CS 161 Spring 2024 — Introduction to Computer Security — Discussion 12

Question 1 ***Intrusion Detection***

FooCorp is deciding which intrusion detection *method* to employ in a few target scenarios. In the following parts, consider which of the intrusion detection methods learned in class would be most appropriate (NIDS, HIDS, or logging), and justify why.

Q1.1 FooCorp is hosting a web application over HTTPS and needs to detect any use of blacklisted characters in real time.

Q1.2 FooCorp is hosting a web application over HTTP and wants to pass all user traffic through an anomaly detection algorithm (which uses some computationally expensive mAcHinE LeARniNg). The web application needs to have low latency when many users are online during the day.

Q1.3 FooCorp uses the Simple Mail Transfer Protocol (SMTP) for email and wants to be able to quickly detect phishing attacks against any of their internal computers. SMTP runs on port 25 and is unencrypted.

Q1.4 FooCorp doesn't trust its employees and sets-up a NIDS to monitor their traffic. However, many employees use TLS, hindering what can be monitored.

FooCorp decides to turn their NIDS into a *Man-in-the-Middle*, giving it a certificate that all the employee's computers trust. Whenever an employee visits a website they complete a TLS handshake with the NIDS, the NIDS connects to the requested website using TLS, and any traffic between the employee and website is forwarded across the two TLS links by the NIDS.

Which security principle does this violate? Describe everything an attacker can do if they compromise the NIDS.

FooCorp now needs to decide which intrusion detection *technique* to employ in a few target scenarios. In the following parts, consider which technique would be most appropriate (signature-based, anomaly-based, specification-based, or behavioral), and justify why.

Q1.5 FooCorp wants to detect script kiddies (hackers who primarily use publicly available tools or exploits).

Q1.6 FooCorp wants to detect a seasoned l33t h4x0r who crafts custom exploits for each attack.

Q1.7 FooCorp wants to detect publicly-available malware that a hacker manually tweaks to avoid signature checks.

Q1.8 FooCorp wants to detect any attempts by their employees to access the protected `/etc/passwd` file.

Question 2 ***Low-level Denial of Service***

In this question, you will help Mallory develop new ways to conduct denial-of-service (DoS) attacks.

CHARGEN and ECHO are services provided by some UNIX servers. For every UDP packet arriving at port 19, CHARGEN sends back a packet with 0 to 512 random characters. For every UDP packet arriving at port 7, ECHO sends back a packet with the same content.

Mallory wants to perform a DoS attack on two servers. One with IP address A supports CHARGEN, and another with IP address B supports ECHO. Mallory can spoof IP addresses.

Q2.1 Is it possible to create a single UDP packet with no content which will cause both servers to consume a large amount of bandwidth?

- If yes, mark 'Possible' and fill in the fields below to create this packet.
- If no, mark 'Impossible' and explain within the provided lines.

◯ Possible ◯ Impossible

If possible, fill in the fields:

Source IP: _____ Destination IP: _____
Source port: _____ Destination port: _____

If impossible, why?

_____

_____

Q2.2 Assume now that CHARGEN and ECHO are now modified to only respond to TCP packets (post-handshake) and not UDP. Is it possible to create a single TCP SYN packet with no content which will cause both servers to consume a large amount of bandwidth? Assume Mallory is off-path from the two servers.

- If yes, mark 'Possible' and fill in the fields below to create this packet.
- If no, mark 'Impossible' and explain within the provided lines.

◯ Possible ◯ Impossible

If possible, fill in the fields:

Source IP: _____ Destination IP: _____
Source port: _____ Destination port: _____
Sequence #: _____ Ack #: N/A

If impossible, why?

_____

_____

Question 3 ***A Tour of Tor***

As a reminder, when connecting to a normal website through Tor, your computer first queries the Tor "consensus" to get a list of all Tor nodes, and using this information it connects to the first Tor node and, from there, creates a circuit through the Tor network, eventually ending at an exit node.

Q3.1 (4 min) Consider the scenario where you are in a censored country and the censor choses not to block Tor, the censor is the adversary, and no Tor relays exist within this country. How many Tor relays must your traffic pass through, including the exit node, to prevent the censor from blocking your traffic.

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q3.2 (4 min) Consider the scenario where you are the only user of Tor on a network that keeps detailed logs of all IPs contacted. You use Tor to email a threat. The network operator is made aware of this threat and that it was sent through Tor and probably originated on the operator's network. How many Tor relays must your traffic pass through, including the exit node, to guarantee the network operator can't identify you as the one who sent the threat?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q3.3 (4 min) Consider the scenario where there is a single hostile Tor node but you don't know that node's identitity, and that node can be an exit node. You want to keep confidential from this node what HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee this adversary can't know what sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q3.4 (4 min) Consider the scenario where there are mulitple independent hostile Tor nodes but you don't know their identities, and these nodes can be exit nodes. You want to keep confidential from all these nodes what HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee that every independent hostile node can't know what sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q3.5 (4 min) Consider the scenario where there are multiple colluding hostile Tor nodes but you don't know those nodes identities, and these nodes can be exit nodes. You want to keep confidential from all these nodes what HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee that the colluding system of hostile nodes can't know what sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary

Q3.6 (4 min) Consider the scenario where there is a single hostile Tor node but you don't know that node's identity, and that node can be an exit node. You want to have data integrity for the HTTP sites you are visiting through Tor. How many Tor relays must your traffic pass through, including the exit node, to guarantee this adversary can't manipulate the data you receive from the sites you visit?

- ◯ One
- ◯ Two
- ◯ Three
- ◯ Four
- ◯ Tor doesn't stop this adversary