

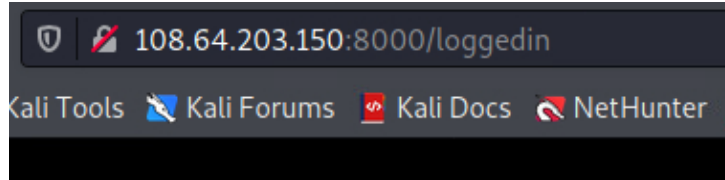
Offensive Security Table (10 points per row; 50 total points)

Host IP	1.) What was accessed, and how was it accessed? 2.) Screenshot of the machines IP address 3.) Screenshot of sensitive information, planted flags, or whatever was exploited
108.64.203.150	<p>1.) I gained access to the web server through access to a web shell at the url of //lehs. This was running as root so I added a user with a uid 0 and deleted their password. I then logged in through ssh and had root access on the machine as well. I planted two flags in the /ISSUES_WITH_SERVER directory.</p> <pre data-bbox="365 489 1433 751">root@ubuntu18:/ISSUES_WITH_SERVER# ifconfig ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 108.64.203.150 netmask 255.255.255.0 broadcast 108.64.203.255 inet6 fe80::202:31ff:fe15:6618 prefixlen 64 scopeid 0x20<link> ether 00:02:31:15:66:18 txqueuelen 1000 (Ethernet) RX packets 1394898 bytes 165037003 (165.0 MB) RX errors 0 dropped 3949 overruns 0 frame 0 TX packets 134277 bytes 35587981 (35.5 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre> <p>2.)</p> <p>3.) Issues Flags:</p> <pre data-bbox="357 835 1021 972">root@ubuntu18:/# cd ISSUES_WITH_SERVER/ root@ubuntu18:/ISSUES_WITH_SERVER# ls ssh_issue web_shell root@ubuntu18:/ISSUES_WITH_SERVER#</pre>
108.64.203.175	<p>1.) I gained access to the surprise machine through easy to guess login as cpre231/cpre231 on an open telnet connection. This user is a sudoer so I had complete access to the machine. I added a user jboicken and planted a flag in the / directory that agrees with a previously left flag.</p> <p>2.)</p> <pre data-bbox="365 1262 1450 1524">cpre231@surprise:~\$ ifconfig ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 108.64.203.175 netmask 255.255.255.0 broadcast 108.64.203.255 inet6 fe80::202:31ff:fe15:661e prefixlen 64 scopeid 0x20<link> ether 00:02:31:15:66:1e txqueuelen 1000 (Ethernet) RX packets 817095 bytes 80885850 (80.8 MB) RX errors 0 dropped 1524 overruns 0 frame 0 TX packets 97130 bytes 7690111 (7.6 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre> <p>3.) “Yes_I_Agree --- >” Flag:</p> <pre data-bbox="357 1566 1037 1686">vmlinuz.old YoUr_DeFaULT_CreDs_ArE_BaD 'Yes_I_Agree—>'</pre>

108.64.203.150

- 1.) On the web server, I was able to access a page at /addUser. This let me add a user Jacob who is an employee user. As well, in the change password page, I was able to find out how many users existed by entering in my password incorrectly. This revealed the existence of 3 other users.

2.)



- 3.) User registration and loggedin errors:

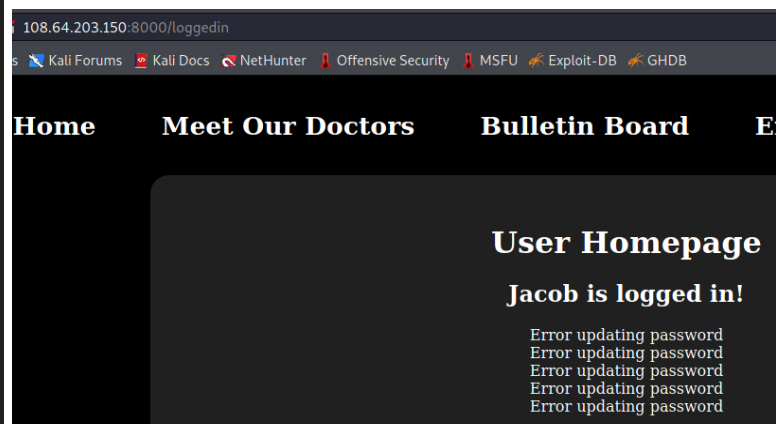
User Account Registration

Username

Password

User Number

☒ Employee
☐ Patient



215.127.208.150

- 1.) Unlike the previous web server, this one had removed the /llehs url. However, it still contains the command parsing script and the hidden web shell in the home page. But the ssh daemon prevented root login and passwordless login, so I used the root web shell to add a user jboicken, add them to the sudo group, and set their password to toor using the chpasswd command.

```
$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 215.127.208.150 netmask 255.255.255.0 broadcast 215.127.208.255
    inet6 fe80::202:31ff:fe15:2b18 prefixlen 64 scopeid 0x20
    ether 00:02:31:15:2b:18 txqueuelen 1000 (Ethernet)
    RX packets 3975379 bytes 687657983 (687.6 MB)
    RX errors 2 dropped 18444 overruns 0 frame 0
    TX packets 630504 bytes 114951803 (114.9 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0
```

2.)

