CONFIDENTIAL

ROCKSTAR CORP

Network Vulnerability Assessment

Conducted by

Don't get rooted keep them booted.

CONFIDENTIAL

THIS PAGE IS INTENTIONALLY LEFT BLANK

Preface

This document, prepared by b00tr00t engineers, contains proprietary and confidential information of a highly sensitive nature. Reproduction or distribution without the express written permission of b00tr00t or RockStar Corp is strictly prohibited. b00tr00t engineers identified existing and potential vulnerabilities and collected evidence of malicious activity on behalf of RockStar Corp. b00tr00t engineers provided remediation advice to RockStar Corp. Findings identified by b00tr00t were not validated as corrected.

Please contact RockStar Corp for further information regarding these findings and their resolution status.

Detailed logs can be found in the resource folder

Disclaimer

b00tr00t conducted this testing on the applications and systems that existed as of September 2020, but security threats are changing daily. This report intends only to provide documentation investigation conducted by b00tr00t during September 2020. This report cannot and does not protect against personal or business loss as the result of the use of the applications or systems described. b00tr00t offers no warranties, representations or legal certifications concerning the applications or systems it tests. b00tr00t makes no claim, and this document doesn't represent or warrant the completion was without error, nor the application is, tested, suitable, and free of any defects. This document doesn't ensure compliance with any industry, standard, provider, accreditation or organisation. By commissioning and accepting the report, submitted by b00tr00t on the 26th of September 2020, you agree b00tr00t shall not be held responsible for any losses or damages, caused to you, or anybody else, by anything, in any way, ever.

Contents

1. Purpose

b00tr00t was contracted by RockStar Corp to perform an investigation and network vulnerability assessment in response to suspicious cyber activity.

2. Scope

The scope of this investigation is limited to RockStar Corps Hollywood Servers. RockStar Corp requested r00tb00t probe `ICMP` configuration, open ports and investigate employee reports of suspicious cyber activity.

b00tr00t has defined the scope as follows;

- *Assess RockStar Corp's Hollywood network*
- *Probe hosts and document response to `ICMP`*
- *Scan and document host ports*
- *Investigate suspicious activity*
- *If possible, correct or adequately mitigate any discovered threats*
- *Provide RockStar Corp investigation summary*
- *Provide RockStar Corp a mitigation strategy*

Hosts in scope by IP address
11.199.141.91/28
11.199.158.91/28
15.199.94.91/28
15.199.95.91/28
167.172.144.11/32
Hosts in scope by location
Hollywood
Hosts not in scope by location
New York
Miami
Chicago
Test Limitations
PrivEsc, Hash Cracking, DoS

3. Summary of results

The investigation and testing of RockStar Corp's Hollywood branch resulted in the discovery that Hollywood Application Server, with the IP of `167.172.144.11/32`*, had been breached. b00tr00t identified thirteen misconfigurations and multiple potential vulnerabilities, of varying severity, but no evidence it leads to an attacker(s)* **initial***, attack surface and entry. Further enumeration and forensic analysis by b00tr00t lead to the discovery of a modified* `/etc/hosts` *file, evidence of* `DNS` *cache poisoning and a text file in the same* `/etc/` *folder named* `packetcaptureinfo.txt`*. The text file contained a Google drive download link to a Wireshark network traffic capture file. b00tr00t evaluated the data and concluded it was of the RockStar Corp Hollywood Servers. b00tr00t engineers searched the captured network traffic for suspicious activity and uncovered evidence that would suggest an insider threat is most likely responsible for the attacker's initial entry.*

3.1. Positive findings

b00tr00t found the overall security of the network to be relatively secure. b00tr00t engineers documented evidence of a firewall named `fail2ban` *that filtered attempts from simple port scans and, mostly acceptable security practices for server configuration and other features, such as* `sudo`*,* `crontabs`*, and* `file permissions`*, that would mitigate various textbook privileged escalation attacks.*

