IT 125-41194

Alex Arnold

4-07-25

Lab 10

**Research Cisco's Email Security Appliance. In your own words, (no copy & paste) write a paragraph on what you learned.**

Cisco email security appliance is a product that is designed to protect form email based threats. These include things such as malware attached to emails, spam, and phishing attempts. This is done through content scanning (reviewing the email file for malicious code, viruses and so on), reputation filter (databases of known untrustworthy sources / domains), and spam detection (I am assuming it is some form of content scanning for characteristics matching phishing and other text based threats.). The data for reputation filtering, phishing defense and malware defense all seem to come from Cisco Talos who is a cybersecurity subsidiary of the main Cisco company.

**Research Cisco's Web Security Appliance. In your own words, (no copy & paste) write a paragraph on what you learned.**

The Web Security Appliance is another device (can also be deployed as a VM) that secures an enterprise business network. This device though is the gateway for web traffic vs email traffic. This device allows for website filtering / blocking (preventing employees from accessing things like social media), set acceptable use policy controls (related to the previous item), detailed reporting on web traffic and security events (I wouldn’t want to have to much of the web traffic as it can become a legal issue as well and also cause headaches if the company collects info that they have to report users for), and lastly there is security tailored for mobile devices in particular. This system seems to use a similar reputation system that I would bet is also managed by the Cisco Talos company.

**Research Cisco Talos. In your own words, (no copy & paste) write a paragraph on what you learned.**

Cisco Talos is Cisco’s Security and threat intelligence organization. They are the research team that identifies, analyzes, and responds to cyber threats that Cisco has detected. They are the ones that provide the databases that power the Reputation systems, scans for known viruses and malicious code as well as phishing attempts. My Insite (from working at Barracuda Networks) is that the protection devices phone home about any data that they capture as well as having honeypot devices that are set up to purposely gather potentially harmful emails and scan for potentially harmful websites. This data then is reviewed by Talos and then added to the databases of domains, harmful code, and other digital signatures that they can match to protect clients.

**Choose one of the six attack categories discussed in the book. (MAC Table, VLAN, DHCP, ARP, Address Spoofing, STP) In your own words, (no copy & paste) write one paragraph describing the details of how one of the attacks in that category works, and one paragraph describing the mitigation technique for that attack.**

A MAC Table attack is also known as a MAC flooding attack. This attack consists of an attacker overloading a switches MAC Table with fake MAC addresses. This then causes the switch to send traffic to all ports instead of the correct port. In doing this the attacker can then be listening on one of the ports for the data allowing them to intercept it and potentially gain unauthorized access to the systems and services. The overflowing MAC table causes the switch to go from unicast forwarding mode (one recipient) to broadcast mode (send data on all ports). This kind of attack is difficult to detect at the early stages without proper monitoring inplace. It is only when the traffic begins to degrade the networks performance and peoples network speeds that is will be noticed. At which point the attacker could have already gathered valuable data. Besides data gathering this can also be used as a form of Denial of Service attack by overwhelming the switch and disrupting network traffic vs a direct attack on a server or service.

In order to Mitigate this form of attack administrators can use Port security, VLAN segmentation, DHCP Snooping, Dynamic ARP inspection, ACLS (Access Contril Lists), and have alerts set up on the manages switches. Port Security allows the administrator to set a specific number of MAC addresses that can be allowed per port (this can both restrict the volume of MAC addresses and alert when the limit is reached.). VLAN segmentation will limit the scope of the attack to only a specific subsection of the network reducing the potential impact. DHCP snooping can assign trusted and untrusted ports preventing a rogue DHCP server from being added from an untrusted port. ACLs restrict traffic based on ip or MAC address thus creating a kind of white list that tells the switch who is allowed to send data. Regular monitoring and alerts will help to notice these kinds of issues early on and prevent things from getting out of hand. Using all of these different tools will help to increase the security of the network and prevent issues before they become an issue.