Web Application Penetration Testing

Ebrahim Hegazy – Www.Security4Arabs.com

About Myself

- Ebrahim Hegazy (@Zigoo0)
- 2009 → Junior Linux System Administrator
- 2011 → Security Engineer
- 2013 → Cyber Security Analyst (ThreatIntel)
- 2014 → Cyber Security Consultant (Pentesting)
- 2015 → Sr. Systems Security Engineer
- 2017 → Sr. Cyber Security Consultant
- Bug Bounty Hunter since 2013 (Yahoo, Google, Telekom.de, Avira, Paypal, Barracuda, Facebook, Twitter ….. And more.)
- Speaker for multiple international security conferences

Course Target?

- مشاركة العلم
- إثراء المحتوي العربي في هذا المجال
- التركيز علي التطبيق العملي في جميع الدروس
- إعطاء الفرصة للجميع من خلال مجانية الكورس
- كسر الخوف من المصطلحات المعقدة
- تنمية مهارات المتدربين بشرح أساسيات أكثر من مجال
- صدقة جارية لي ولوالدي رحمه الله

Course Agenda

1) Downloading & Installing Course Requirements
2) Linux Basics
3) BurpSuite and how to use it
4) Introduction Topics
5) Web Applications Vulnerabilities (Easy Level)
6) Web Applications Vulnerabilities (Medium Level)
7) Advanced Web Applications Vulnerabilities
8) Real Life Demo (Bug Bounty Hunting)

Course Requirements

- Installing necessarily browser plugins (Wappalyzer, FlagFox, FoxyProxy, SEO Status PageRank/Alexa Toolbar, Tamper data)
- Virtualbox
- Ubuntu & Windows
- Java & Burp Suite

First Session

- Deep dive into data leaks (Haveibeenpwned.com & Shodan.io)
- سنقوم في هذا الدرس بشرح كيف تمت عمليات الإختراق علي المواقع العملاقه وكيف تم تسريب مليارات من الحسابات الإلكترونية في الفترة الأخيرة
- https://hacked-emails.com/api?q=$Email$