Findings tallied by Risk Rating						
Observation	**High**		**Medium**		**Low**	
	Corrected	**Pending**	**Corrected**	**Pending**	**Corrected**	**Pending**
Network Breach		✖				
Keylogger		✖				
DNS Spoofing		✖				
Weak brute force protection		✖				
Weak credentials		✖				
DNS cache poisoning		✖				
ICMP Enabled				✖		
SSH Enabled on default port				✖		
SSH Permit root login				✖		
SFTP login for a standard user				✖		
wget for a standard user				✖		
Bash for a standard user				✖		

ICMP Results		
✔ REJECTING	15.199.95.91/28	Hollywood Database Servers
✔ REJECTING	15.199.94.91/28	Hollywood Web Servers
✔ REJECTING	11,188,158.91/28	Hollywood Web Servers
✔ REJECTING	11.199.141.91/28	Hollywood Application Servers
✖ ACCEPTING	167.172.144.11/32	Hollywood Application Servers

*Fig 1. Hosts blocking **ICMP** requests are colour coded green showing they are compliant.*

167.172.144.11/32	
Location	*Hollywood*
OS	*Debian GNU/Linux 9 (stretch)*
CPU	*Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz*
RAM	*4096K*
Kernel	*Linux GTscavengerHunt 4.9.0-11-amd64*
Hostname	*GTscavengerHunt*
Open Ports	*TCP - 22, 5355*
	UDP – 53, 123, 4355
SSH	*Allowed*
SFTP	*Allowed*
ICMP	*Allowed*
PermitRootLogin	*Yes*
Crontabs	*Protected*

Fig 2. Points of interest are colour coded red.

4. Recommendations

Network Breach *High Severity*

Synopsis:

Evidence of network breach

Description:

Discovery of a suspicious file containing network traffic capture data, later confirmed Hollywood network traffic, that there was a network breach and uncovered evidence that suggests it was an inside actor that allowed attackers initial access

Solution:

- *Change all account password*
- *Future enumerate system for any of the attacker's activity*
- *Take correct identified vulnerabilities*
- *Unmask internal threat actor.*
- *Schedule regular security audits to and ensure patching is adequate*

Key Logger — High Severity

Synopsis:

Evidence of network traffic requesting keylogger

Description:

Discovery of a suspicious file containing network traffic capture data, later confirmed Hollywood network traffic that contained data suggesting an attacker may have downloaded a keylogger onto the network.

Solution:

- *Run virus and malware scanning check install logs and ensure its adequate removal*

DNS Spoofing — High Severity

Synopsis:

Modified DNS cache records in `/etc/hosts` file.

Description:

Discovery of a suspicious file containing network traffic capture data later confirmed Hollywood network traffic that included information suggesting an insider thread as a potential initial entry point.

Solution:

- *Remove `DNS` entry from `/etc/hosts`*
- *Consider installing program suck as tripwire so monitor for file changes*

Weak Login Credentials — High Severity

Synopsis:

Weak default login credentials supplied for testing

Description:

b00tr00t were supplied weak default login details to access servers for testing and analysis

Solution:

- *Enforce strict password policy ensure users use passwords over at least 12 characters long*
- *Ensure log in has max auth and time outs to stop brute-forcing*

ICMP Enabled — Medium Severity

Synopsis:

`ICMP` traffic was incorrectly filtered and replying to `fping` requests.

