What your Network Looks Like to the Bad Guys

Dave De Coster
decoster@wisc.edu
Disclaimer!

This is a VERY brief overview
Assumptions

• Following common best practices
• Have a firewall
• Patched
• Anti(virus|malware|spam|et cetera) running
• Passwords set

• All the other “normal” things
What can you see from the outside?

• If you run very few services, probably very little
• But.....
The Perimeter

The crunchy shell
Theory
Featureless barrier
Exposes very little
Keeps them guessing
Reality

A barrier
Get glimpses of the inside
Commonly Overlooked

Firewalls have external management capabilities as well.
Firewall Admin Interfaces

Commercial
- SNMP
- SSH
- Proprietary

SOHO
- Web / SOAP
- SSDP (UPnP)
- Telnet
Simple Network Management Protocol

• Typically used for collecting information from network connected devices
  • Modems, Routers, Switches, Servers, Printers, and more
• When asked nicely, it'll respond with lots of information
• `snmpget -c public -v 2c [IP] 1.3.6.1.2.1.1.1.0`

```
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.3(3)M6, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Tue 04-Aug-15 05:50 by prod_rel_team"
```
Simple Service Discovery Protocol

• Can be found on port 1900/UDP
• Provides a pointer to where the device’s admin interface is
• Designed for Plug’n Play
• Unfortunately, it often gets bound to the external interface
HTTP/1.1 200 OK
LOCATION: http://192.168.1.1:37215/upnpdev.xml
SERVER: Linux UPnP/1.0 Huawei-ATP-IGD
CACHE-CONTROL: max-age=86500
EXT:
ST: upnp:rootdevice
USN: uuid:00e0fc37-2525-2828-2500-5c7d5e42b8a4::upnp:rootdevice
SSDP (non-router)

HTTP/1.1 200 OK
CACHE-CONTROL: max-age=1800
DATE: Wed, 30 May 2018 02:09:35 GMT
EXT:
LOCATION: http://192.168.1.10:8011/upnpdevicedesc.xml
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01
01-NLS: 8b5a241a-1dd2-11b2-b980-b1899108f595
SERVER: Linux/3.0.8, UPnP/1.0, Portable SDK for UPnP devices/1.6.18
X-User-Agent: redsonic
ST: upnp:rootdevice
USN: uuid:48343631-3438-3633-3533-8CE7486120D0::upnp:rootdevice
SSDP
Substitute the IP you probed and...
NTP
Network Time Protocol

Great for synchronizing times
Has multiple modes
Some modes spit out more info
NTP Version Queries

version="ntpd 4.2.6p2@1.2194 Thu Apr 23 19:52:02 UTC 2015 (2)",
processor="x86_64", system="Linux/3.4.10", leap=0, stratum=2,
precision=-20, rootdelay=0.537, rootdispersion=2.108, peer=759,
refid=10.191.50.58, reftime=0xdeb87a12.e3f47f3a, poll=6,
clock=0xdeb87a63.ef6adc08, offset=0.028, frequency=1.415, noise=0.038,
jitter=0.050, stability=0.012
VNC/Remote Desktop

Very convenient for users, but (may) provide console access to the world
Enough Doom and Gloom

What can I do?
Limiting Exposure

• Check your firewall configs
  • Restrict access to only those things that need it

• You can still provide access to devices while making life difficult to everyone else
Limiting Exposure

- Consider Egress blocking
  - Block SSDP and SNMP responses
Limiting Exposure

- Enforce the use of VPN
  - Helps mitigate the exposure of RDP/VNC
Limiting Exposure

• Look to see what your network looks like from the outside
• Provider-type services
  • Shodan
    • https://www.shodan.io
    • Easy to use
    • Data is pre-parsed
  • Censys
    • https://scans.io
    • Little more involved
    • Data is raw
Limiting Exposure

• Do it yourself
  • Qualys
    • Has an option to scan from off-campus
    • Talk to the Office of Cybersecurity for details
  • Nmap
    • https://nmap.org
    • Make sure that you have permission to scan before testing yourself!
Questions?