CS 491/591: Introduction to Computer Security

Final Exam sample questions

1. Security principles and access control

a) What are the 3 fundamental security principles?

b) Which of the 3 fundamental security principles do keyed hashes mainly help with?

c) Which security principle does the Bell-LaPadula model address?

d) Give an example of a system that uses access control lists to implement security.

2. Linux (24 pts)

Consider the snippet below of a log file named `log.txt`

```
foo    pts/0  174.127.210.2    Tue Nov 29 05:48 - 06:27  (00:38)
foo    pts/0  131.252.220.66   Mon Nov 28 17:21 - 17:28  (00:06)
root   pts/0  166.176.57.39    Sun Nov 27 11:44 - 11:36  (23:51)
foo    pts/0  133.20.13.5      Tue Nov 22 05:40 - 06:36  (00:55)
prx    pts/0  166.177.58.91    Mon Nov 21 19:33 - 20:29  (00:55)
foo    pts/0  166.177.58.132   Mon Nov 21 13:50 - 16:24  (02:34)
root   pts/6  174.127.210.2    Mon Nov 21 05:50 - 07:44  (01:54)
```

a) Write a single command line that uses any of the commands from `cat`, `grep`, `sort`, `awk`, `cut`, and `uniq` along with pipes (`|`) to output all IP addresses that the user `foo` has logged in from.

b) Write a `find` command to return all files under `/etc` that have been modified since the beginning of this month.

Consider the following lines in a file:

```
abcd
dabc
cdab
bcda
```

c) Write the lines that match the 3-character regular expression **`c..$`**

Permission bits `rwx` specify access allowed for a user, group, or others. Consider the following commands being executed in a Linux shell:

```
umask 000; touch x
umask 037; touch y
```

d) What are the permission triplets for `x`?

e) What are the permission triplets for `y`?

f) Which file on a Linux machine would an administrator visit to find the most recent login attempts?

3. Cryptography (8 pts)

a) What class of algorithms provide source integrity using symmetric keys?

b) What advantage does the cipher-block chaining (CBC) mode of encryption provide over electronic code book (ECB) mode?

4. Authentication (8 pts)

a) What is not trusted in a "Zero Trust" network?

b) What protocol do federated identity providers use to implement authentication as a service?

5. Network Security (18 pts)

a) Write the smallest CIDR prefix that includes both 10.0.0.35 and 10.0.0.40

b) How many hosts are in a `/25` CIDR prefix?

c) The network I'm currently on is `131.252.0.0/28`. Consider hosts that are up and running with IP addresses of `131.252.0.2`, `131.252.0.8`, and `131.252.0.32`. If I perform an `nmap` ARP scan on each IP address, which will respond?

d) Write an `iptables` command that uses a single rule and CIDR prefix to drop all traffic originating from Portland State IP addresses (131.252.0.0 to 131.252.255.255)

e) What would a bank like Wells Fargo be looking for when searching the certificate transparency reports hosted by sites like `crt.sh`?

f) What would an adversary or penetration tester be looking for when searching the certificate transparency reports hosted by sites like `crt.sh`?

6. Host Security (8 pts)

a) Name one technique described in class that adversaries use to bypass signature detection systems

b) What type of resource does `chroot()` restrict access to?

c) What type of resource does Linux Seccomp restrict access to?

7. Application Security (8 pts)

A developer is considering the following mechanisms to prevent memory corruption attacks:

1. Address Space Layout Randomization
2. Control-Flow Integrity
3. Pointer Authentication Codes

a) List the mechanisms that can directly protect against an adversary overflowing a buffer on the stack in order to inject code and execute it.

b) List the mechanisms that can directly protect against an adversary overflowing a buffer on the stack in order to perform return-oriented programming?

c) List the mechanisms that can directly protect against an adversary tampering with function pointers.

8. Privacy (10 pts)

a) In what situation will a cookie be sent in a `SameSite=None` policy where it will not be sent in a `SameSite=Lax` policy

b) If an adversary hijacks the entry node used by a request in Tor, what is revealed out of the following pieces of information: the client location, the request payload, the server location?

c) If an adversary hijacks an exit node used by a request in Tor, what is revealed out of the following pieces of information: the client location, the request payload, the server location?