# Transcript: IT Podcast - Ep 113 - C836 Lesson 10 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU 's IT audio series, flexible, portable, profound.

Hey, everybody. This is Arthur with WGU. I'm one of the course instructors for C 836, Fundamentals of Information Security, and a quick note before we get started. This series is meant to enhance the learning material and not meant to replace it. This is Chapter 10. Let's go ahead and get our notes together for this, because this particular chapter is technology driven and very acronym heavy.

Let's go ahead and get started. Protecting networks. Proper network design provides us with one of the cheap tools that we need to protect ourselves from the variety of threats that we might face. A well configured patch network is the foundation of any security program. With a properly laid out network, we can prevent some attacks entirely, mitigate others, and if nothing else, fail gracefully. Here are some of the tools that we use to defend our networks. Pardon me.

In no way is this a comprehensive list. This is just some of the tools that we can use. Network segmentation, firewalls, IDS, IPS, wireless secure protocols, VPNs, secure protocols, Mobile Device Management, MDM, port scanners, packet sniffers, and the controversial honeypot. Network segmentation and firewalls. Network segmentation is when a network is segmented, we divide it up into smaller networks, each acting as its own small network called the subnet. We can control the flow of traffic between subnets, allowing or disallowing traffic based on a variety of factors, or even blocking the flow of traffic entirely, if necessary. Firewalls are a mechanism for maintaining control over the traffic that flows into and out of our networks. Firewalls naturally create network state, and that's when installed.

Firewalls and DMZ. These are the different types of firewalls that you could deal with in the field. Packet filtering, stateful, deep packet inspection, proxy servers, and demilitarized zone, or DMZ. Now, DMZ is not a firewall, but it's a segment that the firewall creates. Packet filtering is the oldest of the firewall technologies. It just filters packets based on the source, destination of the IP address, and the protocol port number being used. Stateful firewalls create a tracking table where it tracks the flow of the information connection starting from the inside of the network to the outside. It keeps this table, updated, and it closes out the connections as traffic it's stopped. Deep packet inspection is where it goes one step further than stateful firewalls.

Not only does it keep the table that's created, but it also gets down and sees the actual content that's flowing in and out of each packet. Proxy servers can serve as a check point to allow us to filter traffic. In other words, the proxy server acts as a legitimate middleman, not a man-in-the-middle attack, but a middleman in our networks for the end-user, goes to the proxy server. The proxy server requests the desired traffic based on the end-user. A demilitarized zone is like I said earlier, it's a special zone that is created where it's a lower trust zone than the internal network. But it's a higher trust zone than the inner network or external network. This is where we would put our mail servers, web servers, or anything that needs to communicate with the Internet on a daily basis.

But we don't need to have it on our internal network. Intrusion Detection, IDSs. An IDS perform strictly as a monitoring and alerting tool to notify us that an attack or undesirable activity may be taking place. IPS actually takes action based on what is happening in the environment and it's response to the attack. The difference between IDS and IPS is IDS notifying is not an action, IPS actually goes and blocks the particular traffic that is going on. Signature-based IDS and IPS works very similar to that of most anti-virus systems, where it comes down, you get the signature that matches the undesirable traffic. The IDS, IPS method blocks it based on the signature that's there. Anomaly-based takes a little longer than signature in order to configure the baseline of the network to see what's going on.

There are more positives with anomaly-base, but with anomaly-base, it can actually stand up against zero-day attacks, which are attacks that have no signature for. It sees it as something undesirable going on on the network.

The impact of intercepted data. Now, to understand the impact of intercepted data, all you have to do is look at the news. There are breaches in the news. Unfortunately, almost daily now. This is just the world we live in. But a couple of these items here can actually help us improve or lower our risk of dealing with intercepted data. One of the most common concerns when we are sending sensitive data over, the network is having data intercepted by someone else and having it misuse. Given that many networks are available today in offices, hotels, coffee shops, restaurants, and other places, the opportunity to accidentally expose data to danger is very large. I want to say this to you. For those of you that still use open public Wi-Fi, I would recommend that you stop in my professional opinion.

I would say go through the process and get an unlimited data plan for your mobile carrier that allows you to do some hotspotting. That will allow you to connect your wireless devices directly to that. That will lower that risk for you in your own personal lives. If that is still too expensive for you, I would recommend buying a VPN service and connecting to that VPN when you get on these open networks before you transfer any sensitive data.

