Questions

Student’s Name

Institution of Learning

Questions

Question 1a. There are many problems which can be seen in this process. Firstly, one would like to say that reassembly is just a part of fragmentation, but it is not exactly the same. Intermediate devices do not reassembly, while intermediate routers can do that since they are able to fragment a single datagram. That is the main difference and the problem when it comes to reassembling processes with intermediate devices. One would like to say that reassembly on the final destination has many reasons for being implemented. Firstly, a router cannot see the entire message or all its fragments because fragments may use various routes in order to get to the destination. Secondly, this process increases complexity of using routers. Thirdly, it is essential to wait for the fragments and then send the reassembled message. It slows down the entire process which makes not reassembled routers work faster, sending all of the fragments quickly without hesitations, so the receiver gets them on time.

Nevertheless, there are still some problems like the fact that a fragment may be lost, and it would be impossible to get the entire message unchanged. Also, there may be a potential danger when utilization data link layer frame capacity between different routers.

Question 1b. In a situation then a sender (Host B) sends TCP fragments using out-of-order sequence number which is higher than it was expected; the receiver (Host A) cannot get these segments. Hence, the TCP/ IP protocol states about the inability of the receiver to perform the set task. Then, the segments are being sent to sender again with sequence that can receive them, and resend to receiver. This way, it is possible to send the data effectively.

Question 2. There is a way to detect APR spoofing attack, taking into consideration the many times it has been under similar attacks. The problem with APR lies in the absence of authentication. Hence, attacks on ARP often lead to LAN attacks which are more difficult to deal with. There is another problem concerning the fact that ways of dealing with spoofing attacks are usually passive with analysis of IP mapping or Ethernet which also takes a long time. Hence, it is difficult to discover, not to mention prevent, the attack. Thus, one would like to recommend an active technic while detecting ARP spoofing. In this method, it is required to inject ARP request along with TCP SYN packets. They should be injected into the network; this is done for inconsistency probe. It would increase the security level greatly, and it is also faster, although there are some weaknesses, such as difficulty while working with MAC when it comes to detecting IP addresses.

Question 3. FMS attack has been introduced and analyzed in 2001 (Fluhrer, Mantin, & Shamir, 2001). When speaking about this attack, one thinks of an attacker using the track of WEP protected network that may record encrypted packets. Thus, the attacker uses RST bytes that can be easily predicted. This way, the initialization vector is unprotected which gives the attacker an ability to get RST 3 bytes as well as keys to all packets.

The Chopchop attack is different from this one because the attacker uses it for decoding the last M bytes of text. This way, he or she can get the decoded packet. Nevertheless, the root key is not being revealed during an attack.

Hence, the Chopchop attack requires a four byte CRC32 being appended to the data before decoding. A four byte has a checksum ICV. Then, the packet that has P checksum is being used as an element for the polynomial ring F2. In case of correct checksum, P mod PCRC=PONE holds, and PONE and PCRC are polynomials which are known.

Question 4. This decision can achieve the main purpose of protecting routing modification attacks. After all, this choice allows guarding update messages, which are being routed between two symmetric key types distribution approaches. The first approach requires a centralized controller to have the needed keys in the BGP routers. After that, it is possible to call protocols. There is also another approach. In this case, there is no centralized controller. Hence, the needed keys are being transmitted to the BGP routers by AS.

One would also like to state that BGP's goal is to advertise the routing path info for IP prefixes, and in this case, BGP routers have to create TCP connections with different BGP. This way, it is possible to pass the information as update messages between BGP. Then, in case BGP router gets many paths with the same prefix, it is able to determine and pick the best one having its own criteria. It shows that the decision is an effective one, and it was a smart choice of the company. Although there may be minor issues with prefix advertisement, the benefits exceed the risks.

Question 5. Snort has a powerful detection system and that is the reason it is being rather popular among the users. It is being used for detecting and preventing systems from threats. Snort is free, so people can use it openly, and they are also able to apply various modifications depending on the network and devices they are using. Rule options in Snort are being divided using semicolons with parentheses. There are three parts that create an option such as option keyword, semicolon and option value. The latter is being used in order to give value to the option keyword that identifies the desired option. Semicolon is a toll for separating the value from the keyword.

Snort has basic rules such as msg which is the message value on the alert and pocket logs. SID is a keyword for identifying rules in this network. It may be used by output modules and log scanners. There are particular SID ranges. The first one ranging from 0 to 99 is for future use. The second one from 100 to 1,000,000 is for official Snort Distribution rules. There are also SIDs which are above 1,000,000.