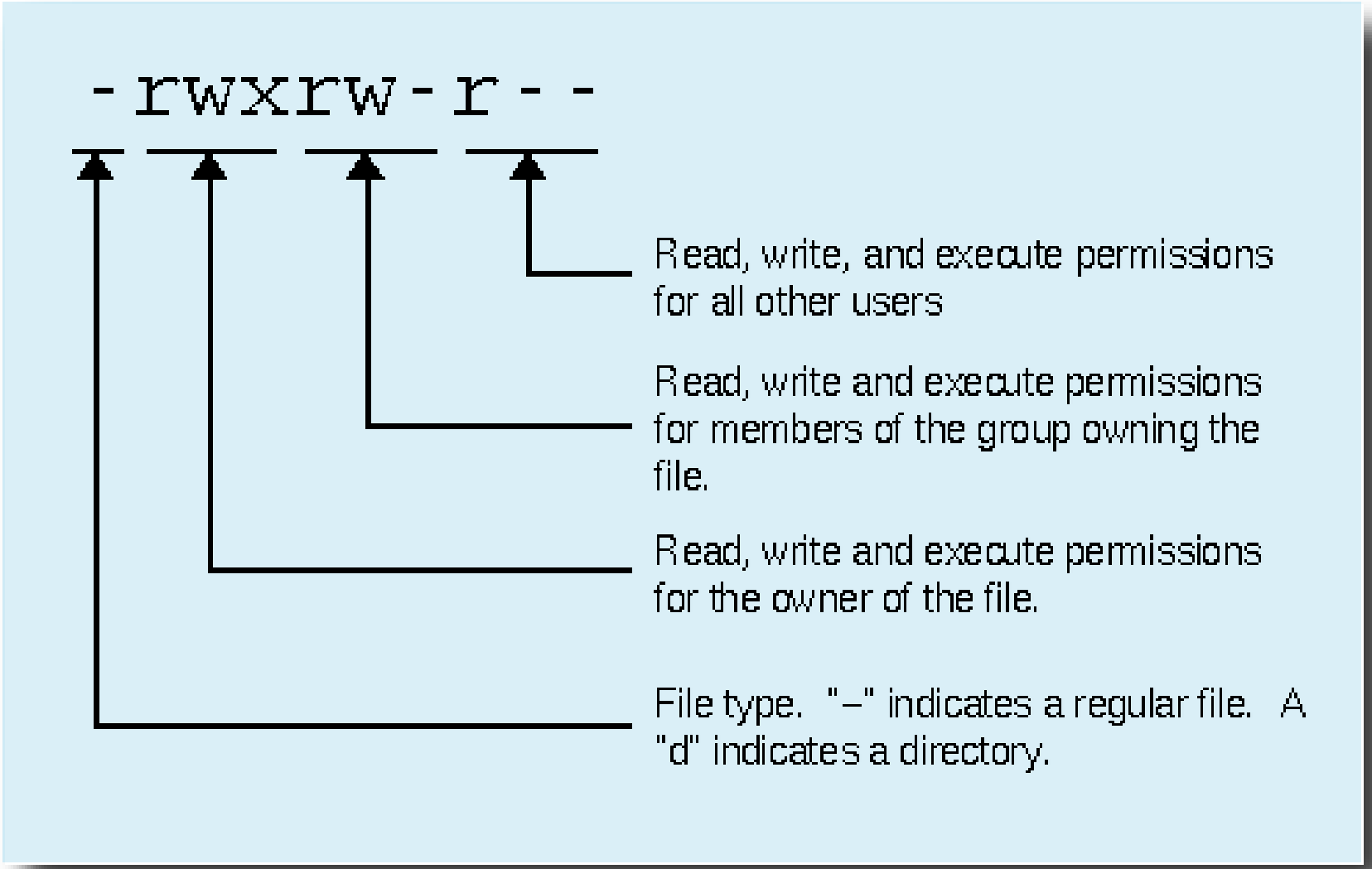
Part (1) - Linux Basics

- Introduction to Linux.
- Packages & installation process
- Command line examples
- (man, apt-get, apt-cache, find, curl, wget, touch, >, >>, |, ;, head, tail, grep, cut, sort, nano, &, ps, df, top, files permissions)

Intro to Linux

- Open Source Technology
- Hackers Friendly
- Easy packages installation
- Lots of flavors
- Etc etc

Files Permissions



Your Today Task

- **Your today task is to:**
  - install LAMP stack
  - Create a file, allow access to that file to root user ONLY.
  - You learned how to list processes, can you list p sub-processes?
  - RHCE (http://muhammedessa.com/portfolio-item/rhel7-rhcsa-rhce/)

Part (1) - Introduction Topics

- 1- OSI Model in a Nutshell (Life of a Packet)
- 2- Wireshark & NetworkMiner
- 3- TCP/UDP/HTTP/HTTPS Protocols
- 3- Nmap basics
- 4- HTTP Methods & HTTP Response Types
- 5- HTTP Headers
- 6- Web Authentication Methods, Cookies, Sessions
- 7- Encryption, Encoding, Hashing

Encryption, Encoding, Hashing

- Hashing: irreversible mathematical function that converts user input into a fixed size output. (used for Integrity checks)
- Encryption: converting human readable data/message into cipher-text, so only a person holding the right KEY can decrypt the message. (used for security purposes, authentication and authorization)
- Encoding: The purpose of encoding is to transform data so that it can be properly (and safely)

Hashing

- Irreversible (One way function)
- Fixed output size
- Examples: md4, md5, sha1, sha2 etc
- Demo time.