Description:

Server discovery and port scanning was possible via `fping` and `nmap`

Solution

- *Edit `/proc/sys/net/ipv4/icmp_echo_ignore_all` and set value to `1`*
- *Ensure the firewall is blocking scanners*

SSH listening on default port — Medium Severity

Synopsis:

`SSH` is listening on default port `21`

Description:

Access to the sever was achieved using supplied default login credentials via `SSH` port `21`

Solution:

- *Add second port, preferably above the default range and the higher, the better, and set listen for SSH*

SSH PermitRootLogin allowed — Medium Severity

Synopsis:

`root` login enabled via `SSH`

Description:

`PermitRootAccess` set to yes in `/etc/ssh/sshd_config`

Solution:

- It is good practice to enforce login to `root` via switch user (`su root`) and rather than via allowing access via `SSH` to control access and stop brute-forcing.

wget enabled for standard users — Medium Severity

Synopsis:

`wget` can be used by standard users to upload files

Description:

`wget` enabled for standard users and file upload successful in shared directories such as `/var/tmp`

Solution:

- `wget` useable by default account connected and file upload successful in shared directories such as `/var/tmp`

sftp access enabled for standard users — Medium Severity

Synopsis:

`sftp` via default `SSH` settings can be accessed via port `21` by standard users to upload files

Description:

`sftp` login was allowed using supplied default credentials and file upload successful in shared directories such as `/var/tmp`

Solution:

- `sftp` is a great secure alternative for the very insecure `ftp` and comes installed as part of `OpenSSH` with default setting allowing instant access. Options for hardening `sftp` its include;
- Matching – add a condition to `/etc/ssh/sshd_config` to match specific credentials such as a group of the supplied user credentials to control access
- Add second port preferably above the default range, higher is better and set `sftp` to listen

bash enabled for standard users — Medium Severity

Synopsis:

`Bash` enabled for standard users (`non sudo`)

Description:

Engineers were able to run scripts and commands from a standard user that could be used for `automated enumeration`, `planting loggers` and `malware`, attempts at `privesc`

Solution:

- Disable `bash` for all users other than `root` by removing `/bin/bash` for the user in the `/etc/passwd`

5. ICMP

`ICMP` is a Network layer protocol which can be utilised by attackers and penetration testers to probe servers. Hackers also utilise `ICMP` as an attack surface. `ICMP` probes are instrumental tools and the first weapon of choice for any hack. `ICMP` requests can be disallowed in the firewall and by changing the value of `icmp_echo_ignore_all` file from `0 to 1; nano /proc/sys/net/ipv4/icmp_echo_ignore_all`. Disabling `ICMP` stops devices replying to scanners and probes, rendering the tools useless and finding an initial entry point complicated but still not impossible.

Phase 1: Observations

`fping` Hollywood host IP, resolve subnet and ping list (-g) and `STD OUT` to log file

```
kali@kali:~$ fping -g 15.199.95.81/28 >> hollywood_fping.log
kali@kali:~$ fping -g 15.199.94.81/28 >> hollywood_fping.log
kali@kali:~$ fping -g 11.199.158.91/28 >> hollywood_fping.log
kali@kali:~$ fping -g 11.199.141.91/28 >> hollywood_fping.log
kali@kali:~$ fping -g 167.172.144.11/32 >> hollywood_fping.log
```

Search log file for any servers responding to `ICMP`

```
kali@kali:~$ cat hollywood_fping.log | grep alive
167.172.144.11 is alive
```

Ensure I didn't just have a single response in the log file

```
kali@kali:~$ wc -l hollywood_fping.log
57 hollywood_fping.log
```

`ping` *because why not?*

```
kali@kali:~$ ping 167.172.144.11 -c3
PING 167.172.144.11 (167.172.144.11) 56(84) bytes of data.
64 bytes from 167.172.144.11: icmp_seq=1 ttl=52 time=480 ms
64 bytes from 167.172.144.11: icmp_seq=2 ttl=52 time=479 ms
64 bytes from 167.172.144.11: icmp_seq=3 ttl=52 time=479 ms

--- 167.172.144.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 478.622/479.335/480.420/0.779 ms
```

6. Ports

Ports are the way in! We are simulating an attack and will use `nmap`'s `SYN` attack that works on the Transport layer. Attacks utilised `SYN` probing when a server is not responding to simple `ping` requests. Changing your default ports from the standard