Logto allows the packet to log to the custom file instead of standard file. Minfrag is being used for adding the value of threshold when it comes to smallest IP fragments. It can be used while preventing and detecting attacks and mechanism set to break the fragments. Dsize allows matching the size of packet’s payload. Dsize <more than 1500> is for gigantic ones; and dsize <less than 64> is for runts. Content allows finding packet payload patterns. There are also flags which are responsible for particular values. They are as follows: “F - FIN (LSB in TCP Flags byte); S – SYN; R – RST; P – PSH; A – ACK; U – URG; 2 - Reserved bit 2; 1 - Reserved bit 1 (MSB in TCP Flags byte)” (Roesch, 1999). There is also seg that is being used as a rule for sequence value of TCP. Ack is used for acknowledge field of the header which allows detecting pings of NMAP TCP. Itype checks the ICMP type field when given a particular value (Roesch, 1999). Icode allows testing the ICMP code field when given a specified value. There are also other good rules when it comes to Snort which allow ACK scans. One would like to state that when using or designing a rule, it is important to take into consideration content options. Hence, whenever content matters as much as the order, the creator has to take advantage of it in order to build an effective code.

Nevertheless, when it comes to good rules, one would recommend the TRW or threshold random walk. It detects port scans using sequential hypothesis testing with external source being used for every new connection. This way, it is possible to determine whether the destination exists by analyzing whether there is more support for the source to be scanned or not scanned. That is why one does not think that Bro can do a better job that ACK scan. It uses threshold walk approach which is not as effective as the one described above.

Question 6. SQL can be injected during the attack by the hacker. He or she can inject SQL through cookies fields or into the input. Thus, any users’ input from fields and cookies may be a threat and attacked. SQL attack may be detected by analysis of particular SQL meta-characters (single-quote or the double dash).

XSS attack is different from SQL injection because it is a security vulnerability of computer device found in Web applications. With this attack, hacker may damage the client-side script and inject threats into it so they may be harmful for users watching certain Websites. Hence, the method of attack and the main targets are the most important differences between these injections and attacks. For example, during XSS attack, a hacker can access to the most important users' information in case he or she is able to damage the web pages with a certain script, and that makes a big difference compared to SQL.

Question 7a. Pair of parentheses has to enclose the options of rules which are following the header. Despite the amount of options, they are divided using semicolon. The action is being implemented with all options criteria being true. In most cases, the option usually has a keyword and argument part. The rules are:

Log – for logging to a packet in various ways with different levels in accordance to the arguments and command line. Snort command allows determining the right command line arguments for each network.

Pass - it is used for ignoring the packet by Snort. It also fastens operations in Snort especially when packets are unchecked.

Activate – allows creating an alert and activating more rules which check other conditions. Activate is necessary for more tests of a captured packet, and dynamic rules are being used on this case.

Alert – allows sending alerts in case the rule conditions for a special packet are true. One can send an alert in various ways such as to console or file. Alert does more functions than Log because it does not only log, but also sends messages.

Dynamic – it is an action rule that becomes active thanks to Activate. It is being used only in case of threats.

Question 7b. Firstly, it is important to state that Trojan can create the file of the same name to the file it has no access to in order to cause a name duplication error. Everything is linked to bits' speed because there may be a great amount of files being created and deleted, depending on the speed.

Hence, the way for Trojan to achieve the set result is by harmful code or software, such as Trojan horse. System administrator does not know that this code has access to the system because it may look like a normal program. It may get into the system like a normal program, and only later, system administrator realizes its harm. Later, this code masks within a device. It is not being detected by antiviruses because it disguises itself as a legal program. Basically, Trojan can transmit 4 characters without being blocked by rules when a system administrator is the one letting this code onto the device.

Question 8. AH authenticates and ESP encrypts and authenticates the data ("AH and ESP Protocols", 2010). Although they are used separately in most cases, it is also possible to use them together. As it was mentioned before, AH only authenticates detecting data alteration and safeguarding from hackers, where a hash-based message authentication code performs this task.

When it comes to ESP, it does not only authenticate, but also encrypts. It is more complicated than AH because of its function of surrounding the payload. Nevertheless, ESP authentication is not for the entire IP packet, but for ESP header and encrypted payload only.

Although some may think that it is bad for security, it is not so because it actually has some advantages.

One would say that it is safe to use ESP without AH as well as with it. Nevertheless, authentication has to be done, no matter what, because absence of authentication leaves encryption unprotected. Thus, ESP should always be used for authentication, or it should be used together with AH. It is recommended over AH because it has more capacities.

References

"AH and ESP protocols." (2010). *IBM Corporation*. Retrieved from http://pic.dhe.ibm.com/infocenter/zos/v1r12/index.jsp?topic=%2Fcom.ibm.zos.r12.halz002%2Ff1a1b3a0282.htm

Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the key scheduling algorithm of RC4. *Wiki-Files*. Retrieved from http://wiki-files.aircrack-ng.org/doc/technique_papers/rc4_ksaproc.pdf

Roesch, M. (1999). Writing snort rules. *USSRback.com*. Retrieved from http://www.ussrback.com/docs/papers/IDS/snort_rules.htm