Week 13 Day 3 Activity Exploring Kabana

Questions:

1 - 225 visitors from India in the past 7 days

2 – 8 Mac IOS users from China in the past 24 hours.

3 – 60% 404 and 0% 503

Wget url

curl -X POST https://reqbin.com/echo/post/json

-H 'Content-Type: application/json'

-d '{"login":"my\_login","password":"my\_password"}'

curl --cookie-jar ./ryancookies.txt --form "log=Ryan" --form "pwd=123456" <http://localhost:8080/wp-login.php>

open source intelligence (osint) links

openintel.html

<DL><p>

<DT><H3 ADD\_DATE="1624313544" LAST\_MODIFIED="1641937124">OpenIntel</H3>

<DL><p>

<DT><H3 ADD\_DATE="1625019478" LAST\_MODIFIED="1641937237">General OSINT</H3>

Click to expand inline (197 lines)

CompTIA Pentest+

Comprehensive exam covering all pen testing stages

Planning and Scoping

Information Gathering and Vulnerability Scanning

Attacks and Exploits

Reporting and Communication

Tools and Code Analysis

$381 - $949 with instructional bundle

The EC-Council Certified Ethical Hacker (CEH)

$1199 MJ says every HR interviewing is looking for this one.

OSCP

LPT master training

OSCP Pen 200 and the advanced 300

CMWDP ? mobile and web app hacking

CISST – broad and well respected cert.

OSINT – open source intelligence – google them!

Robot.txt file widely used

Port scans/brute force/social engineering --- All felonies

Googling them, not illegal

OSINT Framework.com

72.167.0.0 – 72.167.255.255 CIDR 72.167.0.0/16

IP address -72.167.191.69 – Network exploitation with nmap and Metasploit to determine the attack surface.

Server – ns25.domaincontrol.com

Email – [dns@jomax.net](mailto:dns@jomax.net)

Expire – 604800

Site:Megacorpone.com

Follow link to Index of assets notice

*Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80*

Mail server IP  
51.222.169.212

-

AS16276

-

OVH SAS

"google(dorks OR hacking)" AND (overview OR tutorial)

Crt.sh – strong tool for certificate transparency info - also port availability

In recon-ng load marketplace install recon/dona==mains-hosts/hackertarget

Modules load recon….

Keys add shodan\_api

Options list

Modules load recon/domains-hosts/hackertarget

Marketplace search shodan\_ip

Marketplace show all ?

Marketplace install recon/hosts-ports.shodan\_ip

Modules load recon/hosts-ports/shodan\_ip

Info

Options set SOURCE sans.org

Modules load recon/domain-hosts/hackertargets

Run to launch hackertargets module

Marketplace info

Marketplace search reporting/html

Marketplace install: reporting/html

Info

List

Options list

“Set customer and creator options”

Options set CREATOR scriptkiddie

Options set CUSTOMER deepdarkweb

Run

Xdg tool

Xdg-open /home/nOct1/.recon-ng