPv6 | ARP spoofing |
| Port? | FTP | IP Address | DNS Spoofing |
| VLAN | IDS | Wifi | DoS |
| VPN | IPS | Radio Waves | DDoS |
| Segments | Switch | Access control list |  |
| Onion routing | WPA2 | Digital Key |  |
|  | IPSec | MAC |  |
|  | DNS |  |  |
|  | ICMP |  |  |
|  |  |  |  |

1. Wireless networks function on many of the same principles discussed in class. Study https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network and go through the steps to ensure that your home or a friends wireless network is secure. Provide here a log of the steps you took and explain why you took them.

As a precursor, I live on campus and use campus wifi. As such, I do not have access to routers and a lot of these tips may already be enforced by the university.

1. My connection already utilizes WPA2-enterprise.
2. I do not have appropriate access to change my router’s default settings.
3. I cannot keep my router up to date.
4. I cannot disable “remote management”, WPS, or UPnP features.
5. Towson already has TU-openaccess as a guest network.
6. I do not have an administrator log-in, and as such cannot log out of an administrator account.
7. I have custom rules defined in my windows defender firewall on my pc, but I cannot enforce firewall rules on the router, as I do not have access to it.
8. All the devices I regularly use automatically patch themselves with new OS and software updates, they require password access to log onto, and are in a secure location physically, limiting the chance that anyone can tamper with them against my knowledge.
9. Create a brief ‘tip sheet’ to give to your friends and family on being secure on public WiFi networks (like on an airport). Along with tips, give a small explanation on the consequences of not taking security precautions on public networks. (One page minimum)

Using public wifi networks is an inherently risky behavior for most users. There are various threats present that all stem from the issue of not knowing who else is listening. These threats range from Man-in-the-Middle attacks, where a malicious actor can either listen in on a conversation or actively disrupt your communication entirely, to the theft of personal information (even more so than private networks). However, there are steps users can take to promote security in their use of public wifi, limiting exposure to possible attack vectors.

Some of the tips that Norton (a company specializing in computer security) recommends includes:

* Avoid accessing sensitive info [11]. If nothing compromising is ever seen or communicated, then there’s no way anyone secretly listening in can steal it.
* Stick to HTTPS websites [11]. HTTPS is short for Hyper Text Transfer Protocol Secure, which is different from regular HTTP. The S means that any data transmitted is encrypted, making it virtually impossible for it to be intercepted. Depending on the browser, HTTPS websites typically have a padlock next to them in the address bar, letting users know they are secure.
* Use two-factor authentication (2FA) [11]. 2FA is useful because it requires users to have access to both login info and a physical trusted device. In the case someone does end up stealing a password, 2FA prevents them from stealing your account. The only realistic case in which an attacker would be able to get around 2FA would be if they stole both your login info and the device linked to your 2FA, which is much more improbable. As a rule of thumb, users should enable 2FA on any platform that supports it. There are applications like Authy which exist to manage all of a user’s 2FA connections for them too!
* Keep your operating system (OS) up to date [11]. Groups that make OS’s frequently put out security updates for their platform, patching out security vulnerabilities for users. If these vulnerabilities are never patched out, then they remain as possible attack vectors for malicious actors, compromising the security of a device and increasing the likelihood of backdoors, viruses, or worms being successfully installed in an attack.

References

[1] “What is cybersecurity?,” IBM, https://www.ibm.com/topics/cybersecurity (accessed Sep. 30, 2023).

[2] “What is network security?,” Cisco, https://www.cisco.com/c/en/us/products/security/what-is-network-security.html (accessed Sep. 30, 2023).

[3] GeeksforGeeks, “TCP/IP model,” GeeksforGeeks, https://www.geeksforgeeks.org/tcp-ip-model/# (accessed Sep. 30, 2023).

[4] GeeksforGeeks, “What is OSI model: 7 layers explained,” GeeksforGeeks, https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/ (accessed Sep. 30, 2023).

[5] “What’s a MAC address and how do I find it?,” Technology Services, https://slts.osu.edu/articles/whats-a-mac-address-and-how-do-i-find-it/ (accessed Sep. 30, 2023).

[6] “What is address resolution protocol (ARP)?,” Fortinet, https://www.fortinet.com/resources/cyberglossary/what-is-arp (accessed Sep. 30, 2023).

[7] L. Rosencrance, G. Lawton, and C. Moozakis, “What is User Datagram Protocol (UDP)? definition from searchnetworking,” Networking, https://www.techtarget.com/searchnetworking/definition/UDP-User-Datagram-Protocol (accessed Sep. 30, 2023).

[8] “What is a computer port? | ports in Networking | Cloudflare,” Cloudflare, https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/ (accessed Sep. 30, 2023).

[9] D. Ghimiray, “What Is WPA2 (Wireless Protected Access 2)?,” What is WPA2 (wireless protected access 2)?, https://www.avg.com/en/signal/what-is-wpa2 (accessed Sep. 30, 2023).

[10] “What is VLAN (virtual lan)? - it glossary,” SolarWinds, https://www.solarwinds.com/resources/it-glossary/vlan (accessed Sep. 30, 2023).

[11] C. Stouffer, “Public wi-fi: An ultimate guide on the risks + how to stay safe,” United States, https://us.norton.com/blog/privacy/public-wifi (accessed Oct. 2, 2023).