Access Control — 8 of 8 points

When a user whose userid is 500 executes the command /bin/passwd from shell, a new process is created by fork. Answer the following questions accordingly.

✓ Immediately after forking, the new process's three user IDs (euid,ruid,suid) should be _____ 2/2

- ○ (0, 0, 0)
- ○ (500, 500, 0)
- ◉ (500, 500, 500) ✓
- ○ (0, 500, 500)

✓ Then the newly created process uses "exec" to load the program, which is owned by root and has the setuid bit set. After loading the program, the process's (euid,ruid,suid) should be _____ 2/2

- ○ (0, 0, 500)
- ○ (500, 0, 500)
- ○ (500, 500, 500)
- ◉ (0. 500, 500) ✓

✓ If the process wants to drop its privilege temporarily, the process's (euid,ruid,suid) should be changed to _____ 2/2

- ◉ (500, 500, 0) ✓
- ○ (500, 0, 0)
- ○ (500, 500, 500)
- ○ (0, 500, 0)

✓ And if the process wants to drop its privilege permanently, the process's (euid,ruid,suid) should be changed to _____ 2/2

- ◉ (500, 500, 500) ✓
- ○ (500, 500, 0)
- ○ (0, 500, 0)
- ○ (500, 0, 0)

Answer by selecting True of False — 18 of 18 points

✓ Strictly enforcing same-origin policy can successfully prevent against cross-site scripting (XSS) attacks. 2/2

- ○ True
- ◉ False ✓

✓ Using input validation to reduce applications vulnerabilities, it is better to blacklist what is not allowed that whitelisting what is allowed. 2/2

- ○ True
- ◉ False ✓

✓ As a security principle; complexity always enhances security. 2/2

- ○ Tues
- ◉ False ✓

✓ Cookies cause privacy concerns because when executed by the browser they can send off sensitive information (such as keystrokes) to the websites that set the cookies. 2/2

- ○ True
- ◉ False ✓

✓ You cannot delete a file if you cannot write to the file. 2/2

- ○ True
- ◉ False ✓

✓ Only owner of a directory can create new files under a directory. 2/2

- ○ True
- ◉ False ✓

✓ As a general security principle, it is strongly recommended to make the security depends on the keep the system designs secret. 2/2

- ○ True
- ◉ False ✓

✓ If you keep your Wifi SSID (network name) hidden; no one will be able to access your network. 2/2

- ○ True
- ◉ False ✓

✓ You can use IPSec without the sender and received knowing that it has been used 2/2

- ◉ True ✓
- ○ False

Select the network layer where the attack in the different rows occur **6 of 6 points**

These are some attacks happen in different network layer. Match the network layer in the column with the attack that occurs in the corresponding row (on attack per column).

	Link Layer	IP Layer	Transport Layer	Score	
ARP spoofing attack.	◉	○	○	2/2	✓
Smurf DoS attack.	○	◉	○	2/2	✓
SYN flooding attack.	○	○	◉	2/2	✓

SSL/TLS — 8 of 8 points

Please answer the following questions about SSL/TLS. Assume we are using the simple protocol run version discussed in class.

✓ M1: C -> S: Client Hello — 2/2

The first message sent from the client to the server, it contains the following information. Select ALL the things that are included in the message

- [x] Client Nonce ✓
- [x] Encryption algorithms to be used ✓
- [ ] Encryption keys
- [x] SSL version number ✓

✓ M2: S-> C: Server Hello, ServerCertChain — 2/2

The second message sent from the server to the client, it contains the following information. Select ALL the things that are included in the message

- [x] SSL version number ✓
- [x] Server Nonce ✓
- [ ] Encryption Keys
- [x] Encryption algorithms to be used ✓

✓ M3: C -> S: ClientKeyExchange, ChangeCipherSpec, ClientFinished — 2/2

ClientKeyExchange contains _____

- (●) pre_master_secret key encrypted using the server's public key ✓
- ( ) pre_master_secret key encrypted using the clients private key
- ( ) the client public key to be used in the encryption process
- ( ) pre_master_secret key sent in clear text

✓ M4: S -> C: ChangeCipherSpec, ServerFinished — 2/2

ServerFinished contains _____

- (●) hash of all the previous messages ✓
- ( ) hash of all the previous messages sent by the client
- ( ) hash of all the previous messages sent by the server