Department Of Computer Engineering and I T

Course: Information Security – Laboratory(CO4002_P)

Programme : Final Year BTech Computer Engineering, Sem :VII

Yaha editing matt karo -_-
Lol anon editing chalta hai isme

Course Outcomes: At the end of this course, students will be able to,

1 Identify and evaluate threats to network security and data loss.

2 Determine the TCP/IP Security model, vulnerabilities and attacks.

3 Design firewalls and Intrusion Protection Systems

4 Analyze the network using tools and the security for operating systems, program and database.

List of practical

1) *To apply secure software lifecycle for a given case study*
2) To study and implement OWASP attacks.
   Study 2018 OWASP Attacks
   - Injection
   - Broken Authentication
   - Sensitive data exposure
   - XML external entities
   - Broken access control
   - Security misconfigurations
   - **Cross Site Scripting (XSS)**
   - **Insecure Deserialization**
   - **Using Components with known vulnerabilities**
   - **Insufficient logging and monitoring**

   Perform Attacks
   - SQL injection
   - XSS
   - CSRF

   (Install kali linux in Virtual box. Use software BWAPP or DVAP to perform following attacks .)

https://www.greycampus.com/blog/information-security/owasp-top-vulnerabilities-in-web-applications

3) To study network analysis and monitoring tools such as: Wire shark, Nmap, Hping.

Wireshark

1. The Basic HTTP GET/response interaction
   Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

   - What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   - When was the HTML file that you are retrieving last modified at the server?
   - How many bytes of content are being returned to your browser?
2. The HTTP CONDITIONAL GET/response interaction

- Inspect the content of the server response. Did the server explicitly return the contents of the file?
- What is the HTTP status code and phrase returned from the server in response to the second HTTP GET? Did the server explicitly return the contents of the file?

3. Retrieving Long Documents
   - How many HTTP GET request message were sent by your browser?
   - What is the status code and phrase associated with the response to the HTTP GET request?

(https://www.studocu.com/en/document/mount-royal-university/network-infrastructure-and-security/tutorial-work/comp-3533-lab-2-http-wireshark-questions-answers/1288492/view)

Nmap
Commands to

- detect details about hosts in the network
- show all the open ports
- scan IP portal
- find port ranges
- find protocol list
- for virus and os detection

(Install Nmap using command)
Hping3
Perform DOS attack using Hping3
(Install Hping in kali linux)

4) To study TCP/IP vulnerabilities, attacks and defence mechanism .
5) To study Routing Protocol attacks and defence mechanism.
6) To implement a firewall. How to setup Firewall using GUFW in Ubuntu 16.04(https://www.youtube.com/watch?v=4eSbe1Ik3dg)
7) To study and implement IDS using open source tool.(SNORT) https://www.youtube.com/watch?v=iBsGSsbDMyw Using software-based network intrusion detection systems like SNORT to detect attacks in the network.
8) Create the environment for the database application. Perform database administration and performance of database Application.(grant, revoke)
9) Hardening of OS. https://www.tutorialspoint.com/computer_security/computer_security_securing_os