STUDENT

0009-LTS

TENTAMEN

Digital tentamen - ASC400

Kurskod	ASC400
Bedömningsform	--
Starttid	19.03.2024 07:30
Sluttid	19.03.2024 10:30

Bedömningsfrist	--
PDF skapad	24.01.2025 12:15

Section 1

Uppgift	Uppgiftstitel	Status	Poäng	Uppgiftstyp
ℹ	General Info			Information eller resurser

Auto Graded Questions

Uppgift	Uppgiftstitel	Status	Poäng	Uppgiftstyp
1	Q1	Delvis rätt	1/4	Matchning
2	Q2	Delvis rätt	7.5/9	Matchning
3	Q3	Delvis rätt	6/10.5	Matchning
4	Q4	Rätt	9/9	Matchning

Essay Questions

Uppgift	Uppgiftstitel	Status	Poäng	Uppgiftstyp
5	Q5	Besvarad	8/15	Essä
6	Q6	Besvarad	1/8	Essä
7	Q7	Besvarad	12/14.5	Essä
8	Q8	Besvarad	6/10	Essä
9	Q9	Besvarad	6/8	Essä
10	Q10	Besvarad	8/12	Essä

1 Q1

Ersätt med din uppgiftstext...

Which of the following is the right definition for the below security methods?

	Uses Public Key Encryption for message authentication	Provides confidentiality	Provides Message integrity + implied message authentication	Provides a way to exchange keys
DIGITAL SIGNATURE	○	○	○	◉
MESSAGE AUTHENTICATION CODE (MAC)	○	○	◉	○
SYMMETRIC ENCRYPTION	◉	○	○	○
DIFFIE-HELLMAN	○	◉	○	○

2 Q2

Ersätt med din uppgiftstext...

Threat or Vulnerability?. Indicate the correct categorization for each of the following examples:

	Threat	Vulnerability
Unauthorized access to data	○	◉
Unpatched operating system	○	◉
Malware	◉	○
Spoofing	◉	○
Weak password	○	◉
Misconfigured firewall	○	◉

3 Q3

Match the Role-based categorization of the following IoT protocols.

	Security	Device management	Data transmission	Operating systems	Communication
Contiki	◉	○	○	○	○
Bluetooth	○	○	○	○	◉
Zigbee	○	◉	○	○	○
DTLS	◉	○	○	○	○
Ubuntu Core,	○	○	○	◉	○
LwM2M	○	○	○	○	◉
MQTT	○	○	◉	○	○

4 Q4

Which description fits each of the following security attributes.?

	Authentication	Integrity	Confidentiality	Accountability	Authorization
Protects against unauthorized disclosure.	○	○	◉	○	○
Provides secure identification of users, devices or services.	◉	○	○	○	○
Maintains data consistency, and accuracy.	○	◉	○	○	○
Ensures that users can only access or use certain resources.	○	○	○	○	◉
Ensures continual access to resources.	○	○	○	○	○
Allows tracing actions and events back in time.	○	○	○	◉	○

5 Q5

1. List and explain briefly each of the hacking phases (steps) that an attacker goes through while attacking a system.(10pts)
2. Give at least an example of a tool or a method used in each phase.(5pts)

The typical flow of penetration testing:

1.) Reconnaisce - where the hacker looks after information of a system - example weak configurations or password, gather data - The hacker gathers data and after getting enough of information the hacker can then make a try of attacking the system by example ddos - to make the system not available to access. Identify - Identify the vurnebility. Attack- attack the target after identification. Gather information - Sometimes attackers stay in the system and gather information for a long time instead of destroying the system.

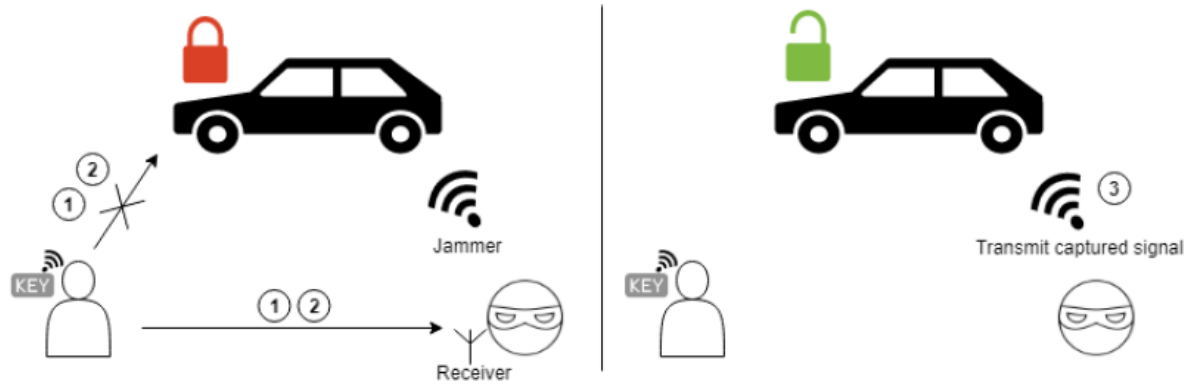
2. Nmap , wireshark, metasploit.

1)- Angriparen samlar först information om systemets svagheter och sedan identifierar honom vilken svaghet som passar just den attack som ska utföras, sedan kan attack utföras genom den valda svagheten. Oftast brukar angripare stanna i systemet lång tid för att samla på sig information och på det viset göra mer skada.

