Types of Vulnerabilities

William H. Wolfe II **(12 mins)**

Specifics about WEP Vulnerabilities. Static-WEP uses an RC4 algorithm, and there's a standard 24-bits what's called Initialisation Vector, that is selected and keys do not rotate. Therefore, it's extremely simple to get a WEP packet, run it through a variety of different tools and be able to actually compromise that WEP key in under 15 minutes. There are some examples that you can find on the web and YouTube that actually perform this function much quicker using some of the typical tools made available in Kali.

The Static-WEP does not protect the wireless LAN user integrity and that means that we can have replay attacks, or bit flipping attacks.

WEP shared key authentication is also flawed in the sense that the access point challenges the client to ensure the possession of a valid encryption key and an attacker can actually infiltrate that particular process and obtain the key stream so they end up with the cipher text, XOR, or 'exclusive or' with the plaintext challenge, and they can receive the key stream.

Man-in-the-Middle attacks pose another threat to networks because I can now force the client off the intended network, and force them or lure them to associate them to a rogue network. So I might have a rogue access point that I want them to associate with, and a Man-in-the-Middle attack will allow that to occur.

It's very easily done because we have MAC Address Spoofing, the rogue device setup, denial-of-service attacks and makes for very easy sniffing and war driving.

Rogue devices - we spoke about these earlier is any device that is sharing the RF environment but it's not managed by you. So an employee going out, purchasing their own wireless router, plugging it into the network in the office and providing a SSID so that they can connect their laptop. That would obviously be against security policies for the company, but it would also be considered a rogue device.

Rogue devices as we saw earlier can either be wired or over the air. Rogues are dangerous because they can be set up to have the same extended Service Set Identifier as opposed to the unique SSID as your network and therefore, if I can cause you to associate to my rogue AP on the same SSID that you trust, I can now place you into an environment that's a honeypot, where now I can get additional information because you trust me.

What do we need to do to help break this malicious intent? We need to be able to classify the traffic. We need to do to be able to classify a rogue device. We need to be able to detect bad or malicious traffic, or non-managed traffic. We need to report it, and we need to track it, and in some cases with advanced capability we actually have a rogue containment where we can actually shut down or contain the rogue device from having any effect on our network.

Rogues can be perpetrated by insiders, which is most likely the case, or a malicious hacker. Most of the time you will see insiders creating the rogue AP environments.

Dictionary attacks - that we spoke about earlier. Basically a dictionary is a database file that contains variations of the passwords. Some people refer to these dictionary attack tools as utilizing files that contain rainbow tables. Weak passwords can easily be cracked by standard dictionaries. Complex passwords can also be cracked by way of using rainbow tables even if the passwords are protected by a encryption or coding hash process. It just takes a little bit longer for the dictionary attacks to take place.

We spoke about MAC address spoofing. Again, MAC address spoofing will allow us to inject packets into the wireless network from a client device that has been authorized based upon MAC filtering. So now I look like that authorised device.

Wireless sniffing - there's good and bad just like any packet capturing. Most of the time, packet capturing is used to help diagnose or isolate significant technical problems on a network, but that same tool can be used for bad, just as easily as it can be used for good.

Denial-of-service attacks. RF jamming specifically either intentionally or unintentionally, an RF transmitter in the same frequency range or band as the wireless local area network can in fact disable access to the network. Now, as I mentioned, denial-of-service attacks are also perpetrated by management frame manipulation, and management frame protection can help mitigate this.

We can also have problems with misuse of the spectrum. We can silence the wireless network by flooding it with a Request-to-Send and Clear-to-Send frames, and again we can have authentication floods and dictionary attacks which will overload the system causing unnecessary processing and essentially, over-subscribe the CPUs and the processing capability within the access points, or in cases such as Cisco WLAN controller environment or cloud-based wireless such as Meraki and Aerohive. These overloading of the systems could in fact take place.

The 802.11 environment as specified by the IEEE as the wireless group have a number of standard Layer 2 exploits that can be made visible by tools such as Dsniff, Nmap and other tools. We'll take a look at some of the most common tools here in just a little bit.

Penetration testing. The Metasploit project.

We have application security problems, malware just like we have in a wired environment. We can have malware on our devices, and it can affect the wireless environment. In fact, some malware could be written in such a way that it is very specifically going to impact the wireless environment and not the wired environment. So, very specific attack vectors for wireless.

In summary, before we cover a couple of additional topic areas. Wireless LANs are very easy targets today. Everyone is using wireless. Wireless is becoming pervasive, very rare that you see anyone actually connected with a wired connection today unless they're on a desktop because we all like to be mobile. We'll all be using our smart devices, our tablets.

Passive SSID probe sniffing and WEP attacks are just the beginning or the first stage of wireless LAN exploits. So again, security by obscurity by turning off the broadcast SSID doesn't necessarily help us because we can still sniff for the probes frames.

WEP, the key attacks are far and few between today since most people are not using WEP.

Sophisticated wireless LAN exploits are generally tied to management frame manipulation or crafted management frames.

In the end if the attacker can gain access to the wireless network, it can launch a variety of higher-layer exploits over that media, and since the wireless LAN is ultimately an extension of the wired LAN, those exploits can take place in the wired environment, and therefore have an effect on the entire infrastructure of your network.