Intrusion Detection

Question 1 ***Intrusion Detection*** **(15 min)**

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 black-listed 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 publically available tools or exploits)

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

Q1.7 FooCorp wants to detect publically-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*** **(8 min)**

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

Q2.1 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.

i. 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?

_____

_____

ii. 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?

_____

_____