Ord: 142

6 Q6

Refer to the exhibit below and Answer the following:
1- The attack type/name (2pts)
2- Explain how it works. (6pts)



1- - Relay attack

2) It works by that the attacker has an receiver thats extends the key signal so that if the attacker is close enough to the car, the car can then mistake it for the actual key and in that way the car can get started and driven. But in the first picture its not possible because there is a jammer that prohibits signal reaching the car and in that way the car can not be opened and driven away.

På första bilden så försöker angriparen förlänga signalen från bilnyckeln så att bilen kan misstolka information och på så sätt möjliggöra användningen av bilen. Men detta är inte möjligt efter som det finns en jammer som blocker den förlängda signalen och därav förhindra en stöld.

På andra bilen - Det fungerar genom att angriparen har en receiver som förlänger signalen från bilnyckeln där sedan om angriparen står tillräckligt nära bilen så misstolkar bilen denna signalen från självaste nyckeln men egentligen är det en relay device som förlänger signalen. Bilen kan sedan öppnas o startas.

Ord: 177

7 Q7

- Explain the concept of Defense-in-Depth (DiD) (2.5pts)?
- Explain two of the six control functionalities used in DiD (4pts)
- Explain what TOR over VPN is and compare it to VPN over TOR. (4pts)
- Briefly explain what information the ISP, the VPN server provider and the TOR exit node can see when a connection is established using each of the two techniques. (4pts)

Skriv in ditt svar här

* DiD - Is the way of how to stay safe security wise - one is that everyone is responsible for the security, Another is detect vurnelbilities early.

* two of the six controll funtionalities used in DiD - One is to Detect if there is a weakness in the system and then act on in it, the other one is how to recover data in a good and secure way if a fault occurs. - If a system goes down so that it doesnt affect the rest.

* Tor over Vpn: First it connects to VPN and then to Tor-network, the data gets first encrypted in Vpn and then over to the TOr-network. in comparision to VPN over Tor - Here it first connects to Tor-network then over to Vpn, the vpn network sees traffick incoming from tor vpn and then before it reaches destination its goes through vpn.

* When Tor over vpn : The ISP sees that a connection coming in from a vpn-network and then can see that encrypted data leaves in the exit node of tor. The exit node knows the destination of the information.

*When vpn over Tor: Here ISP sees a connection coming in from a Tor-network and then into vpn, the isp sees that decrypted data leaves in the exit node.

Ord: 219

8 Q8

Write a security requirement for each of the categories below:

1. Confidentiality (2pts)
2. Authentication (2pts)
3. Authorization (2pts)
4. Session management (2pts)
5. Accountability (2pts)

Skriv in ditt svar här

1) The system must be secure in terms of sensitive information - password etc (Protects against unauthorized disclosure)

2) Every User or system must be able to be identified example by using mfa - multifactor authentication.Provides secure identification of users, devices or services.

3) System should Ensure that users can only access or use certain resources.

4) Session management should always be available and be updated to the latest.

5) System should provide a way that Allows tracing actions and events back in time.

Ord: 84

9 Q9

Write at least one solution to each of the following OWASP IoT vulnerabilities. Explain why we still have these vulnerabilities:

1. Weak, guessable & hardcoded passwords (2pt)
2. insecure web interface (2pts)
3. Insecure network services (2pts)
4. Use of insecure or outdated components (2pts)

Skriv in ditt svar här

1) An solution can be that the system demands that passwords gets changed to a new one after a certain of time, or that system implements more authentication in terms of digitals signatures och mfa. I think that we still have these vullnerabilities is that employeers does not take security of the system serious or they doesnt have the knowledge of how important it is and that can cause a lot of damage.

2) Insecure webbinteferance the solution for it can be to use https where the session of to connect needs to go through a tls handshake and that makes it harder for an attacker to make damage or steal information.

3) Insecure network services can be a problem, because old system may not have the new updates that required and that it can be a chance for and intruder to take advantage of.

4) Outdated components can cause a lot of harm if the system of the component is not updated regularly because it can be an easy target for an attack, the attacks gets more sophisticated so the components must be regularly updated.

Ord: 186

10 Q10

1. Identify the priority levels of the CIA attributes in: (1) OT and (2) in IT systems (2 pts)
2. Explain how/why the CIA attributes are prioritized differently in OT and IT systems (2 pts)
3. Give at least two reasons why ICS (Industrial Control System) is more vulnerable than IT systems. Justify the answer. (4 pts)
4. What major damages can a malware cause to an ICS in particular? (2pts)
5. Why most of the ransomware against ICS are paid? (2pts)

Skriv in ditt svar här

1) ot - (Confidentiality , integrity, accountability, availability)

it - (Availability, confidentiality, integrity, accountability)

2) For OT here its is important that sensitive information is secure and that data doesnt get get changed.

But for IT the most important is availability and it is because its more vulnerable to that a system is down compared to OT.

3) ICS - is more vulnerable because ics controls and manages industrial processes so if it gets infected that can cause a lot of harm and all the processes/operations must be stopped until it gets solved compared to IT system where it can have a more redundant system to a venerability.

4) The major damages it can cause it that the system can be controlled and give different commands that cause the system to be out of function. Its possible if the attacker jams the signal between the ics and the machines.

5) Its paid because its hard to restore and that it is cheaper to pay it instead of the system being out of function which makes a lot damage economically.

Ord: 180