HORSE TRAP

A simulated insider privilege escalation

Giann Berrospi and Michael Doronio

What is it?

An insider attack simulation targeting vulnerable user data inside an unauthorized workstation

Demonstration of a trojan horse and persistence

Exploration of data analysis and lessons learned

Why it matters...

60% of data breaches are caused by an inside threat

Harder to detect as a threat

Easier to attack network if you already have access to sensitive data

In 2020 , GE was the victim of an insider attack by two of their employees

Setting the Stage

Disgruntled HR employee

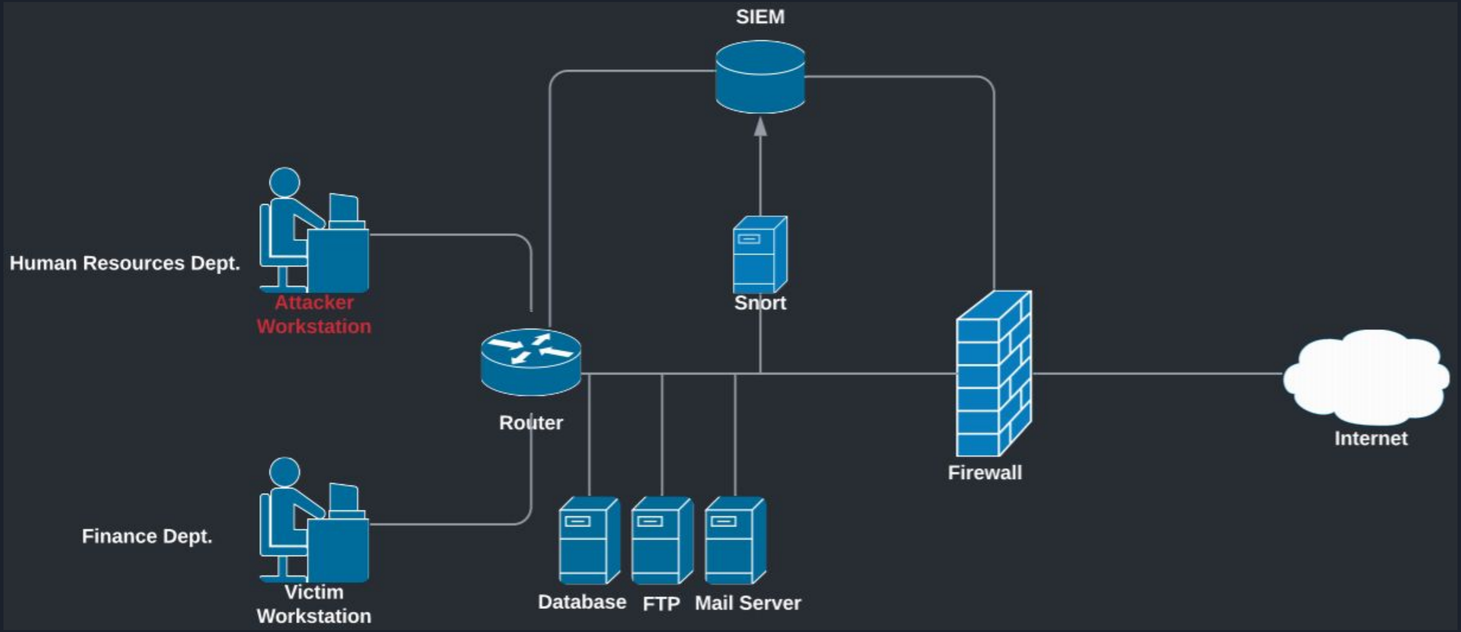
Wants to steal information /assets

Plans to start their own company

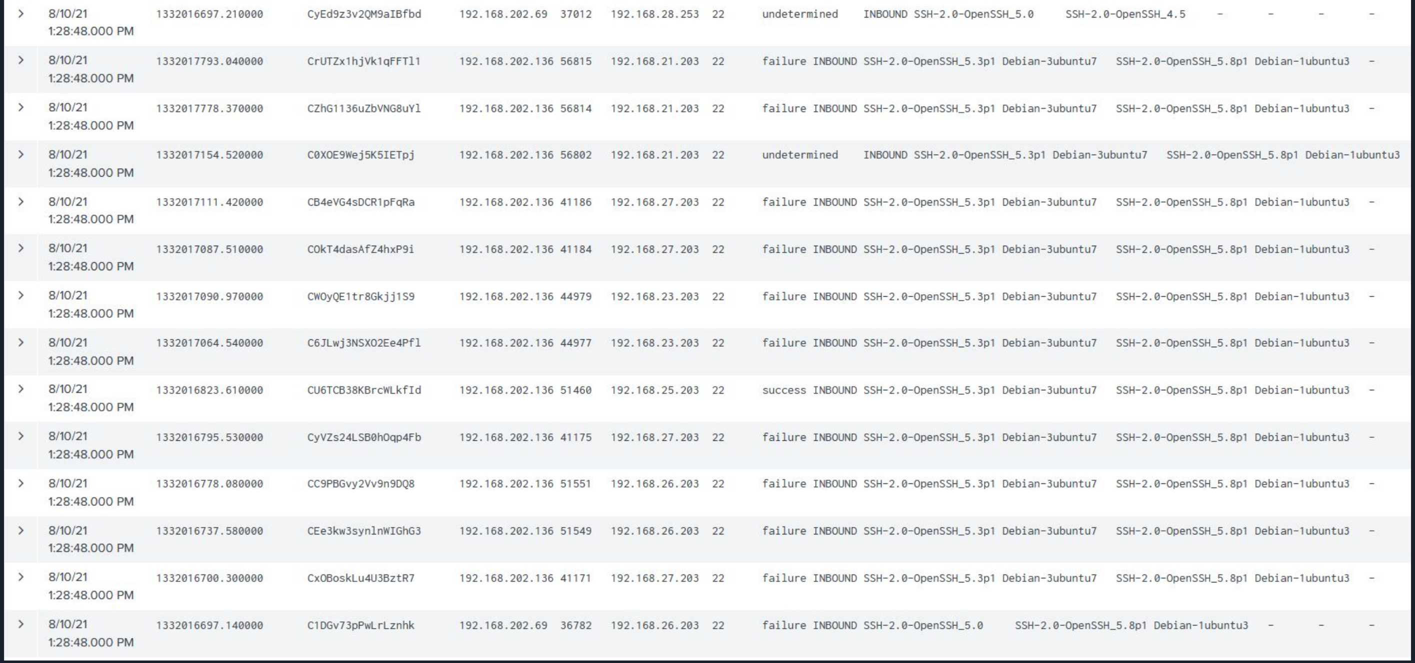
Target the head of the finance department to get what they need

QnJvdWdodCB0byB5b3UgYnkgQSBTZWNyZXQgT3JnYW5pemF0aW9uCg==

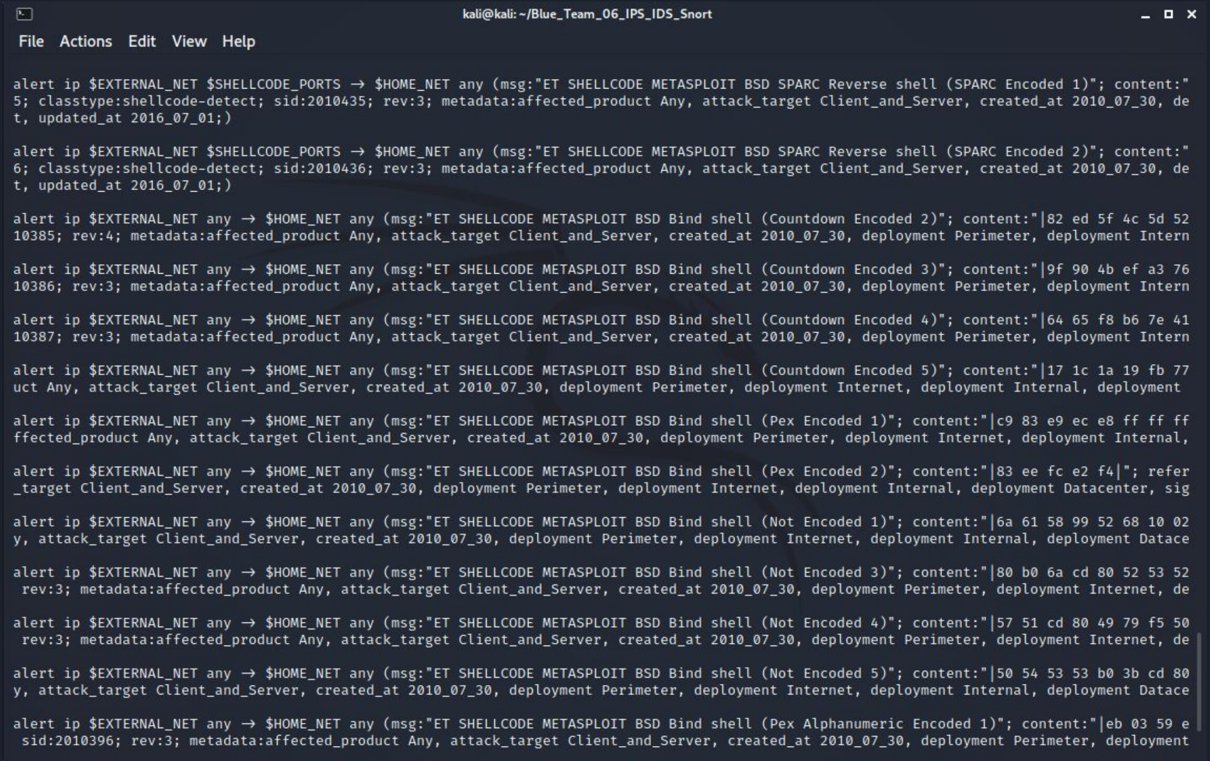
The Network


SIEM
Human Resources Dept.
Attacker Workstation
Snort
Router
Firewall
Internet
Finance Dept.
Victim Workstation
Database
FTP
Mail Server