*default ports (such as **21** for **SSH**) can stop their rapid discovery. Picking perhaps above **20,000** will get you out of default scan range (**1000**) adding considerable time an attacker scanning your server and mitigates abuse by bots.*

Phase 2: Observations

*Created a folder for **nmap** log files*

```
kali@kali:~$ cd Documents/
kali@kali:~/Documents$ mkdir -p Week8/nmap
kali@kali:~/Documents$ cd Week8
kali@kali:~/Documents/Week8$
```

*Start **nmap SYN** scan(**-SS**), **STD OUT(-oA)** to log file, target **167.172.144.11** with verbose output (**-v**). I have coloured the important bits yellow*

```
kali@kali:~/Documents/Week8$ sudo nmap -sS -oA nmap/syn 167.172.144.11 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 14:49 EDT
Initiating Ping Scan at 14:49
Scanning 167.172.144.11 [4 ports]
Completed Ping Scan at 14:49, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:49
Completed Parallel DNS resolution of 1 host. at 14:49, 6.86s elapsed
Initiating SYN Stealth Scan at 14:49
Scanning 167.172.144.11 [1000 ports]
Discovered open port 22/tcp on 167.172.144.11
Increasing send delay for 167.172.144.11 from 0 to 5 due to 11 out of 14 dropped
probes since last increase.
Increasing send delay for 167.172.144.11 from 5 to 10 due to 237 out of 789
dropped probes since last increase.
Increasing send delay for 167.172.144.11 from 10 to 20 due to max_successful_tryno
increase to 4
Increasing send delay for 167.172.144.11 from 20 to 40 due to max_successful_tryno
increase to 5
SYN Stealth Scan Timing: About 46.40% done; ETC: 14:51 (0:00:36 remaining)
Increasing send delay for 167.172.144.11 from 40 to 80 due to max_successful_tryno
increase to 6
Increasing send delay for 167.172.144.11 from 80 to 160 due to
max_successful_tryno increase to 7
Increasing send delay for 167.172.144.11 from 160 to 320 due to 20 out of 66
dropped probes since last increase.
Increasing send delay for 167.172.144.11 from 320 to 640 due to
max_successful_tryno increase to 8
SYN Stealth Scan Timing: About 47.14% done; ETC: 14:52 (0:01:08 remaining)
Increasing send delay for 167.172.144.11 from 640 to 1000 due to 11 out of 28
dropped probes since last increase.
SYN Stealth Scan Timing: About 46.58% done; ETC: 14:53 (0:01:44 remaining)
Warning: 167.172.144.11 giving up on port because retransmission cap hit (10).
SYN Stealth Scan Timing: About 47.02% done; ETC: 14:54 (0:02:16 remaining)
SYN Stealth Scan Timing: About 47.44% done; ETC: 14:55 (0:02:47 remaining)
SYN Stealth Scan Timing: About 47.69% done; ETC: 14:56 (0:03:19 remaining)
SYN Stealth Scan Timing: About 47.94% done; ETC: 14:57 (0:03:49 remaining)
SYN Stealth Scan Timing: About 48.18% done; ETC: 14:58 (0:04:19 remaining)
SYN Stealth Scan Timing: About 48.43% done; ETC: 14:59 (0:04:49 remaining)
SYN Stealth Scan Timing: About 48.68% done; ETC: 15:00 (0:05:17 remaining)
SYN Stealth Scan Timing: About 48.95% done; ETC: 15:01 (0:05:48 remaining)
SYN Stealth Scan Timing: About 49.26% done; ETC: 15:02 (0:06:24 remaining)
SYN Stealth Scan Timing: About 49.64% done; ETC: 15:03 (0:07:04 remaining)
```

```
SYN Stealth Scan Timing: About 50.06% done; ETC: 15:05 (0:07:48 remaining)
SYN Stealth Scan Timing: About 50.53% done; ETC: 15:07 (0:08:35 remaining)
SYN Stealth Scan Timing: About 51.07% done; ETC: 15:09 (0:09:27 remaining)
SYN Stealth Scan Timing: About 51.71% done; ETC: 15:11 (0:10:26 remaining)
SYN Stealth Scan Timing: About 52.48% done; ETC: 15:14 (0:11:31 remaining)
SYN Stealth Scan Timing: About 53.43% done; ETC: 15:17 (0:12:44 remaining)
SYN Stealth Scan Timing: About 54.58% done; ETC: 15:20 (0:14:07 remaining)
SYN Stealth Scan Timing: About 56.08% done; ETC: 15:25 (0:15:41 remaining)
SYN Stealth Scan Timing: About 58.24% done; ETC: 15:31 (0:17:28 remaining)
SYN Stealth Scan Timing: About 61.89% done; ETC: 15:41 (0:19:34 remaining)
SYN Stealth Scan Timing: About 71.57% done; ETC: 16:01 (0:20:24 remaining)
SYN Stealth Scan Timing: About 80.52% done; ETC: 16:16 (0:16:48 remaining)
SYN Stealth Scan Timing: About 86.82% done; ETC: 16:24 (0:12:29 remaining)
SYN Stealth Scan Timing: About 92.35% done; ETC: 16:31 (0:07:45 remaining)
SYN Stealth Scan Timing: About 96.20% done; ETC: 16:35 (0:04:00 remaining)
SYN Stealth Scan Timing: About 98.18% done; ETC: 16:37 (0:01:57 remaining)
SYN Stealth Scan Timing: About 99.16% done; ETC: 16:38 (0:00:54 remaining)
Completed SYN Stealth Scan at 16:59, 7800.03s elapsed (1000 total ports)
Nmap scan report for 167.172.144.11
Host is up (0.00048s latency).
Not shown: 634 filtered ports, 365 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7807.07 seconds
           Raw packets sent: 9187 (401.404KB) | Rcvd: 13385 (682.628KB)
```

