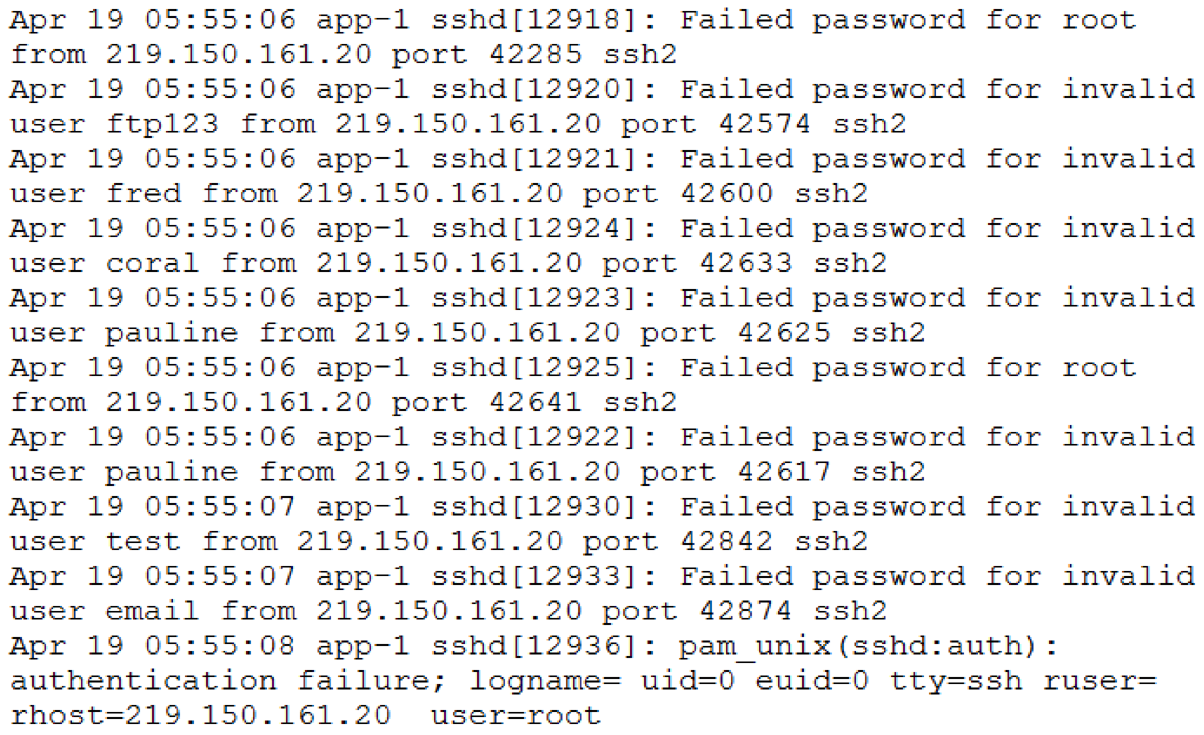
MUHAMMAD HAMAD – BONUS Assignment –LOG MYSTRIES

Q: Was the system compromised and when? How do you know that for sure?

Ans: In auth.log file there are some attempts of guessing password before actually the access was gained, you can see the following log, that system was compromised actually



```
Apr 19 05:55:06 app-1 sshd[12918]: Failed password for root
from 219.150.161.20 port 42285 ssh2
Apr 19 05:55:06 app-1 sshd[12920]: Failed password for invalid
user ftp123 from 219.150.161.20 port 42574 ssh2
Apr 19 05:55:06 app-1 sshd[12921]: Failed password for invalid
user fred from 219.150.161.20 port 42600 ssh2
Apr 19 05:55:06 app-1 sshd[12924]: Failed password for invalid
user coral from 219.150.161.20 port 42633 ssh2
Apr 19 05:55:06 app-1 sshd[12923]: Failed password for invalid
user pauline from 219.150.161.20 port 42625 ssh2
Apr 19 05:55:06 app-1 sshd[12925]: Failed password for root
from 219.150.161.20 port 42641 ssh2
Apr 19 05:55:06 app-1 sshd[12922]: Failed password for invalid
user pauline from 219.150.161.20 port 42617 ssh2
Apr 19 05:55:07 app-1 sshd[12930]: Failed password for invalid
user test from 219.150.161.20 port 42842 ssh2
Apr 19 05:55:07 app-1 sshd[12933]: Failed password for invalid
user email from 219.150.161.20 port 42874 ssh2
Apr 19 05:55:08 app-1 sshd[12936]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=219.150.161.20  user=root
```