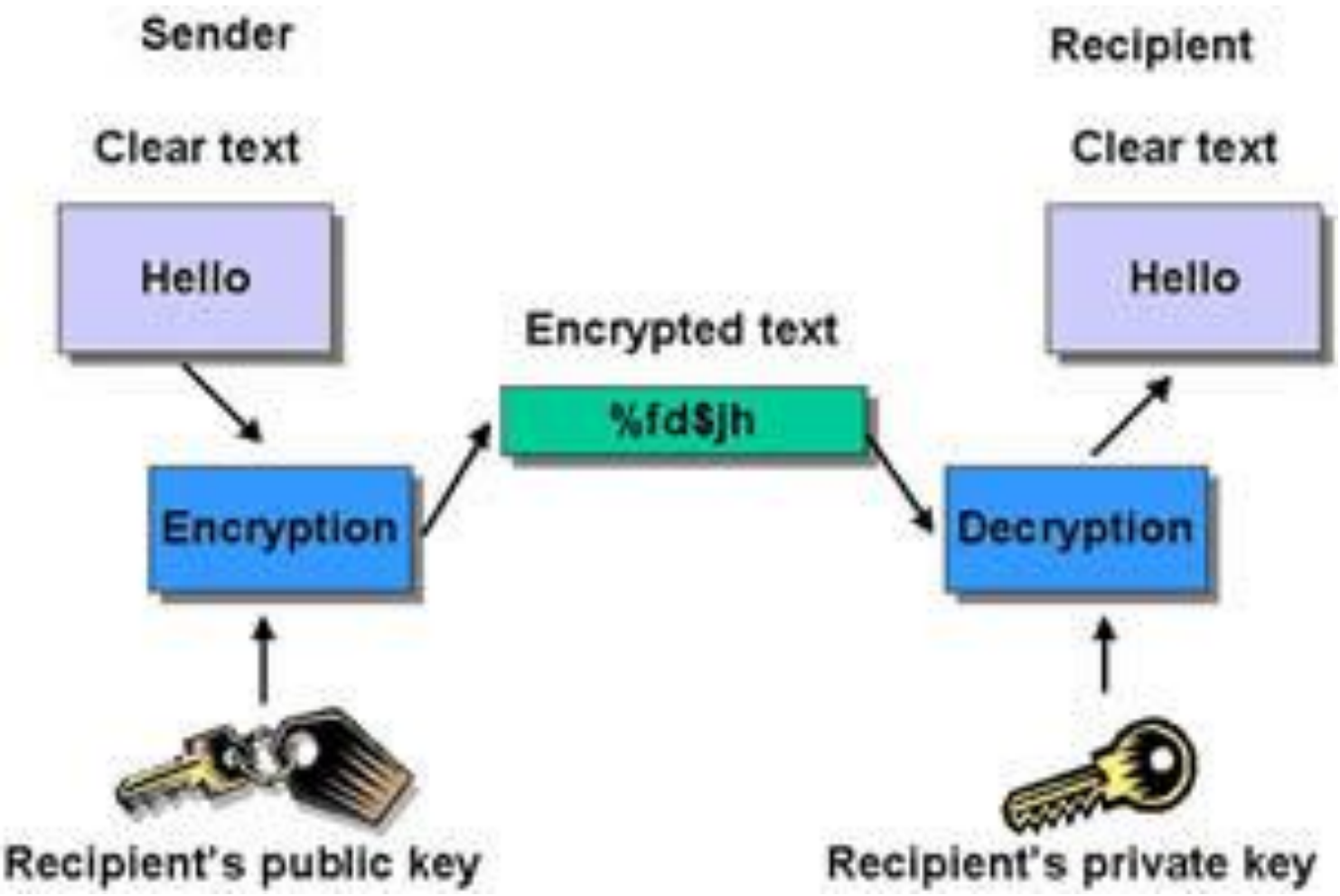
Encoding

- The purpose of encoding is to transform data so that it can be properly (and safely) consumed by a different type of system.
- Example: base64, rot13, Hex, URL, etc etc
- Demo Time!