7. Enumeration

*RockStar Corp has provided us with a default login details **`jimi/hendrix`** to r00tr00t o conduct an enumeration and investigation. B00t r00t was able to utilise wget to upload a bash enumeration script called LinEnum to produce a detailed report that details a range of system information and vulnerability information that could be used for privilege escalation.*

B00tr00t uncovered evidence of malicious activity when engineers noticed a suspicious modification to the /etc/hosts adding an entry to the DNS cache which appears to be an application layer DNS cache poisioning attach.

Phase 3: Observations

*SSH as user **jimi** and password **hendrix** to connect to host **`167.172.144.11`** on the default port 22 which was open.*

```
kali@kali:~$ ssh jimi@167.172.144.11
jimi@167.172.144.11's password:
```

`sftp` login?

```
kali@kali:~$
sftp jimi@167.172.144.11
jimi@167.172.144.11's password:
Connected to 167.172.144.11.
sftp>
```

Enumerate and check for common misconfigurations

```
$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 9 (stretch)"
NAME="Debian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
VERSION_CODENAME=stretch
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Get `kernel` version

```
$ cat /proc/version
Linux version 4.9.0-11-amd64 (debian-kernel@lists.debian.org) (gcc version 6.3.0
20170516 (Debian 6.3.0-18+deb9u1) ) #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20)
```

Get `hostname`

```
$ hostname
GTscavengerHunt
```

`netstat` open ports compare results with `nmap`

```
$ netstat -ltnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN
-
tcp6       0      0 :::22                   :::*                    LISTEN
-
tcp6       0      0 :::5355                 :::*                    LISTEN
```

`cat sshd_config` for weak brute force protection

```
cat /etc/ssh/sshd_config
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

`ICMP` check if `ignore_all` is set to enabled. `(0=Disabled)`

```
$ cat /proc/sys/net/ipv4/icmp_echo_ignore_all
0
```

Check if `SSH` allows `root` access

```
$ cat /etc/ssh/sshd_config | grep PermitRoot
```

```
PermitRootLogin yes
# the setting of "PermitRootLogin yes
```

*Check permissions on **shadow***

```
$ ls -al /etc/shadow
-rw-r----- 1 root shadow 2147 Mar 18  2020 /etc/shadow
```

*Check for **crontab** misconfiguration*

```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab.'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )
#
$ python3 -V
Python 3.5.3
```

*Spawn interactive **shell** because low priv shell sucks!*

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
```

Worth a try.

