COMS 4180 Network Security Written Assignment 3

Due Wednesday April 6, 2016 by 10:00pm Eastern time.
50 points
The homework is to be done individually.
Most of the problems are based on assigned the readings.
NO LATE HOMEWORK WILL BE ACCEPTED.
What to submit: A text/pdf/word file with your answers. Submit via canvas.

1. 8 points

The snort rules below are from community-rules.tar.tar. The rules file is available from snort's web site but there is no need to download it for this problem.

EXTERNAL_NET and HOME_NET are defined variables and indicate anything external to the network being protected and the network being protected, respectively. SSH_PORTS is also a defined variable. Their specific values do not matter for this problem.

a. (4 points) All of these rules use the same basic approach to identify known malicious packets, what is the approach?
b. (4 points) What are two problems with using this type of approach?

alert udp $EXTERNAL_NET 3345 -> $HOME_NET 3344 (msg:"MALWARE-BACKDOOR Matrix 2.0 Server access"; flow:to_server; content:"logged in"; metadata:ruleset community; classtype:misc-activity; sid:162; rev:10;)

alert tcp $HOME_NET 666 -> $EXTERNAL_NET any (msg:"MALWARE-BACKDOOR BackConstruction 2.1 Server FTP Open Reply"; flow:to_client,established; content:"FTP Port open"; metadata:ruleset community; classtype:misc-activity; sid:158; rev:10;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"PROTOCOL-FTP tar parameters"; flow:to_server,established; content:" --use-compress-program "; fast_pattern:only; metadata:ruleset community, service ftp; reference:bugtraq,2240; reference:cve,1999-0202; reference:cve,1999-0997; classtype:bad-unknown; sid:362; rev:20;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $SSH_PORTS (msg:"INDICATOR-SHELLCODE ssh CRC32 overflow filler"; flow:to_server,established; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; fast_pattern:only; metadata:ruleset community; reference:bugtraq,2347; reference:cve,2001-0144; reference:cve,2001-0572; classtype:shellcode-detect; sid:1325; rev:10;)

2. 8 points (2 points for each line)

On a Linux server, what rules would you place in iptables to do the following for incoming traffic? The traffic arrives on interface eth0. Write the rules using iptables syntax.

a. Block all traffic coming from IPv4 addresses in the range 200.168.20.10 to 200.168.20.40, inclusive.

b. Allow all traffic from any IPv4 address beginning with 128.124 and block all other traffic.

c. Allow only TCP traffic to ports 80 and 8080 and block all other traffic.

The following is for outbound traffic:

d. Allow outbound traffic only to SERVERBOB port 22?

3. 8 points

Does an onion routing service provide any benefit if there are only four nodes participating in the network and only two people use the service? Why or why not?

4. 5 points

Run nmap with the option to obtain the most information against some machine (such as your own laptop or a clic machine). What operating system and open ports did nmap detect? Show the output of nmap.

5. 5 points

Of the topologies listed in the Damballa whitepaper Botnet Communication Topologies, what topology makes a botnet easiest to disable if the master(s) are discovered and why?

6. 10 points (5 points each)

a. What is GMBot and what common approach did it use?

b. What cryptographic algorithm did Angler use and what was it used for?

7. 6 points (2 points each)

a. What did Kaspersky say was overwhelmingly the most common application attacked by exploits in 2015? Of the types of applications Kaspersky listed, which ones saw a decrease in the percent of exploits targeting the application from 2014 to 2015?

b. Did Kaspersky observe an increase or decrease in ransomware in 2015 compared to 2014 and approximately how much was the change?

c. What application/type of application did McAfee say had the most zero-day exploits in 2014-2015 and what two reasons did McAfee indicate were likely to result in a continuation of vulnerabilities in this application?