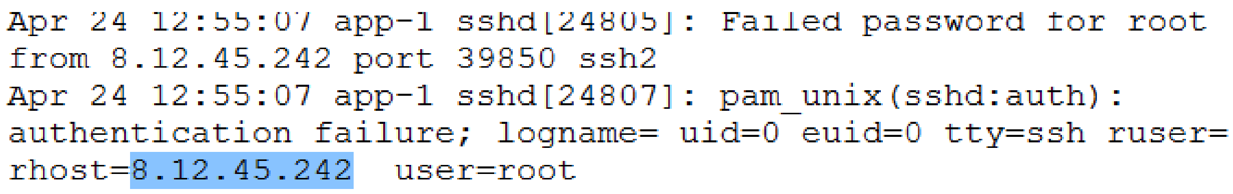
Q: If the was compromised, what was the method used?

Ans: Brute force attack was launched against open ssh daemon to get the root access.

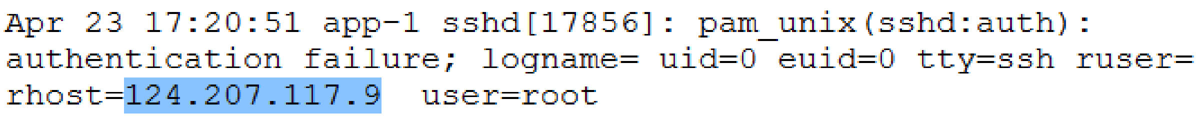
Q: Can you locate how many attackers failed? If some succeeded, how many were they? How many stopped attacking after the first success?

Ans: There were total 31 ip's that were failed , snapshots of some of failed are shown here.

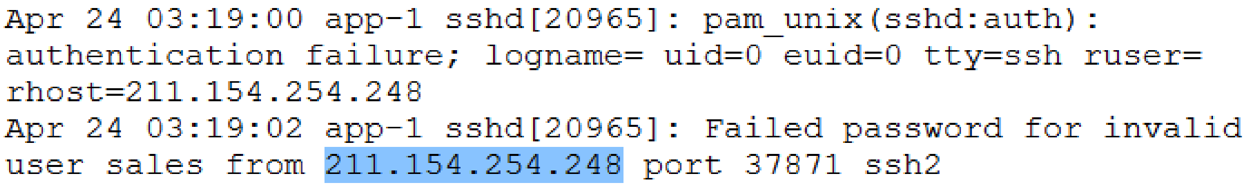
Some Failed attempts:



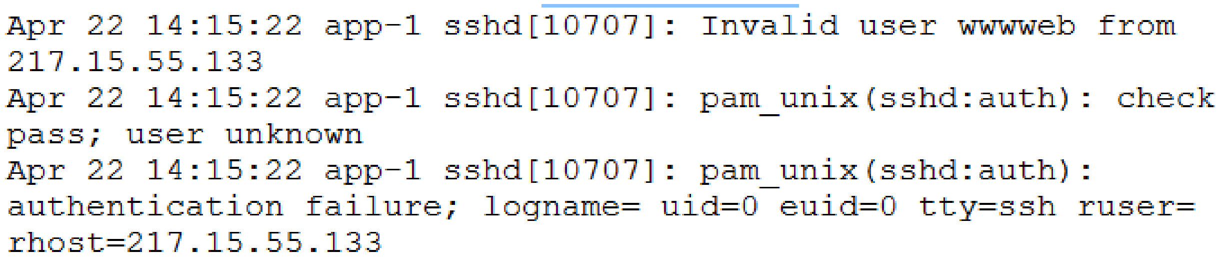
```
Apr 24 12:55:07 app-1 sshd[24805]: Failed password for root
from 8.12.45.242 port 39850 ssh2
Apr 24 12:55:07 app-1 sshd[24807]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=8.12.45.242  user=root
```



```
Apr 23 17:20:51 app-1 sshd[17856]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=124.207.117.9  user=root
```

