ISEC 325 Homework 07

Answer the following questions based on your reading of the text books, the module key points, and the instructor's presentation this week.

1. [2 points] What are some of the considerations to be considered when capturing network traffic?

   Capturing network traffic can be illegal so you must have authorization.

   You must be certain that the sniffer is placed in the correct spot in your network. If you wanted to capture traffic between your outgoing firewall and DMZ it would do you no good if you were sniffing traffic on the internal side of your inner firewall between the firewall and any subnets.

   You have to be careful on how your sniffer is connected to the network things like switches are intelligent enough that it routes traffic to specific MAC addresses which means if you were using a laptop for instance that it would not route the traffic to you. Newer switches have a port that allows you to connect and sniff network traffic. The book suggests installing a hub as well because hubs are not intelligent, I would be concerned with this however because hubs can be a security issue.

   The sniffer cannot decipher encrypted traffic.

2. [3 points] Define intrusion detection, intrusion prevention, and incident response. How are the three ideas related to one another?

   Intrusion detection is exactly what it sounds like you would have a system in place to recognize intrusion by unauthorized persons, intrusion prevention takes it a step farther and allows you to block ips or deter an intrusion. Whether you are utilizing intrusion detection or prevention you should be alerted to unauthorized persons and you would then have an incident response which would first be to get the intruder out of your system and then block them. Incident response would then entail figuring out how you were breached and then fixing that condition.

3. [2 points] How does a network-based IDPS differ from a host-based IDPS?

   A network based IDPS is placed on a computer or appliance that is connected to a segment of an organizations network and then monitors traffic on that network segment watching for outgoing or successful attacks. It looks for patterns in network traffic. It can detect more types of attacks than a host based but it also requires much more maintenance and a complex configuration. Advantages of a network-based system are that they are cheaper and can provide more coverage than the host based system, if they operate in detection-only mode they can be deployed in existing networks with little to no disruption of network operations, and they are not usually susceptible to a direct attack. The disadvantages are they can be overwhelmed by heavy traffic and can fail to catch attacks, they require access to all network traffic to be monitored, they cannot analyze encrypted packets, they cannot ascertain if an attack was successful or not, they cannot easily discern some forms of attacks that involve fragmented packets.

The host based IDPS will reside on a computer or server which is called the host. The host-based system will watch only that host. Host-based systems are known as system integrity verifiers because they will monitor and benchmark the status of system files and can detect when an intruder modifies, creates or deletes files on that system. The host-based system has an advantage over the network-based system in that it can decipher encrypted data. The host-based system only needs to make decisions on its host-based system which can make it effective and reliable. Advantages of the host-based system are that it can detect attacks that a network-based system may not see and can detect local events as well, since it functions on a host system encrypted traffic will have been decrypted, switched network protocols don't affect it because it watches the traffic to its host system only, it is possible for the host-based system to detect things like trojan horse programs because it can detect inconsistencies in how applications and programs were used. The drawbacks of a host-based system are that the host-based system poses more management issues because they have to be configured and managed on each host they are placed on, they are vulnerable to direct attacks and attacks made on the host operating system, it is not designed for multi-host scanning and cannot detect the scanning of network devices, it can be susceptible to denial of service attacks, can use large amounts of disk space for it's logs, and can reduce the performance of your system.

4. [2 points] How does a signature-based IDPS differ from a behavior-based IDPS?

   Signature-based IDPS looks for patterns that match known signatures, signatures are predefined and predetermined attack patterns. Attacks that have distinct patterns are foot printing and fingerprinting activities, exploits and denial of service attacks.

   A behavior based IDPS works off statistical information. It is set up by monitoring normal network traffic which it then uses as it's baseline it then periodically reviews network traffic comparing it to the baseline when the statistical number gets to it's setpoint it sends and alert to the administrator. It has an advantage of being able to detect new attacks because they can look abnormal.

5. [2 points] What is a monitoring (or SPAN [switched port analyzer]) port? What is it used for?

   It is a special port set up on a switch that will allow you to place your device on the network so that you can use a packet sniffer or do packet monitoring. A switch is an intelligent device that uses MAC addresses so that if you place your device anywhere after the switch you will only see the packets in the segment that you have placed the device on. By placing your device on the SPAN port, you can then see all the traffic going through the switch.

6. [2 points] What is active intrusion prevention, and how does it differ from passive?

