Tests & Quizzes

Final Exam

Return to Assessment List

Part 1 of 1 - 77.0/ 100.0 Points

Question 1 of 20

Match the terms with their definitions. 5.0/ 5.0 Points

A. Code and mechanisms to provide software updates securely.

B. Executes script within the context of the browser that was unintended.

C. Executes queries within the context of the database that was unintended.

D. When applied to steganography, “The degree of degradation due to embedding operation”

E. Executes machine code within the context of the running process that was unintended.

D	1. Fidelity
B	2. XSS
C	3. SQLi
E	4. Buffer Overflow Exploit
A	5. TUF

Question 2 of 20

Describe 2 mechanisms for blocking SQLi attacks. 5.0/ 8.0 Points

Two ways you can block SQLi attacks are to perform input validation and blacklisting harmful input within the input field. If we perform input validation where we check if any input is malicious or not would help prevent SQLi attacks within a database. Blacklisting certain text such has

SQL commands will also help prevent SQLi attacks where we have a list of harmful inputs that can lead to a compromise database.

Comment: Looking for escaping (sanitizing inputs) and prepared statements

Question 3 of 20

Explain the difference between Steganography and Software Watermarking. What types of threats are your trying to defend against in each technology? 5.0/ 8.0 Points

Stenography is when you unintentionally put embedded data within any form of file format while Watermarking is intentionally finding embedded data within any form of file format. With watermarking this can protect potential intellectual property that user know its that specific company that implement that software. For example by watermarking a logo of a classified Federal Document then ann user is able to take cautious steps reading that document. With stenography you can embedded secret data. We can used stenography to a software that is being distributed illegally. For example companies use embed string of data on there intellectual property to pinpoint which clients are distributing their software illegally. If Microsoft can add stenography to there activation key to find which sellers are selling Microsoft gray licence keys, they are able to pinpoint the actors and take criminal action.

Comment: Watermarking and steganography are processes in which the digital image is changed in a way that one can see the background image or the text without any kind of corruption in the image.

Watermarking is used to verify the identity and authenticity of the owner of a digital image. It is a process in which the information which verifies the owner is embedded into the digital image or signal. These signals could be either videos or pictures or audio.

Steganography is changing the image in a way that only the sender and the intended recipient is able to detect the message sent through it. It is invisible, and thus the detection is not easy. It is a better way of sending secret messages than encoded messages or cryptography as it does not attract attention to itself.

Question 4 of 20

What is the most critical element of a trusted computing system (such as a TCB)? How is this typically protected? 4.0/ 8.0 Points

The critical element for trusted computing system is creating a some form of trust relationship with the system to use its software. For example after you installed an Operating system within your system, it ask for an activation key. once you enter that key, Microsoft creates a one way hash base on your system hardware. if any chance you image your drive and apply it to a system with a different hardware then Microsoft code will alert that there was a system changed and make your windows not activated due the change. This typically protects mass distribution of software being used without the company gaining a profit. You can also embed logic bombs if you don't want any other system access the information if it ever leaves from a company vault.

Comment: Talk more about components of TCB

Question 5 of 20

Describe the difference between a Type 1 and Type 2 Hypervisor. 8.0/ 8.0 Points

If you were in charge of testing Windows malware in a virtual machine to see what it does (think Cuckoo or MALWR.com), what type of hypervisor would you use and why?

With a Type 2 Hypervisor you generally have from bottom to top, Hardware, primary OS, Hypervisor, and sets of different type of OS within a VM called Guest OS. While Type 1 you generally have hardware, hypervisor and sets of the Same OS that are independently with each other. I rather take Type 2 even if it has overhead because of the primary OS. With different sets of OS, I can use software that can attended work better with a specific OS. for example running a MACOSX guest within a VM, I can run apps tailored to that OS and with certain exe application I can use a windows OS Guest or with a Linux OS i am able to use Linux distro packages within one machine. I am able to freely to use other apps with using separate physically machine.

Question 6 of 20

ASLR and Stack Canaries are both effective methods at thwarting stack overflow vulnerabilities. Explain what each does and what specifically they are able to prevent. 5.0/ 8.0 Points

NOTE: Stack canaries also are called Stack Cookies, or Stack Guards.

ASLR can prevent over buffer flow within memory and stack canaries can prevent jumps of execution within memory. With ASLR it can randomize certain areas within memory, so it can prevent attack leaks wrong area of memory. Windows XP had an issue where attacker would talk to specific part of memory and leak out the credentials of that machine, by using ASLR it is very difficult to pinpoint where is the memory you store windows credentials. With stack canaries it pushes execution within a stack to prevent unattended code to jump off from certain part of memory.

Comment: ASLR and Stack Canaries are both effective methods at thwarting stack overflow vulnerabilities. Explain what each does and what specifically they are able to prevent.

ASLR - Address space layout randomization is a memory-protection process for operating systems that guards against buffer-overflow attacks by randomizing the location where system executables are loaded into memory.

Stack Canaries - are a secret value placed on the stack which changes every time the program is started. Prior to a function return, the stack canary is checked and if it appears to be modified, the program exits immediately.

Question 7 of 20

Describe, at a high-level, how a CSRF/XSRF attack works. Describe what level of access the attacker needs to the server or client (if any). 8.0/ 8.0 Points

Cross site request forgery is when a user logs within a session of a bad implemented website and also the user made a session with an attacker website. that attacker can send request to the user which can make a request to the bad implemented website. the server believes the

client made a request but it was actually the attacker machine that made the request. CSRF are knownly used within bank where attacks can set up transaction that the user has no aware of.