- 3.) Adding user and access to /etc/shadow:

useradd jboicken

Send Command

```

djwolfe:$1$yGKbDvrX$ohyFYF5SVw61R0DDHv4CB0:18746:0:99999:7:::
jboicken:$6$hwOoNtUZ$xWxwtNtiQczlySQAbKGXmNpX9yevE3ds3
/18746:0:99999:7:::

```

215.127.208.175

1.) I connected via ftp and login in as anonymous ie in anonymous mode. This is meant to chroot me into a directory, but it contains a link to / allowing me to bypass that. From there, I was able to access many files that should be root only like /etc/shadow. I then copied shadow from the server.

2.)

```
(root@kali)-[~] # nmap -sC -sV -p 21 -oN nmap.txt --host 215.127.208.175
# ftp 215.127.208.175 -P 100.64.203.152
Connected to 215.127.208.175.
220 Better Hack Yourself before you Wreck Yourself! 18:18:52 CDT
Name (215.127.208.175:root): anonymous
331 Please specify the password.
Password: 100-filtered-ports
230 Login successful.
```

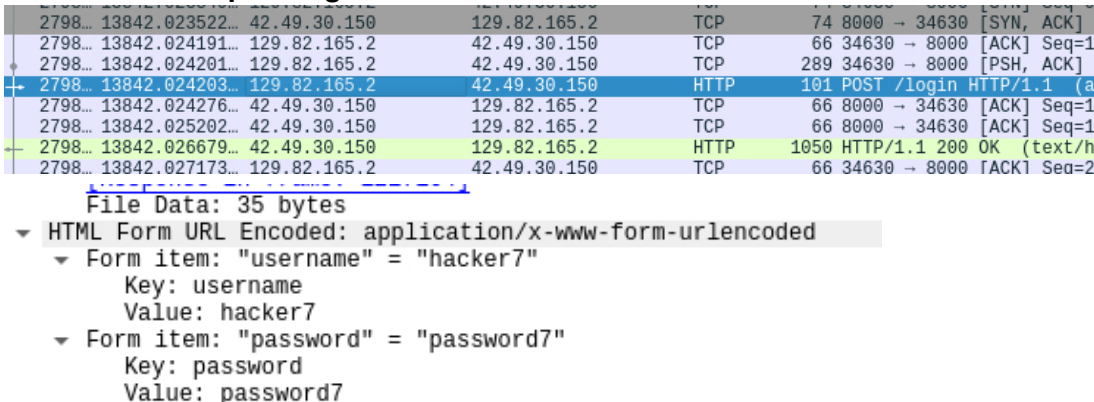
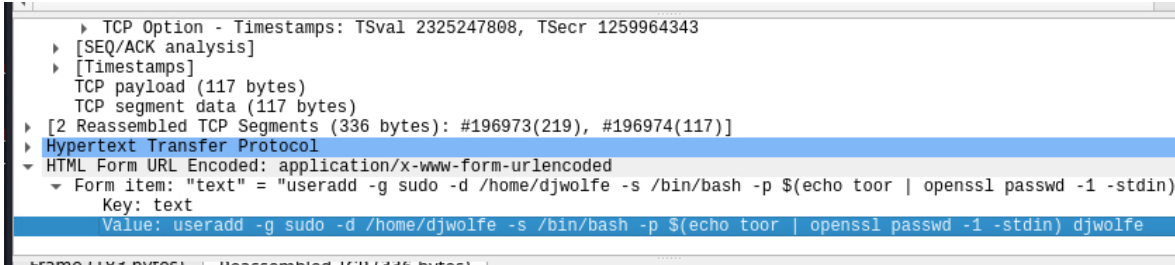
3.) Retrieved shadow file:

```
ftp> get shadow
local: shadow remote: shadow
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shadow (2246 bytes).
226 Transfer complete.
2246 bytes received in 0.00 secs (853.7794 kB/s)
ftp> exit
221 Goodbye.

# ls
Desktop Documents Downloads Kazam_screenshot_00000.png Music Pictures Public shadow Templa

# cat shadow
root!:17394:0:99999:7:::
daemon*:17001:0:99999:7::: (omnip.org) at 2021-04-28 19:00 CDT
bin*:17001:0:99999:7:::
sys*:17001:0:99999:7::: ncy
sync*:17001:0:99999:7:::
games*:17001:0:99999:7:::
```

Incident Response Table (10 points per row; 50 total points)

