CS161 Fall 2026 — Introduction to Computer Security — Discussion 7

Q1 *DNS Walkthrough* **(3 points)**

Your computer sends a DNS request for www.google.com'‘

Q1.1 (1 point) Assume the DNS resolver receives back the following reply:

```
com. NS a.gtld-servers.net
a.gtld-servers.net A 192.5.6.30
```

Describe what this reply means and where the DNS resolver would look next.

Q1.2 (1 point) If an off-path adversary wants to poison the DNS cache, what values does the adversary need to guess?

Q1.3 (1 point) Why do we not use TCP for DNS? Why not use TLS to make the DNS connection secure?

This content is protected and may not be shared, uploaded, or distributed.

Q2 *DNS* **(1 points)**

Q2.1 (1 point) An attacker wants to poison the local DNS resolver's cache using the Kaminsky attack. We assume that the resolver does not use source port randomization, so the attacker will likely succeed.

Using the Kaminsky attack, the attacker wants to poison the resolver's cache for the domain `www.berkeley.edu`.

The attacker constructs a website with lots of images as follows:

```
<img src="http://fake1.berkeley.edu">
<img src="http://fake2.berkeley.edu">
<img src="http://fake3.berkeley.edu">
<img src="http://fake4.berkeley.edu">
                ...
```

◇ **Question:** If the attacker wants the resolver to accept their spoofed response, the transaction id (16-bit value) must be the same as the resolver's request transaction id. If the attacker can only send k responses before the name sever responds, what is the probability that at least one of the attacker's responses will be accepted by the resolver?

◇ **Question:** If the attacker can send multiple responses which use each possible transaction id, why would the attacker want to load many, even thousands of images on their website rather than just a few.

◇ **Question:** Assuming that the attacker has constructed a website with the image tags given above, can the attacker poison the resolver's cache for the domain www.google.com?

This content is protected and may not be shared, uploaded, or distributed.

Q3 *Intrusion Detection* **(8 points)**

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.

Q3.1 (1 point) FooCorp is hosting a web application over HTTPS and needs to detect any use of blacklisted characters in real time.

Q3.2 (1 point) 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.

Q3.3 (1 point) 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.

Q3.4 (1 point) 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.

This content is protected and may not be shared, uploaded, or distributed.

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.

Q3.5 (1 point) FooCorp wants to detect script kiddies (hackers who primarily use publicly available tools or exploits).

Q3.6 (1 point) FooCorp wants to detect a seasoned hacker who crafts custom exploits for each attack.

Q3.7 (1 point) FooCorp wants to detect publicly-available malware that a hacker manually tweaks to avoid signature checks.

Q3.8 (1 point) FooCorp wants to detect any attempts by their employees to access the protected `/etc/passwd` file.

This content is protected and may not be shared, uploaded, or distributed.