Wireless networks security. For legitimate and authorize users on our network are cheap method of protecting traffic flows in the term, we use encryption, encryption used by A2.11 wireless devices is most commonly given to the families of three major categories, WEP, which is deprecated, WPA, which is also deprecated, and WPA2, which is the current standard.

Wireless exposure. Wireless networks. In particular one of the major risk. We consider places where data might be exposed at free Internet access that is commonly provided in a number of places. Just like I referenced before it let's try to minimize the risk of data exposure. VPN is the use of private virtual networks that can provide us with a solution for sending sensitive traffic over unsecured networks. Sensitive traffic over unsecured networks, keyword there.

A VPN connection is often referred to as a tunnel and is encrypted connection between two endpoints and one of the simplest ways to protect our data is to use secure protocols. What that means is, instead of using just common HTTP to send clear text traffic, we use HTTPS, which is encrypted with TLS.

Mobile devices? A mobile device is any device that communicates via a wireless medium. MDM is a Mobile Device Management and a MDM is basically for any device that doesn't come with Windows, OS X, or Linux operating system that has a centralized management area for Windows as a Active Directory. With this MDM, we can actually force users to comply with certain standards before accessing sensitive information. For example, making sure that passwords are set on our devices, making sure that the devices are up to date and patched, and that there is a certain time interval between our password changes. Mobile device management is just for those devices that fall outside of the major operating system categories and with MDM it goes into BYOD, bring your own device. This is often brought up and discussed with mobile device security. There is a huge cost savings for any organization with BYOD but there has to be some policy and procedures that are set in place before you can have users bring their own devices to work on sensitive data and this goes back to that mobile device management.

Here are some network tools. Wireless tools that are here before attackers use to access Wireless devices and potentially bypass all of our carefully planned measures. The two devices that I really want to bring up here are, Kismet, is commonly known for detecting rogue Wireless access points when they attempt to pop up on your network and Netstumbler, which is available for Windows but is not as full of a feature set is Kismet.

Port scanners are scanners that are one of the mainstays of the security community, sorry. Assess how our devices' ports are open and they break off into two categories, port scanners to let you know which ports are open and vulnerability scanners, which actually lay out the vulnerabilities that are listed with those ports.

Nmap, short for network mapper, one of my favorite tools. Although Nmap is generally referred to as a port scanner, it does a great disservice by doing that. Nmap can conduct port scans, search for other hosts, identify operating systems that are running on the host, detect versions, and all that. Nmap is like the Swiss Army knife of network tools and it is absolutely free. I think it's nmap.org and you can go there and download it yourself.

It is an amazing tool. Nmap is the command-line version, zenmap is the graphical version.

Packet sniffers. A network protocol analyzer is also known as a packet sniffer or just plain sniffer, a tool that can intercept traffic commonly referred to as sniffing. Sniffing basically amounts to listening to any traffic that is on the network interface between our computer and any other device that we are looking at. Wireshark. Again, another fantastic free tool is a graphic wireless packet analyzer.

If you haven't yet, I would say download and play with Wireshark. Tcpdump is the command-line interface for Linux and Unix operation for this tool. Wireshark and tcpdump do the exact same thing. It's just that Wireshark has a nice, pretty graphical overlay. Honeypots, highly contradicting statement and controversial. There we go, that's the word I'm looking for. Highly controversial term of network tools because it can detect and monitor and sometimes tamper with the activities of an attacker. The reason why these are so controversial is that you have to move with legal's presence on this because Honeypots can be the difference between entrapment and enticement for an attacker.

If you're just studying them, make sure that for Honeypots you always go through the steps necessary with any legal department and HR to protect yourself and the organization.

Last but not least, we'll bring it out firewall tools is HPing3. HPing3 is a handy little tool that can specially craft ICMP packets to evade normal measures of a firewall and to test their vulnerabilities and see what it is. This can be used for firewalls, IDSes and IPSes. This particular tool crafts packets that you normally would not get.

You can see how your firewall would react or allow traffic depending on what's going on with that particular vulnerability in that way you can then patch that vulnerability or change your firewall rules based off of that. This has been Arthur Moore with C836. You have a nice day. Again. I appreciate you stopping by and listening to this audio series on C836, Fundamentals of Information Security and with this, I would challenge you to contact your course instructors if you're having any issues within the course and apply these concepts to your daily lives and they will flow a lot easier. Thank you very much, and have a nice day.

Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.