

## Computer Crime Investigation

Oblong, Inc., a semiconductor manufacturer, was a late adopter of new technologies—much to the dismay of its high-tech users. Paul was the I.T. manager for Oblong's sales office, located in the financial district of a large city. Due to the complexity of managing firewalls across a very large enterprise, Oblong outsourced their upkeep, monitoring, and incident response to a managed service provider. One of the services this provider offered was a "smut report" that identifies IP addresses surfing questionable Web sites.

On Monday morning, after installing a printer in the conference room, Paul received an e-mail containing a smut report that informed him that someone on his network had been downloading large amounts of porn over the weekend. The following is an excerpt from the report provided to Oblong by the firewall management company.

```
SMUT ALERT
Source IP: 192.168.1.20
Destination: www.reallydirtypornostuff.com
Type: Adult
Time: 04-26-2003:14:34:29
Duration: 25 minutes
Data: 52Mb
```

This was a clear violation of the company's acceptable use policy, and the company president had recently sent out an e-mail explaining Oblong's zero-tolerance policy regarding pornography. Paul was left with the unpleasant tasks of figuring out who the offending party was and gathering the needed information for termination. To make matters more difficult, the company used DHCP and had a number of users traveling in from remote offices who only used the network for a day or two before going back to the branch office.

Paul decided to stop by the coffee shop in the lobby for a latte. Due to the close proximity to the office, Paul often ran into co-workers in the coffee shop, and they often took advantage of the coffee shop's wireless network to chat with their friends, since that was also in violation of the company's AUP. He saw a group in line in front of him and wondered whether any of those people were going to be terminated because of whatever his investigation might turn up later in the day.

Paul went back to his office and got to work. He checked to see which user currently had the specific IP address. The company's DHCP leases were left on the default of three days, so most users would keep the same IP address for a long time even over the weekend. Paul pinged the IP to make sure it was still up:

```
C:\>ping 192.168.1.20
Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=200ms TTL=60
Reply from 192.168.1.20: bytes=32 time=20ms TTL=60
Reply from 192.168.1.20: bytes=32 time=40ms TTL=60
Reply from 192.168.1.20: bytes=32 time=70ms TTL=60
Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 200ms, Average = 82ms
```

The IP address appeared to be up, and it looked familiar. It was the printer that Paul had just installed for the training room; he had not received the permanent IP from engineering yet, so it was still using DHCP. In order to verify, he tried connecting to the printer.

```
C:\>telnet 192.168.1.20
HP JetDirect
Please type "?" for HELP, or "/" for current settings
```

Paul decided to review the logs on the Windows-based DHCP server to find out more about the IP address during the day in question. He noticed that the violation was on a Sunday. Normally, the office was totally empty on weekends. The janitorial staff completed the cleaning on Friday, so it was very odd to see usage on a weekend. He checked the network switch and conference that the network drops in the common areas were disconnected - they were. The offending system had to be located in one of the offices.

Now, Paul needed to figure out what computer owned the MAC address:

```
DHCP offer - 192.168.1.20 to 00-E0-98-9E-41-27
```

Paul checked the network for the MAC address, but it was not on his subnet. He checked the vender code - it was a Linksys card - not

the kind that they used on company issued systems. He then logged into a router that was on the same physical subnet to map IP addresses to MAC addresses.

```
Router#show ip arp
Protocol Address      Age(min)  Hardware Addr   Type   Interface
Internet 192.168.1.100    0         0010.5aa7.5ee6   ARPA   FastEthernet0
Internet 192.168.1.50     -         00e0.1eq7.0581   ARPA   FastEthernet0
Internet 192.168.1.1      0         0020.78cb.f43c   ARPA   FastEthernet0
Internet 192.168.1.5      15        0010.5aa7.e5fa   ARPA   FastEthernet0
Internet 192.168.1.20    15        0030.c1c1.8328   ARPA   FastEthernet0
Internet 192.168.1.103   15        00e0.989e.731e   ARPA   FastEthernet0
```