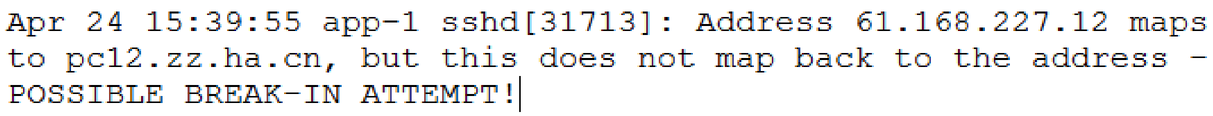


```
Apr 24 03:19:00 app-1 sshd[20965]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=211.154.254.248
Apr 24 03:19:02 app-1 sshd[20965]: Failed password for invalid
user sales from 211.154.254.248 port 37871 ssh2
```

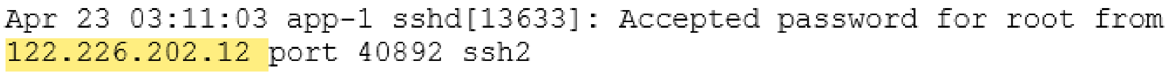


```
Apr 22 14:15:22 app-1 sshd[10707]: Invalid user wwwweb from
217.15.55.133
Apr 22 14:15:22 app-1 sshd[10707]: pam_unix(sshd:auth): check
pass; user unknown
Apr 22 14:15:22 app-1 sshd[10707]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=217.15.55.133
```

Some Successful break in:



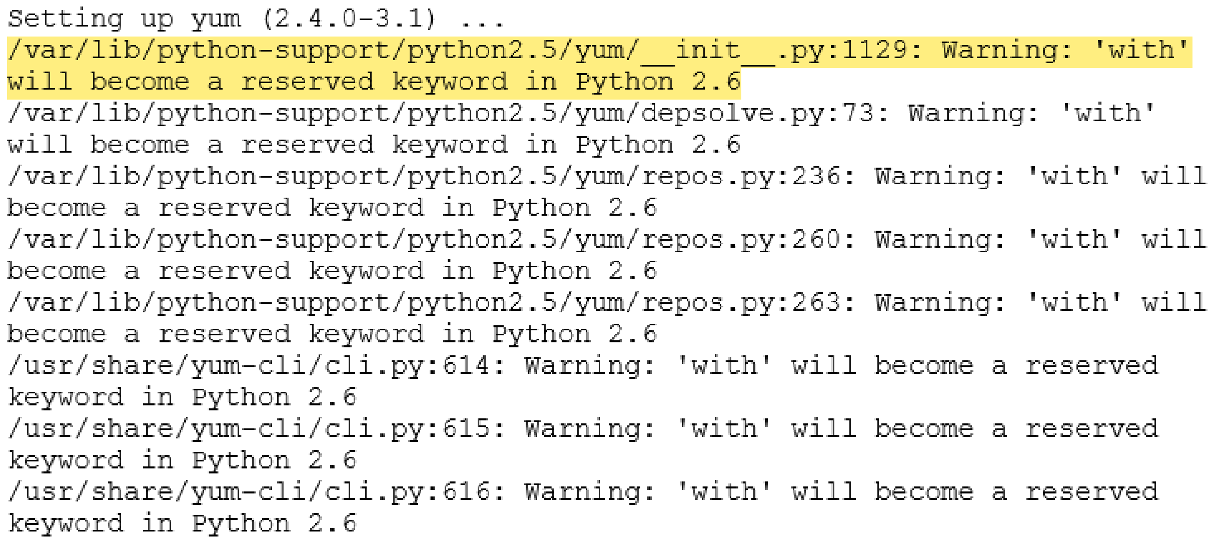
```
Apr 24 15:39:55 app-1 sshd[31713]: Address 61.168.227.12 maps
to pc12.zz.ha.cn, but this does not map back to the address -
POSSIBLE BREAK-IN ATTEMPT!
```



```
Apr 23 03:11:03 app-1 sshd[13633]: Accepted password for root from
122.226.202.12 port 40892 ssh2
```