Encryption

- Symmetric: uses the same key to encrypt and decrypt.
- Examples: AES, DES, 3DES, TwoFish, BlowFish
- Asymmetric: uses public key for encryption and private key for decryption.
- Examples: RSA, DH, DSA, ECDH etc
- Demo Time! :D

Asymmetric


Sender
Recipient
Clear text
Clear text
Hello
Hello
Encrypted text
%fd$jh
Encryption
Decryption
Recipient's public key
Recipient's private key

Encryption Demo

- Caesar Cipher (Symmetric)
- RSA (Asymmetric)
- Certificate Chain
- Browser trusted CA’s
- Generate your own public & private keys.

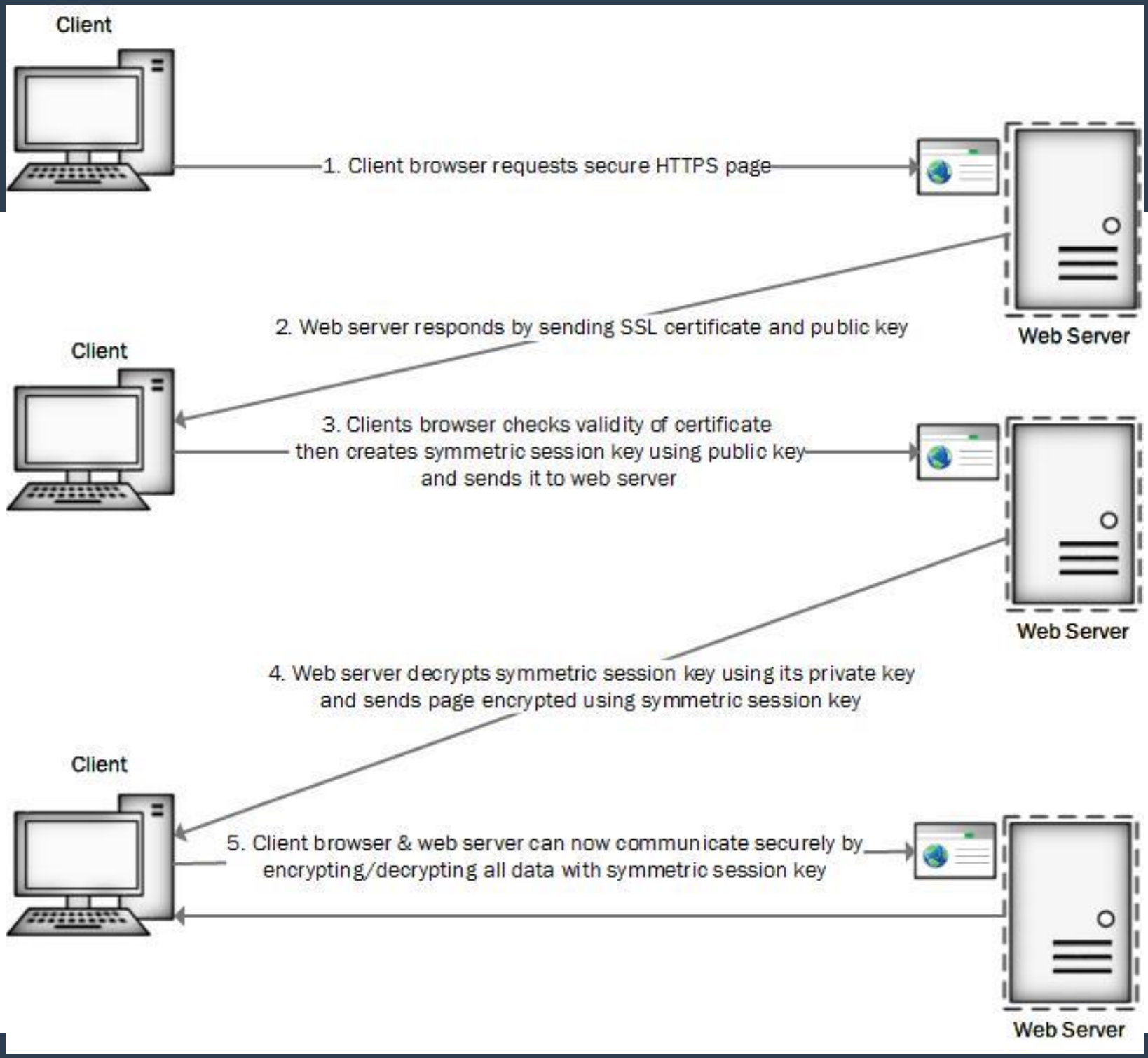
Task

- Your task for today is to watch this video:
  https://www.youtube.com/watch?v=eun8LJQ7YZs
- What is OCSP? Why we need it?
- What is root, Intermediate Certificate?
- CISSP All in one exam guide (7)

