

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] SSDP Honeypot + Find Hosts for Scanning/Spoofing!](#)

Ruby - December 15, 2014, 11:19 pm

Overview of this tutorial.

For this tutorial I'll be using tcpdump to monitor certain ports for traffic and log that traffic to a file. Tcpdump is essentially the command-line version of Wireshark. The OS I'm using in this tutorial is Ubuntu 14.10.

With an SSDP honeypot you'll be able to pick up a lot of different SSDP scans and see the servers and the hosts people are using for scanning. Typically the hosts people are using for scanning also spoof. Wooh!

Code sudo apt-get install tcpdump
Install tcpdump.

Code sudo screen
Start a screen session.

Code sudo tcpdump -i eth0 'port 1900' -w ssdpcapture.pcap
This will start the tcpdump process on the interface eth0 (may be different on your server), monitor port 1900 for traffic, and log that traffic to the file ssdpcapture.pcap.

Code ctrl a d
Detach from your screen session.

Now you wait a couple days and let that honeypot pick up lots of different SSDP scans.

Code sudo screen -r
After a couple days have passed, ssh back into your server and reconnect to your screen session.

Code ctrl a c
This will kill the tcpdump process. In order to read the ssdpcapture.pcap traffic log, we have to kill the process.

Code exit
This will close your screen session. Tcpdump does not output the capture file correctly if a screen session is open (bug).

Code sudo tcpdump -r ssdpcapture.pcap
This will read the ssdpcapture.pcap traffic log and output its contents.

This is what some of the output of ssdpcapture.pcap traffic log should look like. This is clearly an SSDP scan...

...So now we go to bgp.he.net and use their bgp looking glass to find the host of the IP address from the ssdpcapture.pcap traffic log!

Ta da! A host for scanning/spoofing!

[Private Layer](#) (this host is already semi-public anyway). ?

askarne - December 16, 2014, 1:45 am

Not really true, I do port scan on a couple of servers that don't allow IP scanning or spoofing

Ruby - December 16, 2014, 9:12 am

(Dec 16, 2014 02:45 AM)askarne Wrote: [\[CITE\]](#) Not really true, I do port scan on a couple of servers that don't allow IP scanning or spoofing

You're going to have explain what you're trying to say because it doesn't make sense.

Zappos - December 16, 2014, 2:59 pm

(Dec 16, 2014 10:12 AM)Goliathuss Wrote: [\[CITE\]](#) You're going to have explain what you're trying to say because it doesn't make sense.

He's saying that on hosts that don't condone suspicious activity like port scans, he does it anyway. And if the company is dead enough and the process is mostly electronic, it's true because I do that all the time and not once even got a slight warning from the hosting company

Ruby - December 16, 2014, 4:41 pm

(Dec 16, 2014 03:59 PM)Zappos Wrote: [\[CITE\]](#) He's saying that on hosts that don't condone suspicious activity like port scans, he does it anyway. And if the company is dead enough and the process is mostly electronic, it's true because I do that all the time and not once even got a slight warning from the hosting company

Yeah I understand that much, what I don't understand is why you're both saying it. It's obvious. The hosts you find from this honeypot you have to just assume are cool with scanning. Although you can scan with any host.

Zappos - December 16, 2014, 9:26 pm

(Dec 16, 2014 05:41 PM)Goliathuss Wrote: [\[CITE\]](#) Yeah I understand that much, what I don't understand is why you're both saying it. It's obvious. The hosts you find from this honeypot you have to just assume are cool with scanning. Although you can scan with any host.oh okay now I understand the thread a little more. Although I'd still be careful with the hosts you do find.