```
jimi@GTscavengerHunt:/etc$ sudo -l
[sudo] password for jimi:
Sorry, user jimi may not run sudo on GTscavengerHunt.
jimi@GTscavengerHunt:/etc$
```

*Check **SUID***

```
jimi@GTscavengerHunt:/etc$ find / -perm -4000 2>/dev/null
/bin/su
/bin/mount
/bin/ping
/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/chsh
```

```
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/gpasswd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
```

*Check **GUID***

```
jimi@GTscavengerHunt:/etc$
find / -perm -2000 2>/dev/null
/run/log/journal
/run/log/journal/398d1113da1bb8bd2884b0125e1de61f
/var/local
/var/mail
/usr/local
/usr/local/include
/usr/local/etc
/usr/local/bin
/usr/local/share
/usr/local/share/man
/usr/local/share/ca-certificates
/usr/local/src
/usr/local/games
/usr/local/sbin
/usr/local/lib
/usr/local/lib/python2.7
/usr/local/lib/python2.7/dist-packages
/usr/local/lib/python2.7/site-packages
/usr/local/lib/python3.5
/usr/local/lib/python3.5/dist-packages
/usr/bin/screen
/usr/bin/chage
/usr/bin/ssh-agent
/usr/bin/wall
/usr/bin/bsd-write
/usr/bin/crontab
/usr/bin/expiry
/sbin/unix_chkpwd
```

`cat hosts` file for suspicious entries

```
$ 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

ooooooollowing 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
```

`nslookup 98.137.246.8` *entered in DNS cache as "rollingstone.com"*

```
kali@kali:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = media-router-
fp72.prod.media.vip.gq1.yahoo.com.
```

`host 98.137.246.8` always good to double-check

```
kali@kali:~$ host 98.137.246.8
8.246.137.98.in-addr.arpa domain name pointer media-router-
fp72.prod.media.vip.gq1.yahoo.com.
```

`whois` on `98.137.246.8` because why not?

```
kali@kali:~$ whois 98.137.246.8

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


NetRange:       98.136.0.0 - 98.139.255.255
CIDR:           98.136.0.0/14
NetName:        A-YAHOO-US9
NetHandle:      NET-98-136-0-0-1
Parent:         NET98 (NET-98-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS10310
Organization:   Oath Holdings Inc. (OH-207)
RegDate:        2007-12-07
Updated:        2019-05-01
Ref:            https://rdap.arin.net/registry/ip/98.136.0.0



OrgName:        Oath Holdings Inc.
OrgId:          OH-207
Address:        770 BROADWAY FL 4
City:           New York
StateProv:      NY
PostalCode:     10003-9558
Country:        US
RegDate:        2018-12-21
```

```
Updated:        2019-05-16
Ref:            https://rdap.arin.net/registry/entity/OH-207


OrgAbuseHandle: OATHA-ARIN
OrgAbuseName:   Oath Abuse
OrgAbusePhone:  +1-408-349-3300
OrgAbuseEmail:  rir-abuse@oath.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/OATHA-ARIN

OrgNOCHandle: OATHN-ARIN
OrgNOCName:   Oath NOC
OrgNOCPhone:  +1-408-349-5555
OrgNOCEmail:  rir-noc@oath.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/OATHN-ARIN

OrgTechHandle: OTC2-ARIN
OrgTechName:   Oath Tech Contact
OrgTechPhone:  +1-408-349-5555
OrgTechEmail:  rir-tech@oath.com
OrgTechRef:    https://rdap.arin.net/registry/entity/OTC2-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#


kali@kali:~$
```

8. Forensics

*b00tr00t carried out a forensic examination of the gathered evidence using a sophisticated program designed to capture and analyse network traffic named Wireshark. B00tr00t engineers found evidence of arp spoofing, which is an attack that occurs between layers two and three of the OSI model and suspicious activity on the application layer with malicious **HTTP** get and post data.*

Phase 4: Observations

Change the directory of the host file and look for any notes from the attacker.