OSI Model

- What happens when I open https://www.google.com/ in my browser?
- OSI Model
- How HTTPS Works?

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable


Client
1. Client browser requests secure HTTPS page
Web Server
2. Web server responds by sending SSL certificate and public key
Client
3. Clients browser checks validity of certificate
then creates symmetric session key using public key
and sends it to web server
Web Server
4. Web server decrypts symmetric session key using its private key
and sends page encrypted using symmetric session key
Client
5. Client browser & web server can now communicate securely by
encrypting/decrypting all data with symmetric session key
Web Server

TCP vs UDP

- Every packet has:
- Source IP, Source Port, Destination IP, Destination Port.
- TCP
- How it works? Example attack? What is it used for? Example protocols?
- UDP
- How it works? Example attack? What is it used for? Example protocols?

Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Function	As a message makes its way across the internet from one computer to another. This is connection based.	UDP is also a protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because error recovery is not attempted. It is a "best effort" protocol.

TCP 3 way Handshake demo

- Wireshark Demo of how TCP 3 way handshake works.

What is DNS and how it works?

- Domain Name System
- How it works?
- Known attacks
- Different Record Types

Known attacks

- DNS Poisoning
- Subdomain Takeover
- DNS Cache Snooping
- DNS Amplification Attacks (DDOS)

Different Record Types

- A
- AAAA
- MX
- CNAME (Alias → Subdomain Takeover)
- PTR
- Tools: dig, nslookup, mxtoolbox.com

Nmap

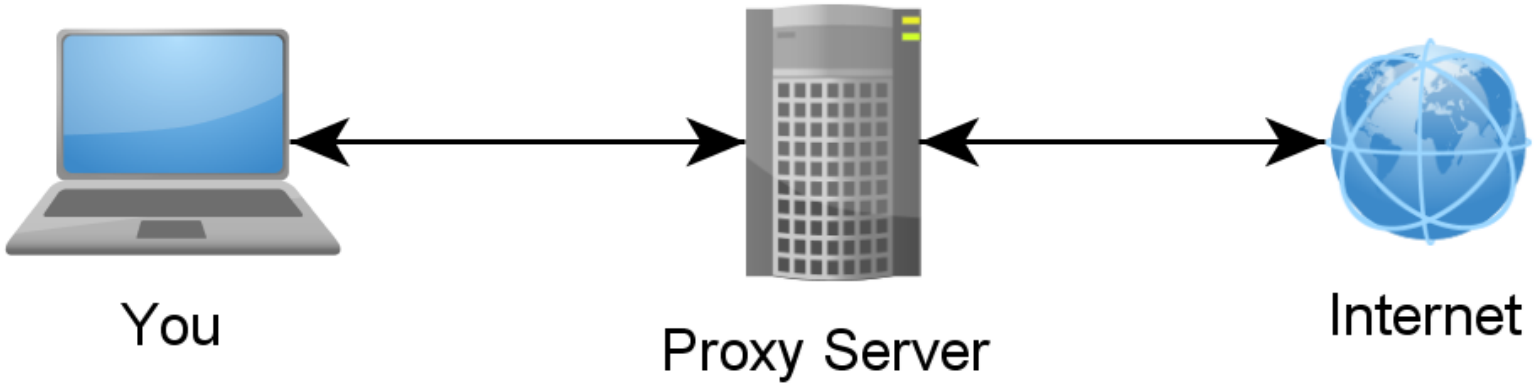
- What is Nmap and why we need it?
- Nmap basics
- Advance Nmap

BurpSuite

- What is Burp and why we need it?
- A Journey into Burp Tabs
- Burp configuration
- Get your hands dirty using burp
- Burp Documentation: https://portswigger.net/burp/help/contents.html

BurpSuite

- What is Burp and why we need it?