With an active intrusion prevention system, the IDPS is set up to automatically block suspicious activity without an operator, it provides a real time response to suspected attacks. A passive intrusion prevention system is set up to analyze network traffic and send alarms either audible, visual or even text messages or emails.

7. [2 points] From a security perspective, which is least desirable, a false positive or a false negative alarm? Why?

   A false negative is a bad thing to happen because it means that your IDPS failed to detect or react to a security event. A false positive although not desirable won't hurt your network but will waste time with investigation. You can even set your IDPS to not alarm on false positives.

8. [10 points] Research the open-source IDPS called "Snort." Write a summary of how Snort fits within the concepts presented this week (e.g. network vs. host, signature vs. behavior, detection vs. prevention, etc.) If a small office wanted to configure Snort for its use, how would you suggest implementing it? Where would it be on the network? How would you configure alerts or responses? I expect several detailed paragraphs and perhaps a diagram for this answer. Cite your sources.

   Snort is an open source IDS that would work well for a small business because it wouldn't carry the hefty price tag of some of the IDPS systems designed for businesses. Writing rules for it looks like it can complex so I would use standard rulesets that have already been developed like exploit a ruleset which looks for exploits against software, exploit-kit a ruleset that looks for exploit kit activity, malware-backdoor a ruleset that detects traffic on backdoor channels, malware-tools a ruleset that deals with tools that can be considered malicious in nature, and the rulesets that help detect attacks on various protocols until I became more familiar with the way it worked. Being new to IDPS systems I would place it behind my outer firewall before any switches that way I wouldn't have to deal with making sure any of my switches had a monitoring port so I would be able to monitor all the incoming packets. By putting it behind my firewall I would be able to see how effective my firewall rules are and change them if I needed to. Because it is placed behind my outer firewall it would be a network-based IDS placed on the incoming segment of my network. It would be an IDS because Snort is only designed for detection and not prevention which makes it an intrusion detection system. Being behind the firewall I would set it up to sniff traffic first so that I could establish a baseline for my normal traffic behavior. Then applying the rulesets, I would be able to use Snort as a behavioral based IDS looking for differences in normal traffic behaviors. Any traffic outside of the normal baseline I would have set for silent alerts to myself or the security team. You could then modify the rules depending on the false positives that you received in order to tweak it to make it more effective. You would need to keep working with it checking false positives and alerts. You would have a lot of work in the beginning combing through logs until you were able to be sure which alerts were false positives and which were true threats. I think you would need to start with a wide approach as well checking all the alerts so that you didn't incur any false negatives and hopefully none. I am not sure that that is the best set up for snort, but it is where

I would suggest to start. One of the cool things about snort is that it takes very little hardware requirements to run and just need a large storage drive for the logs it writes. Because it has a very low cost to run you could always set up another system with snort if the first one worked out or set up a completely new one if needed somewhere else like inside the outgoing firewall to sniff and detect bad behaviors coming from inside your network.

9. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you're still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

I really enjoyed this week's MEET session and reading material in IDPS systems it was something I wanted to learn about since I went to the Ohio Security Summit last year and listened to a group talk about SEIMs and how you really needed to keep up with them and work with checking false positives. Working with IDPS systems is something that interests me because it seems that they will be something that will be a part of network security more and more in the future. It seems like it would be gratifying if you were able to work with a system that did a good job protecting your network. I think I would like that more than policing users and looking for passwords on sicky pad sheets under their keyboards.

I had no idea that something like snort existed and is something you could really set up just to tinker around with if you had time, not that I have time right now. I know it exists and it could be something I remember and look to in the future if I were to work for a small company that can't afford a million-dollar cisco system. I can also definitely see what you are talking about when you say that security doesn't make anything cheaper or faster. I bet many organizations look at the security team as an enemy or something that is always getting in the way if they haven't ever suffered a breach. It would be no different than people that smoke knowing it is a leading cause of death but because nothing has happened to them, they don't need to worry about it. When they find out they have cancer from cigarettes then they are devastated. I am sure to some the security department may not seem necessary or too expensive until they suffer a breach and the company has a serious loss. The next convention I go to I will make sure I stop and talk to some of the reps for these systems and see if I can see them in action.

References

SNORT. (2020). Retrieved from snort.org: https://www.snort.org/

Snort System Requirements. (2008-2017). Retrieved from Flylib.com: https://flylib.com/books/en/3.100.1.199/1/

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.