Q: What happened after the brute force attack?

Ans: Exim mail server was reconfigured and some software were installed



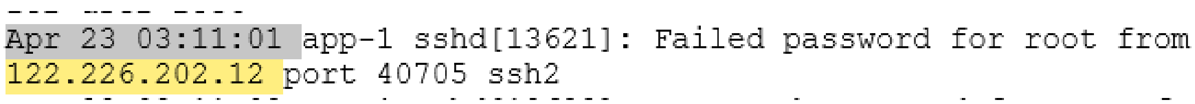
```
Setting up yum (2.4.0-3.1) ...
/var/lib/python-support/python2.5/yum/__init__.py:1129: Warning: 'with'
will become a reserved keyword in Python 2.6
/var/lib/python-support/python2.5/yum/depsolve.py:73: Warning: 'with'
will become a reserved keyword in Python 2.6
/var/lib/python-support/python2.5/yum/repos.py:236: Warning: 'with' will
become a reserved keyword in Python 2.6
/var/lib/python-support/python2.5/yum/repos.py:260: Warning: 'with' will
become a reserved keyword in Python 2.6
/var/lib/python-support/python2.5/yum/repos.py:263: Warning: 'with' will
become a reserved keyword in Python 2.6
/usr/share/yum-cli/cli.py:614: Warning: 'with' will become a reserved
keyword in Python 2.6
/usr/share/yum-cli/cli.py:615: Warning: 'with' will become a reserved
keyword in Python 2.6
/usr/share/yum-cli/cli.py:616: Warning: 'with' will become a reserved
keyword in Python 2.6
```

Q: Locate the authentication logs, was a brute force attack performed? If yes how many?

Ans: Brute Force attacks was performed against the SSH daemon. There were 11 succesful attacks from 6 different IP addresses. There were 27 unsuccessful attacks. Some sanpshots of failed and successful ip’s were provided in question 3.

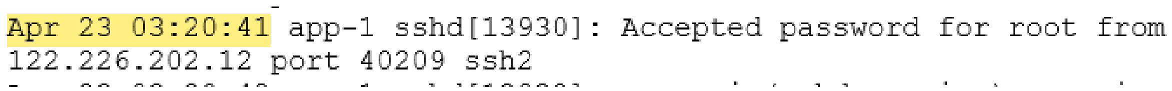
Q: What is the timeline of significant events? How certain are you of the timing?

Ans: Start of attack by 122.226.202.12



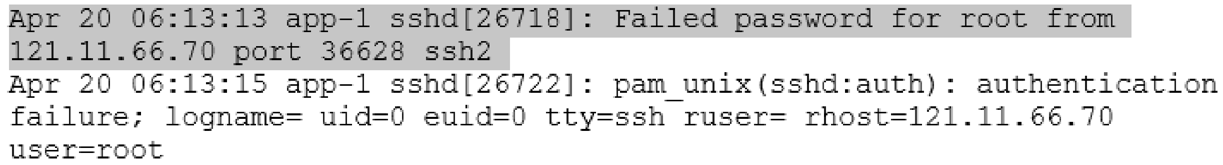
```
Apr 23 03:11:01 app-1 sshd[13621]: Failed password for root from
122.226.202.12 port 40705 ssh2
```

