

PHASE 1 - Ping

Hollywood IPs

- `fping -s -g 15.199.95.80 15.199.95.95`
 - All 16 unreachable
- `fping -s -g 15.199.94.80 15.199.94.95`
 - All 16 unreachable
- `fping -s -g 11.199.158.80 11.199.158.95`
 - All 16 unreachable
- `fping 167.172.144.11`
 - 167.172.144.11 is alive
- `fping -s -g 11.199.141.80 11.199.141.95`
 - All 16 unreachable

Out of all IPs (from the rock star corp list), only 2 are alive

12.205.151.1 - New York Database servers

167.172.144.11 - Hollywood Application Servers

- The vulnerability is that one of Hollywood's IPs is accepting connections.
- You can mitigate this risk by ensuring there is a firewall for each server.

***** Layer 3 is where these findings are *****

PHASE 2 - SYN Scan

sudo nmap 12.205.151.1 -sS

“Starting Nmap 7.60 (<https://nmap.org>) at 2021-11-02 22:01 EDT
Nmap scan report for 12-205-151-1.static.cpe.att.net (12.205.151.1)
Host is up (0.0013s latency).
All 1000 scanned ports on 12-205-151-1.static.cpe.att.net (12.205.151.1) are filtered

Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds”

sudo nmap 167.172.144.11 -sS

“Starting Nmap 7.60 (<https://nmap.org>) at 2021-11-02 22:02 EDT
Nmap scan report for 167.172.144.11
Host is up (0.0024s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
22/tcp open ssh

Nmap done: 1 IP address (1 host up) scanned in 11.99 seconds”

- **The vulnerability would be that if port 22 is open, attackers can try to access the host machine.**
- **This risk can be mitigated by running scans to find which ports are open and exposing a risk for attacks.**

***** Port 22 is open and SYN scan is run on layer 4 *****

PHASE 3

ssh jimi@167.172.144.11 -p 22

```
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ ssh jimi@167.172.144.11 -p 22
The authenticity of host '167.172.144.11 (167.172.144.11)' can't be established.
ECDSA key fingerprint is SHA256:mDZ8+Ud+K3Y6XNWvtyAR4Q2ti1+/V3p0Bm83hF6Ua4w.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '167.172.144.11' (ECDSA) to the list of known hosts.
jimi@167.172.144.11's password:
Linux GTscavengerHunt 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov  3 02:12:41 2021 from 45.29.51.35
Could not chdir to home directory /home/jimi: No such file or directory
jimi$
```

Jimi is not part of the sudoers so i changed directories into etc and used the command **cat hosts**

```
python2.7
python3
jimi$ cat /etc/hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#    /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 GTscavengerHunt.localdomain GTscavengerHunt
127.0.0.1 localhost
98.137.246.8 rollingstone.com

# Following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

jimi$
```

“nslookup 98.137.246.8
8.246.137.98.in-addr.arpa name = unknown.yahoo.com.

Authoritative answers can be found from:”