Shortcomings



```
>  8/10/21          1332016697.210000   CyEd9z3v2QM9aIBfbd    192.168.202.69  37012   192.168.28.253  22   undetermined   INBOUND SSH-2.0-OpenSSH_5.0   SSH-2.0-OpenSSH_4.5   -   -   -   -
   1:28:48.000 PM
>  8/10/21          1332017793.040000   CrUTZx1hjVk1qFFTl1    192.168.202.136 56815   192.168.21.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332017778.370000   CZhG1136uZbVNG8uYl    192.168.202.136 56814   192.168.21.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332017154.520000   C0XOE9Wej5K5IETpj     192.168.202.136 56802   192.168.21.203  22   undetermined   INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
   1:28:48.000 PM
>  8/10/21          1332017111.420000   CB4eVG4sDCR1pFqRa     192.168.202.136 41186   192.168.27.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332017087.510000   COkT4dasAfZ4hxP9i     192.168.202.136 41184   192.168.27.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332017090.970000   CWOyQE1tr8Gkjj1S9     192.168.202.136 44979   192.168.23.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332017064.540000   C6JLwj3NSXO2Ee4Pfl    192.168.202.136 44977   192.168.23.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332016823.610000   CU6TCB38KBrcWLkfId    192.168.202.136 51460   192.168.25.203  22   success INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332016795.530000   CyVZs24LSB0hOqp4Fb    192.168.202.136 41175   192.168.27.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332016778.080000   CC9PBGvy2Vv9n9DQ8     192.168.202.136 51551   192.168.26.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332016737.580000   CEe3kw3synlnWIGhG3    192.168.202.136 51549   192.168.26.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332016700.300000   CxOBoskLu4U3BztR7     192.168.202.136 41171   192.168.27.203  22   failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -
   1:28:48.000 PM
>  8/10/21          1332016697.140000   C1DGv73pPwLrLznhk     192.168.202.69  36782   192.168.26.203  22   failure INBOUND SSH-2.0-OpenSSH_5.0   SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3   -   -   -
   1:28:48.000 PM
```



kali@kali: ~/Blue_Team_06_IPS_IDS_Snort
File Actions Edit View Help

```
alert ip $EXTERNAL_NET $SHELLCODE_PORTS → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (SPARC Encoded 1)"; content:"
5; classtype:shellcode-detect; sid:2010435; rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, de
t, updated_at 2016_07_01;)

alert ip $EXTERNAL_NET $SHELLCODE_PORTS → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD SPARC Reverse shell (SPARC Encoded 2)"; content:"
6; classtype:shellcode-detect; sid:2010436; rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, de
t, updated_at 2016_07_01;)

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 2)"; content:"|82 ed 5f 4c 5d 52
10385; rev:4; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Intern

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 3)"; content:"|9f 90 4b ef a3 76
10386; rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Intern

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 4)"; content:"|64 65 f8 b6 7e 41
10387; rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Intern

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Countdown Encoded 5)"; content:"|17 1c 1a 19 fb 77
uct Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, deployment Internal, deployment

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Encoded 1)"; content:"|c9 83 e9 ec e8 ff ff ff
ffected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, deployment Internal,

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Encoded 2)"; content:"|83 ee fc e2 f4|"; refer
_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, deployment Internal, deployment Datacenter, sig

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 1)"; content:"|6a 61 58 99 52 68 10 02
y, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, deployment Internal, deployment Datace

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 3)"; content:"|80 b0 6a cd 80 52 53 52
 rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, de

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 4)"; content:"|57 51 cd 80 49 79 f5 50
 rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, de

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Not Encoded 5)"; content:"|50 54 53 53 b0 3b cd 80
y, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment Internet, deployment Internal, deployment Datace

alert ip $EXTERNAL_NET any → $HOME_NET any (msg:"ET SHELLCODE METASPLOIT BSD Bind shell (Pex Alphanumeric Encoded 1)"; content:"|eb 03 59 e
 sid:2010396; rev:3; metadata:affected_product Any, attack_target Client_and_Server, created_at 2010_07_30, deployment Perimeter, deployment
```

Conclusion

1. What is your organization’s strategy for insider threats?

2. Are there gaps in your network that an insider can take advantage of?

3. The most valuable assets ought to have the highest levels of security

Resources

CISA. Insider Threat Mitigation Resources. (2021).
https://www.cisa.gov/insider-threat-mitigation

MITRE ATT&CK. Mitre Corporation. (2021).
https://attack.mitre.org/techniques/T1566/