Question 8 of 20

8.0/ 8.0 Points

You are put in charge of assessing a new piece of software for your enterprise. Your specific job is to assess the security up the update mechanism of the software. You are supposed to assess if the update process can be negatively affected or compromised by an outside attacker.

Define a specific threat affecting update mechanisms, and how you'd assess/test the implementation for any security issues.

One threat affecting update mechanism is remove updated files and replace it with malicious files which can affect any machine that tries to make an update. What i would use is the TUF implementation where i revoke any user who is attempting to make an update to my repository. if the attacker is able to make change, luckily i have a role that does integrity check of the attack files and remove those changes and restore does latest packages with one of the roles that can check history of updated packages.

Question 9 of 20

Any code that relies on hash functions needs to take into account that hash function output is variable length. 2.0/ 2.0 Points

- A. True
- B. False

Question 10 of 20

Once issued, CA's do not have a method for revocation of certificates; they become invalid after they expire. 2.0/ 2.0 Points

- A. True
- B. False

Question 11 of 20

By using TOR, a user ensures that all traffic is end-to-end encrypted. 0.0/ 2.0 Points

- A. True
- B. False

Question 12 of 20

Asymmetric encryption requires that a master key be able to decrypt all messages, regardless of sender. 0.0/ 2.0 Points

- A. True
- B. False

Question 13 of 20

Homomorphic encryption allows a 3rd party to decrypt data (e.g., “in the cloud”), perform operations on the data, re-encrypt it, and provide the results of the operations back. 0.0/ 2.0 Points

- A. True
- B. False

Question 14 of 20

CA’s are managed by government, commercial, non-profit and other organizations. 2.0/ 2.0 Points

- A. True
- B. False

Question 15 of 20

AES requires the public key of ALL recipients prior to encryption. 0.0/ 2.0 Points

- A. True
- B. False

Question 16 of 20

Choosing epoch (the number of seconds since 01JAN1970) is sufficient as a random number generator. 2.0/ 2.0 Points

- A. True

B. False

Question 17 of 20

Kerberos strives to provide privacy and anonymity. 2.0/ 2.0 Points

A. True

B. False

Question 18 of 20

8.0/ 8.0 Points

Describe DNS amplification DDoS attacks in technical detail. At a minimum, include: network protocol, if amplification is possible, if spoofing is possible, does it rely on other DNS servers beyond just the target?
Detail as much as possible (a simple 'yes' or 'no' is not sufficient).

DNS amplicfication is when a user disrupts the request of a Domain name server that resolves url names to ip address. By have 100 of clients making request on that DNS the server will be unable to resolve IP address on machine who actually need to be resolve. What an attacker can now can pretend to be the DNS and resolve those IP to the attacker machines which can cause user to leak out information such as documents, password to the wrong party.

Question 19 of 20

6.0/ 8.0 Points

You are an attacker. You would like to snoop on the traffic between a specific TOR user and a specific website. This website is open to the public (not on a .onion address), but the user only connects to the website via TOR.

For the sake of this exercise you are able to install a monitoring utility (hardware or software) at any part of the TOR network. In other words, you have the ability to infect and monitor any point of the network traffic, including the following locations:

- **Install a trojan on the device that the user is using to access the website via TOR**
- **Compromise a TOR entry node**
- **Compromise a TOR relay node**
- **Compromise a TOR exit node**

- **Compromise the website that the user is connecting to**

For EACH item, describe if it would allow you to be able to monitor the traffic between the user and the website. If so, what are your chances of collecting target on your specific user ONLY (and not another random user that might be accessing the same website).

Within the entry node it would be less hard than the relay node. the tor will encrypt traffic once in point of entry and by cracking one key will be easier but once that user hopes in the the relay node than its is nearly impossible because for every hop within the proxy server that data will be encrypt on top continuously. If its the exit node it can be a lot easier because once it exit out, everything will be decrypted . which i can host multiple machines to attempt DOS exit node and host my own "fake" node and reroute to my website that will download Trojan within the machine and once execute the client machine will have a Trojan.

Comment: Make sure you talk about all compromises

Question 20 of 20

Describe, in detail, the most important lesson or topic that you learned in the class. This can be from any module, lecture, quiz or homework. 5.0/ 5.0 Points

Explain how you have applied (or hope to apply) this lesson to an infosec challenge you have faced (or plan on facing).

I learn that creating permission on files, systems and groups are important to implement within an organization or even within day to day lives. by deciding which person should be able to do what with a file is very important in a company. For example you do not want some outside person to able to make unattended modification with that data because that data can be blamed by the owner if that data is unusable no more. As an intern at the DOE, it makes sense that i have limited access to their network drives that. if i wanted to use a network drive i am able to copy it through my desktop but can't overwrite those file to that network drive. If i ever had the remission and mistakenly deleted something important than my manager would be blame within the organization. Setting permission is a great practice for protecting your data and reduces the risks for owner of the data.

Change Profile Picture

Error removing image
Error uploading image
Upload Choose File No file chosen

Save Cancel Connections ✖ Remove

Search for people ...
View More

My Connections | Pending Connections

You don't have any connnections yet. Search for people above to get started.
You have no pending connections.
←Back to My Connections
Search for people ...
$({cmLoader.getString("connection_manager_no_results")}

Done