```
jimi@GTscavengerHunt:/$ cd etc/
```

`ls -al /etc/` for text files

```
jimi@GTscavengerHunt:/etc$ ls -al | grep txt
-rw-r--r--  1 root root     112 Mar 18  2020 packetcaptureinfo.txt
```

`cat` suspicious text file

```
jimi@GTscavengerHunt:/etc$ cat packetcaptureinfo.txt
 Captured Packets are here:
 https://drive.google.com/file/d/1ic-
CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
```

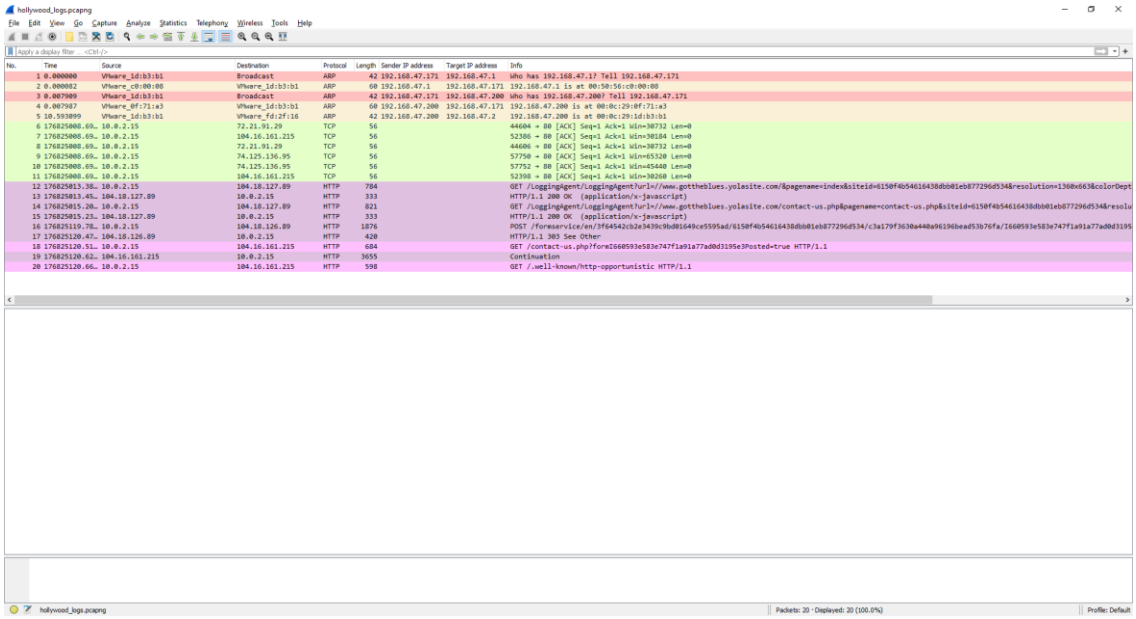
`curl` to download file. I'm going to assume its Wireshark, so `.pcapng` is the extension

```
C:\Users\Tim>curl  https://drive.google.com/file/d/1ic-
CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing -o hollywood_log.pcapng
% Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
Dload  Upload   Total   Spent    Left  Speed
100 62537    0 62537    0     0  31268      0 --:--:--  0:00:02 --:--:--
22609
```

Ensure the file downloaded.