HTTP Methods, Headers and status codes

- HTTP Protocol
- HTTP Methods (GET, POST, DELETE, OPTIONS, HEAD ….)
- HTTP Request Headers
- HTTP Response Headers
- HTTP Status Codes
- Tasks

Tasks

- What is the difference between Cookies and Session
- What is 307 status code?
- What is WebDav?

PHP GET vs POST

- Writing your first GET and POST request (http://www.security4arabs.com/2015/04/03/how-to-start-in-webapps-security/)
- Handling user input
- Filtering user input
- XSS into demo
- Client Side vs Server side

XSS (Cross Site Scripting)

- **Reflected XSS**
- **Stored XSS**
- **Dom based XSS**
- **Demo Time**
  - Google XSS Game
  - Testphp.vulnweb.com

How to Mitigate XSS

- Response Headers
- Filter User input
- Restrict user input
- Client Side vs Server Side.

SOP, CORS, CSP

- Same origin policy requires the source Host to be the same protocol, same hostname and same port in order to read responses from other hostname. Every browser plugin has its own SOP (Flash, Java, Silverlight)
- Cross Origin Resource Sharing is a response header that allows cross origin requests.
- Content Security Policy controls which hostname is able to execute javascript, fonts, css and/or images on the target server.

Advanced XSS

- **Using XSS an attacker can steal user cookies, modify the page content, inject extra headers and more.**
- **Demo: http://185.45.192.228/stealer-xss/js.js**
  - js.js → the java script code that will steal the user cookies
  - Demo.php → PHP code to store user cookies and other user information
  - Logs.txt → user data/cookies will be stored here.

XSSI

- Cross Site Scripting Inclusion occurs when a dynamically generated javascript files holds users confidential information.
- JavaScript files doesn’t respect the SOP.

Solving XSS challenges.

- **Before we start, what are:**
  - URL vs URI, Hostname, Domain Name, TLD, Subdomain, Backend, Frontend, and Endpoint.
  - Client Side & Server Side.
- **Challenges: http://185.45.192.228/xssChall/**
  - Locating XSS payloads, html5sec.org and so on.
  - On* event handlers
  - Testing “ > < with Burp Intruder.
  - Rapid testing of XSS payloads
  - String encoding: https://mothereff.in/html-entities

CSRF – Cross-site request forgery

- What is CSRF? Example?
- DEMO
- Auto form submit
- CSRF vs SOP
- CSRF Tokens and extra headers
- Live demo on Twitter
- Mitigation Techniques

Lets earn some money!

- **Bug bounty programs**
- **Bug bounty platforms:**
  - Hackerone, Bugcrowd, SynAck
  - Vulbox, zerocopter, hackenproof.com
- **Other BBP (Google, Facebook, Telekom.de)**

Lets earn some money!

- **How to get started with Hackerone**
  - Register
  - Find a nice target and read the policy
  - Start to hunt!
  - Private programs vs Public programs.
- **How to write a nice report? CVSS? Markdown?**
- **Following up on reports? Any updates?**

Following up on reports

Lets earn some money!

- Got a bounty, now what?
- Tax forms?

Information disclosure

- Backup files (zip,tar,tgz,sql,rar,tar.gz…)
- Hidden files (.FileName)
- Source code repositories (.git, .svn)
- Source code files (.old,.bak,.php~,.swp)
- JavaScript files
- Github repositories (search github)

Information disclosure

- https://hackerone.com/reports/396467
- Tool to clone git repos to search it locally
- Dirsearch tool / Dirbuster
- Extending dirsearch list (Bo0om)
- Git / SVN extractor
- All files are on Github repo @zigoo0