First acceptance of password from 122.226.202.12



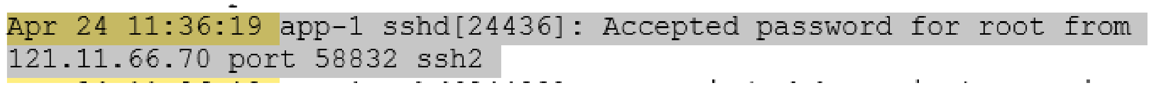
```
Apr 23 03:20:41 app-1 sshd[13930]: Accepted password for root from
122.226.202.12 port 40209 ssh2
```

Start of attack by 121.11.66.70



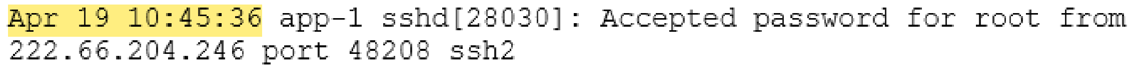
```
Apr 20 06:13:13 app-1 sshd[26718]: Failed password for root from
121.11.66.70 port 36628 ssh2
Apr 20 06:13:15 app-1 sshd[26722]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=121.11.66.70
user=root
```

First acceptance of password from 122.11.66.70



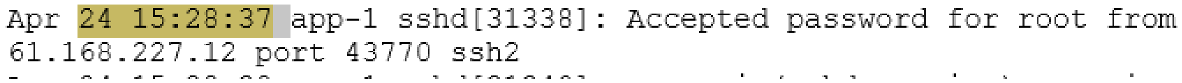
```
Apr 24 11:36:19 app-1 sshd[24436]: Accepted password for root from
121.11.66.70 port 58832 ssh2
```

Password accepted from 222.66.204.246



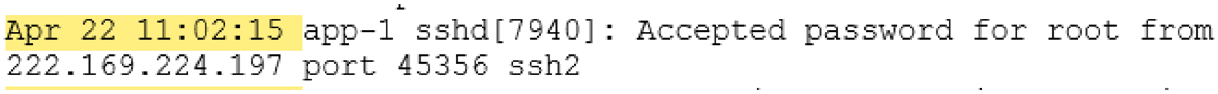
```
Apr 19 10:45:36 app-1 sshd[28030]: Accepted password for root from
222.66.204.246 port 48208 ssh2
```

Password accepted from 61.168.227.12



```
Apr 24 15:28:37 app-1 sshd[31338]: Accepted password for root from
61.168.227.12 port 43770 ssh2
```

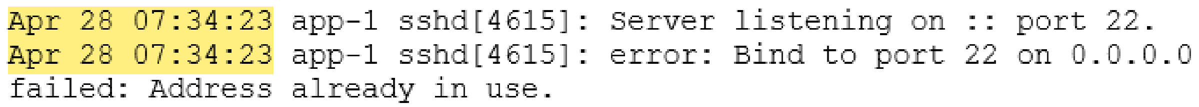
Password accepted from 222.169.224.197



```
Apr 22 11:02:15 app-1 sshd[7940]: Accepted password for root from
222.169.224.197 port 45356 ssh2
```

Q: Anything else that looks suspicious in the logs? Any misconfigurations? Other issues?

Ans: The SSH daemon allows root login. I'd say that's a misconfiguration. It also starts to listen to both IPv4 and IPv6 and thus results in this error message in the logs:



```
Apr 28 07:34:23 app-1 sshd[4615]: Server listening on :: port 22.
Apr 28 07:34:23 app-1 sshd[4615]: error: Bind to port 22 on 0.0.0.0
failed: Address already in use.
```

Q: Was an automatic tool used to perform the attack? If yes which one?

Ans: certainly brute force, because there are too many logs created in short period of time.

Q: What can you say about the attacker's goals and methods?

Ans: Attacker used brute force to guess the password of open ssh daemon and tried to get administrator privilege after that installed some software on victim machine and , and using victim machine scanned for ssh servers.

THE END