```
C:\Users\Tim>dir hollywood_log.pcapng
Volume in drive C has no label.
Volume Serial Number is BC91-DB06
Directory of C:\Users\Tim
26/09/2020  04:44 AM            62,537 hollywood_log.pcapng
1 File(s)         62,537 bytes
0 Dir(s)  196,283,392,000 bytes free
C:\Users\Tim>
```

*Open file **`hollywood_log.pcapng`** in Wireshark and colour code suspicious Wireshark activity, add sender and target **`IP`** columns.*



*Suspicious **`ARP`** requests highlighted in red*

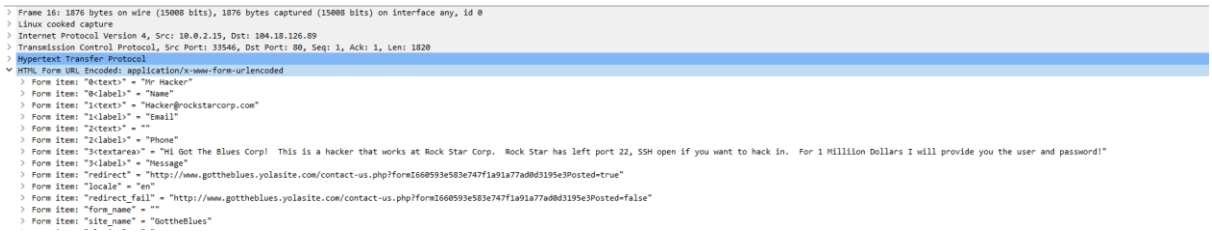
	Time	Source	Destination	Protocol	Length	Sender IP address	Target IP address	Info
1	0.000000	VMware_1d:b3:b1	Broadcast	ARP	42	192.168.47.171	192.168.47.1	Who has 192.168.47.1? Tell 192.168.47.171
2	0.000082	VMware_c0:00:08	VMware_1d:b3:b1	ARP	60	192.168.47.1	192.168.47.171	192.168.47.1 is at 00:50:56:c0:00:08
3	0.007909	VMware_1d:b3:b1	Broadcast	ARP	42	192.168.47.171	192.168.47.200	Who has 192.168.47.200? Tell 192.168.47.171
4	0.007987	VMware_0f:71:a3	VMware_1d:b3:b1	ARP	60	192.168.47.200	192.168.47.171	192.168.47.200 is at 00:0c:29:0f:71:a3
5	10.593099	VMware_1d:b3:b1	VMware_fd:2f:16	ARP	42	192.168.47.200	192.168.47.2	192.168.47.200 is at 00:0c:29:1d:b3:b1

*Suspicious **`GET`** requests to a non-work-related website*

*Close up of **`URLs`***

```
GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616438dbb01eb877296d534&resolution=1360x663&colorDept
HTTP/1.1 200 OK  (application/x-javascript)
GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/contact-us.php&pagename=contact-us.php&siteid=6150f4b54616438dbb01eb877296d534&resolu
HTTP/1.1 200 OK  (application/x-javascript)
POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76fa/I660593e583e747f1a91a77ad0d3195
HTTP/1.1 303 See Other
GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true HTTP/1.1
Continuation
GET /.well-known/http-opportunistic HTTP/1.1
```

*Suspicious **`POST`***



Copy of suspicious post discovered in Wireshark file data that suggest evidence of the inside actor

```
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 Milliion 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?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
    Form item: "locale" = "en"
    Form item: "redirect_fail" =
"http://www.gottheblues.yolasite.com/contact-
us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"
    Form item: "form_name" = ""
    Form item: "site_name" = "GottheBlues"
    Form item: "wl_site" = "0"
    Form item: "destination" =
"DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2ouelFsQG
6ZzGkhh31_Gl2mb5PGk="
        Key: destination
        Value:
DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6
ZzGkhh31_Gl2mb5PGk=
    Form item: "g-recaptcha-response" =
"03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2
MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-
6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8hu4c6u
```