Paul noticed a different MAC address that was similar to the offending MAC address - they were both Linksys cards, and not company standard; deciding that this was his best lead, he investigated further. He knew the following Windows command could be used to find out information about Windows machines using NetBIOS, such as logged-in user, workgroup name, machine name, and other NetBIOS-specific information. He knew this command could also be used to find the MAC address of a machine on a remote network.

```
A:\>nbtstat -A 192.168.1.103
NetBIOS Remote Machine Name Table
Name           Type           Status
-----
JAY_LAPTOP    <00> UNIQUE      Registered
CAMPUS        <00> GROUP       Registered
JAY_LAPTOP    <03> UNIQUE      Registered
JAY_LAPTOP    <20> UNIQUE      Registered
CAMPUS        <1E> GROUP       Registered
JAY           <03> UNIQUE      Registered
MAC Address = 00-E0-98-9E-73-1E
```

The user of a similar MAC address was identified as Jay. The machine was identified as Jay's laptop. This deserved further investigation; besides, Paul had no other leads. Paul called Jay's extension, and Michelle, his secretary, answered and informed Paul that Jay was currently in a meeting. Paul set up an appointment for later that afternoon.

When Paul met with Jay, Jay explained that he was returning from Tokyo with his laptop and network card during the time of the illegal surfing. Paul asked Jay whether he knew of anyone else within the company with a similar laptop. The laptop that Jay was using was one that he personally purchased, and he did not know of any other people within the company with a similar one. He said he had bought the network card at a local electronics superstore.

Jay explained to Paul that many of the employees had been forced to buy their own equipment due to some recent budget cuts. The company provided desktop machines, but many of the employees who wanted laptops, PDAs, and so on, were forced to buy their own. This was also outside the company's AUP, but as long as they job got done, the company turned a blind eye to this.

On his way back to his desk, Paul started looking around the office and noticed a lot of machines that were not purchased by the company. He made a mental note to discuss this issue with his boss; I.T. should not have to support all of these new machines. Paul returned to his desk disappointed, but not willing to admit defeat. He logged into the router and checked MAC information one more time, hoping to find the elusive MAC address. He noticed that not only was the MAC address not there, but also Jay's MAC had disappeared. This was odd, for he was just at Jay's desk, and he had seen Jay downloading his e-mail. Paul again used the following commands to track machines and network cards. He tried to ping the name of Jay's laptop. Windows uses name resolution mechanisms to resolve the machine name to an IP address; in this case, it is a WINS lookup. The lookup was successful, and ping returned the IP address of the machine. If the machine were on the same subnet as Jay, Paul could check his arp cache. The machine was on a different subnet, however, so he used the local router.

```
C:\>ping Jay_laptop
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=200ms TTL=60
Reply from 192.168.1.100: bytes=32 time=20ms TTL=60
Reply from 192.168.1.100: bytes=32 time=40ms TTL=60
Reply from 192.168.1.100: bytes=32 time=70ms TTL=60
Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 200ms, Average = 82ms
```

```
Router#show ip arp
Protocol Address          Age(min)    Hardware Addr    Type    Interface
Internet 192.168.1.100        0           0010.5aa7.5ee6   ARPA    FastEthernet0
Internet 192.168.1.50.50     -           00e0.1eq7.0581   ARPA    FastEthernet0
Internet 192.168.1.1         0           0020.78cb.f43c   ARPA    FastEthernet0
Internet 192.168.1.5         15          0010.5aa7.e5fa   ARPA    FastEthernet0
Internet 192.168.1.20        15          0030.c1c1.8328   ARPA    FastEthernet0
```

Paul decided to visit Jay one more time. Paul asked Jay whether there was anything different about his network connection now compared to this morning. Jay informed Paul that he was in a meeting in the morning and was using the wireless connection. Wireless connection? There was no wireless connectivity. Jay informed Paul that about a month ago the sales group had set up a wireless network so that everyone could work in the conference room.

#### QUESTIONS

1. Was this an intentional attack?
2. Who was responsible for the illegal surfing?
3. How was it accomplished?
4. How was Jay involved in the incident?
5. How can it be prevented in the future?

Bring two printed copies of your analysis to class. Nothing handwritten will be accepted.