

Cyber Security [Web, Network and Computer]: Basic Lab Practice Manual

By

Venkatesan Subramanian and Sandeep Kumar Shukla

Note: This manual is only for the learners who studied the different web, computer and network security concepts and interested in simulating the attack and mitigation techniques.

Acknowledgement: We referred various web sources to practice. We would like to thank all the authors, web sources and blogs.

Chapter 1 Web Security

1. IFRAME Hack	6
1.1 Message posting between frames	6
1.1 Exploitation.....	7
1.2 Protection Measure: Disable IFRAME	7
2. Enable SSL in Apache	8
3. TLS Version Restriction	11
4. Restrict Directory Listing.....	11
5. PHPMYADMIN access from remote machine.....	12
6. Bash_history Access Control	12
7. Always Run Apache with non-privileged account.....	13
8. Remove the server signature [Customize the error].....	13
9. Referrer policy	14
10. Cross Origin Resource Sharing (CORS).....	15
10.1 CORS Example with Access-Control-Allow-Origin header	15
11. Session	17
11.1 Creation.....	17
11.2 Session Fixation Vulnerability.....	17
11.2.1 Solution:	17
11.3 Session Hijacking.....	18
11.4 Plaintext Password in the header	18
11.5 HTTP Auth.....	19
11.6 Cookie based Session.....	19

11.7	Hidden Field.....	20
11.8	Proper logout.....	20
11.9	Password Strength.....	21
11.10	Captcha	21
12.	Log Information - Apache.....	23
13.	Cross Site Scripting.....	24
13.1	Testing the possibility of Cross Site Scripting.....	24
13.2	Reflected XSS.....	24
13.3	DOM based XSS.....	25
14.	File vulnerability	26
14.1	File Injection	26
14.2	SVG File Vulnerability	26
15.	Cross Site Request Forgery.....	27
16.	Denial of Service – Client Side.....	31
16.1	Infinite Alert.....	31
16.2	Disabling the back button	31
16.3	Fill History	32
16.4	Logout.....	32
17.	Reverse Tabnabbing.....	33
18.	Upgrade Insecure requests using the following.....	34
19.	Code Injection Attack	34
20.	SQL Injection Attack	35
20.1	First order SQL Injection	35
20.2	Second Order SQL Injection.....	36
20.3	OAST Attack	37
20.4	Attention required with MySQL	37
21.	Solution for SQLI and other Injections.....	37
21.1	Prepared Statement	38
21.2	Sanitization of the input	40
21.2.1	Use basename function	40
22.	Authorization [Access Control]: Insecure Direct Object References	41
22.1	Folder Issue and solutions.....	41

22.2	HTACCESS	42
23.	XML External Entity (XXE) Injection	44
23.1	Exploit.....	45
24.	Preventing Google Link tracking.....	45
25.	Robots.txt.....	46
26.	Damn Vulnerable Web Application.....	46
27.	CURL based login attempt.....	47
28.	Clipboard Data stealing.....	48
29.	CRLF Injection	49
30.	Local File Includes and Remote Code Execution	51
31.	Stored Procedure through PHPmyadmin	52

Chapter 2 Network Security

1.	TCP SYN flooding.....	54
1.1	Other information.....	55
2.	SCTP Simulation	55
3.	UDP echo-charge flooding.....	56
4.	Packet Flow control using IP tables	57
4.1	On Flow Rate	58
4.2	On Packet Count	60
4.2	More commands in IPtables.....	61
5.	PING command vulnerabilities.....	62
5.1	Flooding	62
5.2	Ping of Death	62
5.3	Covert Channel	63
5.4	Smurf Attack.....	63
5.5	OS fingerprint	64
5.5.1	Solution for Linux.....	64
5.5.2	Solution for Windows	65
5.6	OS fingerprinting through Other Methods.....	65
5.7	Path Identification.....	66
5	Port Knocking	67

6	ARP Cache Poisoning.....	70
	7.1 ARP Table	70
	7.2 Exploit.....	71
	7.3 Sniff the Outgoing packets from the victim on Attacker	71
	7.4 Sniff the incoming packets of the victim	72
	7.5 Important Note for MITM:	73
8.	Wireless Penetration Testing	73
	8.1 Interface	73
	8.2 Monitor Interface	73
	8.3 Monitoring	74
	8.4 Use of ivstools.....	75
	8.5 Password crack.....	75
	8.6 Key extraction using IVs	76
	8.7 Use of airdecap-ng	76
	8.8 Use of airbase-ng.	77
9.	MQTT Using mosquitto.....	77
	9.1 Run the Subscriber	78
	9.2 Run the Publisher	78
	9.3 Multiple MQTT broker on same host	78
	9.4 Possible Vulnerabilities	79
	9.5 Password Authentication	80
	9.6 Denial of Service.....	81
10.	IPSec using Strongswan.....	81
	10.1 Installation.....	82
	10.2 Wireshark Interpretation	85
11.	DNSSEC	86
12.	SSH Authentication using Key in putty	87
13.	Change the SSH default file name	87
14.	IPset	88
15.	Identify the Firewall in target machine	89
16.	DNS Filtering at the local host.....	90
17.	Fake TLS.....	91

Chapter 3 Computer Security

1. Reverse Shell	92
1.1 Using NETCAT for command and Control	93
2. Stack Overflow Attack.....	93
3. Format String Attack.....	97
4. cron Job Scheduling.....	98
5. Systemd Timers	98
6. Assigning task to a particular core [Linux].....	99
6.1 Process ID	99
7. Task Manager and Resource Monitor [Windows].....	99
8. Process Kill	100
8.1 Linux.....	100
8.2 Windows	101
9. Suspend the process [Linux].....	101
9.1 Use account suspend.....	101
10. John the Ripper	102