Host IP	<ol style="list-style-type: none"> 1.) What was accessed? 2.) How was it accessed? 3.) What was the impact of the incident? 4.) How did you respond to the incident? 5.) Screenshot of what was accessed
42.49.30.150	<ol style="list-style-type: none"> 1.) Using wireshark, I found continuous attempts to login to my web server from the ip of 129.82.165.2. 2.) This attacker is trying to brute force the login page of the web server by posting numerous usernames and password to the /login web page. 3.) If the one of our patients or employees has a commonly used password / is easily vulnerable to dictionary attacks, then the attacker could get into their account and modify it or anything they have access to. This violates the ideas of CIA for these users and the server. 4.) To minimize such an attack, we can put a timeout after X attempts to login on an account and alerting users that someone is trying to force into their account. As well, we can enforce password requirements so that it cannot be easily guessed. 5.) Wireshark attempted login: 
42.49.30.150	<ol style="list-style-type: none"> 1.) Using wireshark, I found an attempt to send commands to my server and add a user from the ip 8.196.164.2. 2.) My web server allows for a post request on its home page i.e. / url, so this user was able to send a command as a string to the page in hopes it would execute as a shell command. 3.) My web server is not running as root so useradd could not be run. But if commands are able to be run, they could modify and read whatever the server has access to. 4.) To fix this, I should remove the post request and script that are allowing commands to be passed and could chroot/jail the server so that it cannot gain access to information unless vital. 5.) 

42.49.30.175	<ol style="list-style-type: none"> 1.) I found a flag on my /root directory saying I have a backdoor on my machine. 2.) I checked my /etc/shadow and found that I have a user called backdoor who has no password and shares the uid of root 0. The attacker must have connected through the open telnet port to log in. 3.) This backdoor user was root, so they could modify and access any data on the machine. Thus affecting all ideas of the CIA of this machine. 4.) I removed the user backdoor to prevent logins from such users again. 5.) <pre> root@surprise:~/pwned# ls backdoor_gotcha root@surprise:~/pwned# </pre>
42.49.30.175	<ol style="list-style-type: none"> 1.) I was checking my logs for ftp and found that someone had logged in anonymously from the 219.27.173.2 address. 2.) Looking at my configuration for vsftpd, I found that anonymous login was turned on but chrooted and that uploads are chowned to root. I anon logged on via ftp and found that it was chrooted but contained a link to /. 3.) This allows for anyone to login and upload files that are owned by root. As well, they are able to download files that anyone one can read, which /etc/shadow happened to be. This comprises confidentiality and integrity of the data on this machine. 4.) I disabled anon login for vsftpd and chmod vital files that only root should be able to access. 5.) Login in logs by anon: <pre> Fri Apr 23 09:43:38 2021 [pid 2512] [ftp] OK LOGIN: Client "::ffff:219.27.173.2", anon password "IEU ser@" Fri Apr 23 09:43:38 2021 [pid 2522] CONNECT: Client "::ffff:219.27.173.2" Fri Apr 23 09:43:38 2021 [pid 2527] CONNECT: Client "::ffff:219.27.173.2" Fri Apr 23 09:43:38 2021 [pid 2517] [ftp] OK LOGIN: Client "::ffff:219.27.173.2", anon password "IEU ser@" </pre>
42.49.30.175	<ol style="list-style-type: none"> 1.) Further checking of my ftp logs showed that some had logged into ftp as the cpre231 user. 2.) The password for cpre231 is "cpre231" so the attacker must have guessed/brute forced and found the password by connecting through ftp. 3.) The user cpre231 is a sudoer, so this attacker now had root shell access if they logged in through the open telnet. This would compromise all of CIA for this machine. 4.) I set up a firewall using ufw to prevent any further attacks from outside of the local ip range and changed the password for the cpre231. 5.) <pre> Fri Apr 23 10:09:03 2021 [pid 2878] CONNECT: Client "::ffff:219.27.173.2" Fri Apr 23 10:09:05 2021 [pid 2877] [cpre231] OK LOGIN: Client "::ffff:219.27.173.2" Fri Apr 23 10:45:55 2021 [pid 3499] CONNECT: Client "::ffff:219.27.173.2" Fri Apr 23 10:45:55 2021 [pid 3498] [cpre231] OK LOGIN: Client "::ffff:219.27.173.2" Fri Apr 23 10:46:35 2021 [pid 3503] CONNECT: Client "::ffff:219.27.173.2" Fri Apr 23 10:46:35 2021 [pid 3502] [RSDWL5] FAIL LOGIN: Client "::ffff:219.27.173.2" Fri Apr 23 10:46:36 2021 [pid 3506] CONNECT: Client "::ffff:219.27.173.2" Fri Apr 23 10:46:36 2021 [pid 3505] [2bS3dH] FAIL LOGIN: Client "::ffff:219.27.173.2" Fri Apr 23 10:48:16 2021 [pid 3520] CONNECT: Client "::ffff:219.27.173.2" </pre>