Sidney Robinson

* The steps and commands used to complete the tasks.

***PHASE1:***

*sysadmin@UbuntuDesktop:/03-student$ fping -g 167.172.144.11/32*

*167.172.144.11 is alive*

***PHASE2:***

*Nmap done: 16 IP addresses (16 hosts up) scanned in 335.64 seconds*

*sysadmin@UbuntuDesktop:/03-student$ sudo nmap -sS 167.172.144.11/32*

*Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-15 22:46 EDT*

*Nmap scan report for 167.172.144.11*

*Host is up (0.0046s latency).*

*Not shown: 999 filtered ports*

*PORT STATE SERVICE*

*22/tcp open ssh*

***PHASE3:***

*sysadmin@UbuntuDesktop:/03-student$ ssh jimi@167.172.144.11 -p22*

*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:*

*Permission denied, please try again.*

*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: Mon Aug 16 02:23:31 2021 from 172.98.66.166*

*Could not chdir to home directory /home/jimi: No such file or directory*

*$ ls*

*bin boot dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old*

*$*

***ALSO;***

*$ whoami*

*jimi*

*$ cd /etc*

*$ more hosts*

*# Your system has configured 'manage\_etc\_hosts' as True.*

*# As a result, if you wish for changes to this file to pers*

*ist*

*# then you will need to either*

*# a.) make changes to the master file in /etc/cloud/templat*

*es/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*

*oooooooollowing 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*

*$*

***ALSO;***

*sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8*

*8.246.137.98.in-addr.arpa name = unknown.yahoo.com.*

*Authoritative answers can be found from:*

*sysadmin@UbuntuDesktop:~$*

***ALSO;***

*sysadmin@UbuntuDesktop:~$ sudo nslookup rollingstone.com*

*[sudo] password for sysadmin:*

*Server: 8.8.8.8*

*Address: 8.8.8.8#53*

*Non-authoritative answer:*

*Name: rollingstone.com*

*Address: 151.101.128.69*

*Name: rollingstone.com*

*Address: 151.101.64.69*

*Name: rollingstone.com*

*Address: 151.101.192.69*

*Name: rollingstone.com*

*Address: 151.101.0.69*

*sysadmin@UbuntuDesktop:~$*

***PHASE4:***

$ more packetcaptureinfo.txt

Captured Packets are here:

https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71e

lTkh3eF/view?usp=sharing

* A summary of your findings for each testing phase.

***PHASE1****:*

*The following ranges reported back as unreachable:*

*15.199.95.91/28, 15.199.94.91/28, 11.199.158.91/28, 11.199.141.91/28*

*The following range reported back as alive: 167.172.144.11/32*

***PHASE2:***

*The following ranges have filters:*

*15.199.95.91/28, 15.199.94.91/28, 11.199.158.91/28, 11.199.141.91/28*

*The following range: 167.172.144.11/32 – has an unfiltered and open port;*

*Nmap scan report for 167.172.144.11*

*Host is up (0.0046s latency).*

*Not shown: 999 filtered ports*

*PORT STATE SERVICE*

*22/tcp open ssh*

***PHASE3:***

*Nslookup revealed that ip 98.137.246.8 belongs to 8.246.137.98.in-addr.arpa name = unknown.yahoo.com.*

*This means that rollingstone.com was DNS spoofed on the RockStar server*

***PHASE4:***

***ALSO WIRESHARK FOUND IN PCAP FILE:***

Arrival Time: Aug 15, 2019 09:01:46.812715977 EDT

Transmission Control Protocol, Src Port: 80, Dst Port: 33546, Seq: 1, Ack: 1821, Len: 364

Source Port: 80

Destination Port: 33546

[Stream index: 7]

Status Code: 303

[Status Code Description: See Other]

Connection: keep-alive\r\n

Access-Control-Allow-Origin: \*\r\n

Cache-Control: no-cache\r\n

Location: http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true\r\n

[Request URI: http://forms.yola.com/formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76fa/I660593e583e747f1a91a77ad0d3195e3/]

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

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

Key: 0<text>

Value: Mr Hacker

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

Key: 0<label>

Value: Name

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

Key: 1<text>

Value: Hacker@rockstarcorp.com

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

Key: 1<label>

Value: Email

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

Key: 2<text>

Value:

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

Key: 2<label>

Value: 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 Milliion Dollars I will provide you the user and password!"

Key: 3<textarea>

Value: 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 Milliion Dollars I will provide you the user and password!

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

Key: 3<label>

Value: Message

Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"

Key: redirect

Value: http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true

Form item: "locale" = "en"

Key: locale

Value: en

Form item: "redirect\_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"

Key: redirect\_fail

Value: http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false

Form item: "form\_name" = ""

Key: form\_name

Value:

Form item: "site\_name" = "GottheBlues"

Key: site\_name

Value: GottheBlues

Form item: "wl\_site" = "0"

Key: wl\_site

Value: 0

Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ\_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31\_Gl2mb5PGk="

Key: destination

Value: DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ\_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31\_Gl2mb5PGk=

Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u

Key: g-recaptcha-response

Value [truncated]: 03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6uW0-aWc711YdgRnK3y

* Any network vulnerabilities discovered.

***PHASE1:****Since the network range: 167.172.144.11/32 reported back as alive hackers could focus attacks against that ip range.*

***PHASE2:*** *We have discovered and open tcp ssh doorway on port 22 within the 167.172.144.11/32 IP range*

***PHASE3:***  *The RockStar server has been breached and a DNS spoof was successfully put in place by a bad actor*

***PHASE4:***

*Port 22 ssh is open and a bad actor is willing to exploit it.*

* Findings associated with a hacker.

***PHASE1:*** *None yet, but noted the alive and unreachable ip ranges*

***PHASE2:*** *None yet, but noted a open tcp ssh doorway on port 22 within the 167.172.144.11/32 IP range*

***PHASE3:***  *The RockStar server has been breached and a DNS spoof was successfully put in place by a bad actor*

***PHASE4:*** *A hacker who calls himself Mr Hacker has sent an email to* [*www.gottheblues.yolasite.com*](http://www.gottheblues.yolasite.com) *informing them that port 22 ssh is open and asking for 1 million dollars to give gotheblues credentials to hack RockStar.*

* Recommended mitigation strategy.

***PHASE1:*** *Develop a strategy to firewall and actively monitor all ip ranges.*

***PHASE2:*** *Make plans to filter, firewall and secure port 22 within the 167.172.144.11/32 IP range*

***PHASE3:*** *Find and investigate pcap files collect evidence*

***PHASE4:*** *Close port 22 ssh and harden the RockStar server user password access*

* Document the OSI layer where the findings were found.

***PHASE1:*** *OSI layer 3) Network layer*

***PHASE2:*** *OSI layer7) Application layer*

***PHASE3:*** *OSI layer 3) Network layer*

***PHASE4:*** *OSI layer7) Application layer && OSI layer 2) Data link*