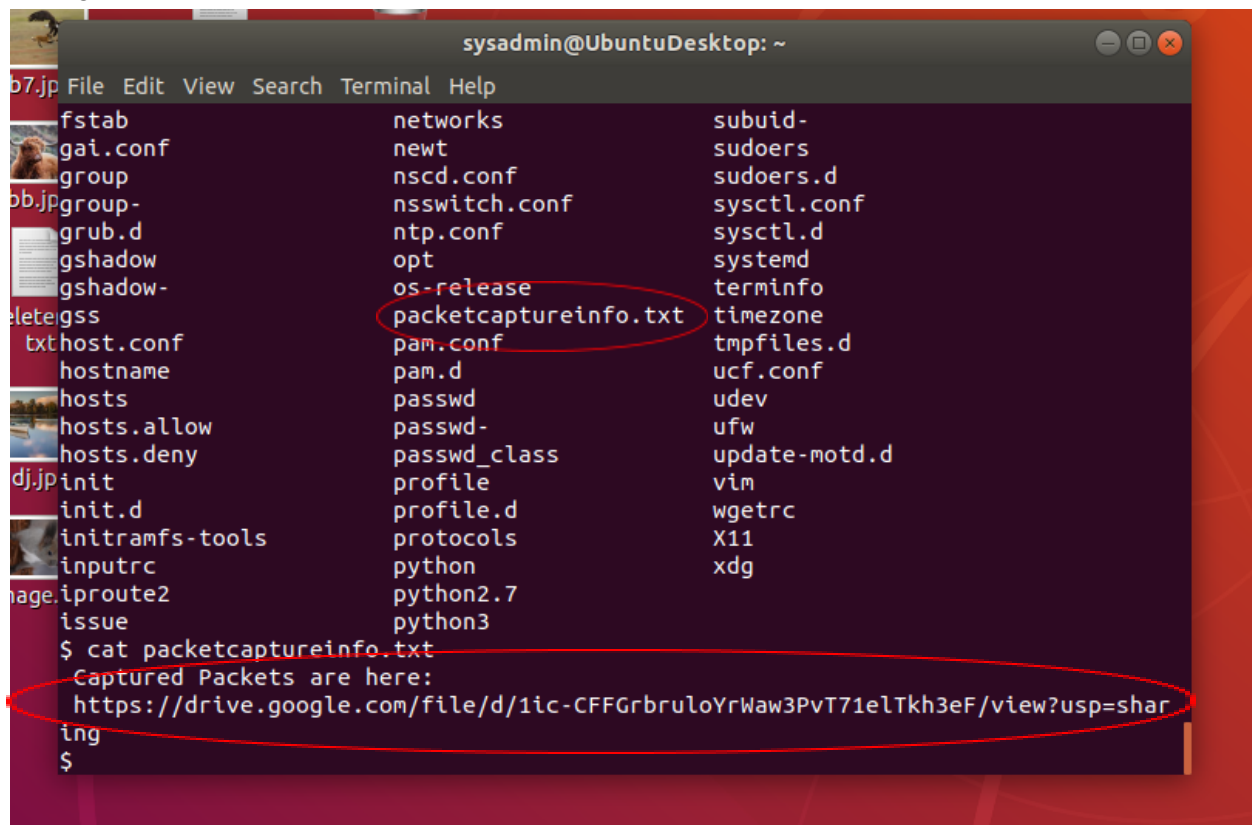
- The vulnerability is that the redirected website can have malicious code to infect the machine that visits that site.
- You can mitigate the risk of this file being modified by making sure only select users have access to it.

*** Layer 7 is where these findings are ***

PHASE 4

ssh jimi@167.172.144.11 -p 22

Changed directories into etc and then used: `cat packetcaptureinfo.txt`



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
fstab networks subuid-  
gai.conf newt sudoers  
group nscd.conf sudoers.d  
group- nsswitch.conf sysctl.conf  
grub.d ntp.conf sysctl.d  
gshadow opt systemd  
gshadow- os-release terminfo  
etc gss packetcaptureinfo.txt timezone  
host.conf pam.conf tmpfiles.d  
hostname pam.d ucf.conf  
hosts passwd udev  
hosts.allow passwd- ufw  
hosts.deny passwd_class update-motd.d  
init profile vim  
init.d profile.d wgetrc  
initramfs-tools protocols X11  
inputrc python xdg  
iproute2 python2.7  
issue python3  
$ cat packetcaptureinfo.txt  
Captured Packets are here:  
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71eLTkh3eF/view?usp=sharing  
$
```

Downloaded the `secretlogs.pcapng`

Opened pcap in wireshark and filtered by using > `http.request.method == "POST"`

HTML Form URL Encoded: `application/x-www-form-urlencoded`

Form item: "0<text>" = "Mr Hacker"

Form item: "0<label>" = "Name"

Form item: "1<text>" = "Hacker@rockstarcorp.com"

Form item: "1<label>" = "Email"

Form item: "2<text>" = ""

Form item: "2<label>" = "Phone"

Form item: "3<textarea>" = "Hi Got The Blues Corp! This is a hacker that works at Rock Star Corp. Rock Star has left port 22, SSH open if you want to hack in. For 1 Million Dollars I will provide you the user and password!"

Form item: "3<label>" = "Message"

Form item: "redirect" =

"http://www.gottheblues.yolasite.com/contact-us.php?forml660593e583e747f1a91a77ad0d3195e3Posted=true"

Form item: "locale" = "en"

Form item: "redirect_fail" =
"http://www.gottheblues.yolasite.com/contact-us.php?forml660593e583e747f1a91a77ad0d3195e3Posted=false"
Form item: "form_name" = ""
Form item: "site_name" = "GottheBlues"
Form item: "wl_site" = "0"
Form item: "destination" =
"DQvFymnlKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkq==:3gjpzwPaByJLFCa2ouelFsQG6ZzGkhh31_Gl2mb5PGk="

Form item: "g-recaptcha-response" =
"03AOLTBQLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOIs6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6l8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u"

- **The vulnerabilities are that the hacker is messaging someone else with credentials to hack into the system and trying to take the IP of someone else.**
- **This risk can be mitigated by ensuring there is a set amount of requests that can be made before the system is alerted.**

***** Layer 2 is where these findings are *****