Timothy Frymire
Aryan Kafley

Cyber/Infrastructure Defense
Assignment 4

Part 1: NMAP Your Network:

NAMP Startup and Info:
Starting Nmap 7.92 (https://nmap.org) at 2021-11-14 15:19 MST
Warning: 192.168.1.79 giving up on port because retransmission cap hit (2).
Warning: 192.168.1.139 giving up on port because retransmission cap hit (2).
Warning: 192.168.1.24 giving up on port because retransmission cap hit (2).
Warning: 192.168.1.179 giving up on port because retransmission cap hit (2).
Warning: 192.168.1.53 giving up on port because retransmission cap hit (2).

This is my UniFi Gateway:
Nmap scan report for unifi.localdomain (192.168.1.1)
Host is up (0.0042s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain dnsmasq 2.84rc2
80/tcp open http
443/tcp open ssl/https
6789/tcp open ibm-db2-admin?
8080/tcp open http-proxy
8443/tcp open ssl/https-alt
4 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(Get
SF:Request,1DF,"HTTP/1\.1\x20302\x20Found\r\nVary:\x20Origin\r\nX-DNS-Pref
SF:etch-Control:\x20off\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transp
SF:ort-Security:\x20max-age=15552000;\x20includeSubDomains\r\nX-Download-O
SF:ptions:\x20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS-Protec
SF:tion:\x201;\x20mode=block\r\nAccept-Ranges:\x20bytes\r\nLocation:\x20ht
SF:tps://\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Lengt
SF:h:\x2047\r\nX-Response-Time:\x209ms\r\nDate:\x20Sun,\x2014\x20Nov\x2020
SF:21\x2022:20:08\x20GMT\r\nConnection:\x20close\r\n\r\nRedirecting\x20to\
SF:x20<a\x20href=\"https://\">https://\.")%r(HTTPOptions,1DF,"HTTP/1\.
SF:1\x20302\x20Found\r\nVary:\x20Origin\r\nX-DNS-Prefetch-Control:\x20off\
SF:r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-
SF:age=15552000;\x20includeSubDomains\r\nX-Download-Options:\x20noopen\r\n
SF:X-Content-Type-Options:\x20nosniff\r\nX-XSS-Protection:\x201;\x20mode=b
SF:lock\r\nAccept-Ranges:\x20bytes\r\nLocation:\x20https://\r\nContent-Typ
SF:e:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x2047\r\nX-Respons
SF:e-Time:\x200ms\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:08\x20GMT
SF:\r\nConnection:\x20close\r\n\r\nRedirecting\x20to\x20<a\x20href=\"https
SF::://\">https://\.")%r(RTSPRequest,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n")%r(X11Probe,2F,"HTTP/1\.1\x20400\

SF:x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(FourOhFourRequest
SF:,1DF,"HTTP/1\.1\x20302\x20Found\r\nVary:\x20Origin\r\nX-DNS-Prefetch-Co
SF:ntrol:\x20off\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Transport-Sec
SF:urity:\x20max-age=15552000;\x20includeSubDomains\r\nX-Download-Options:
SF:\x20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS-Protection:\x
SF:201;\x20mode=block\r\nAccept-Ranges:\x20bytes\r\nLocation:\x20https://\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x204
SF:7\r\nX-Response-Time:\x203ms\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x202
SF:2:20:08\x20GMT\r\nConnection:\x20close\r\n\r\nRedirecting\x20to\x20<a\x
SF:20href=\"https://\">https://\.");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.92%T=SSL%I=7%D=11/14%Time=61918B9D%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,44A,"HTTP/1\.1\x20200\x20OK\r\nVary:\x20Origin\r\nX-DNS-
SF:Prefetch-Control:\x20off\r\nX-Frame-Options:\x20SAMEORIGIN\r\nStrict-Tr
SF:ansport-Security:\x20max-age=15552000;\x20includeSubDomains\r\nX-Downlo
SF:ad-Options:\x20noopen\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS-Pr
SF:otection:\x201;\x20mode=block\r\nAccept-Ranges:\x20bytes\r\nX-CSRF-Toke
SF:n:\x20a6fafe4d-0e81-47a3-9ac1-b44ecc893141\r\nContent-Type:\x20text/htm
SF:l;\x20charset=utf-8\r\nContent-Length:\x20377\r\nX-Response-Time:\x203m
SF:s\r\nSet-Cookie:\x20TOKEN=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9\.eyJjc3J
SF:mVG9rZW4iOiJhNmZhZmU0ZC0wZTgxLTQ3YTMtOWFjMS1iNDRlY2M4OTMxNDEiLCJpY
XQiOj
SF:E2MzY5Mjg0MTQsImV4cCI6MTYzNjkzMjAxNH0\.KasYt6GwamJzPQjey5FMloWVGuIf8_Yw
SF:aRUGkpQOfMw;\x20path=/;\x20samesite=strict;\x20secure;\x20httponly\r\nD
SF:ate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:14\x20GMT\r\nConnection:\x20
SF:close\r\n\r\n\n<!doctype\x20html>\n<html\x20lang=\"en\">\n<head>\n<meta
SF:\x20charset=\"utf-8\">\n<meta\x20name=\"viewport\"\x20content=\"width=d
SF:evice-width,initial-scale=1\"><link\x20href=\"/vendor\.b287c793\.chunk\
SF:.css\"\x20rel=\"sty")%r(HTTPOptions,44A,"HTTP/1\.1\x20200\x20OK\r\nVary
SF::\x20Origin\r\nX-DNS-Prefetch-Control:\x20off\r\nX-Frame-Options:\x20SA
SF:MEORIGIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20includeS
SF:ubDomains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x
SF:20nosniff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nAccept-Ranges:\x2
SF:0bytes\r\nX-CSRF-Token:\x2044ba4457-5459-4ad7-9640-5798b7bc1d93\r\nCont
SF:ent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x20377\r\nX
SF:-Response-Time:\x201ms\r\nSet-Cookie:\x20TOKEN=eyJhbGciOiJIUzI1NiIsInR5
SF:cCI6IkpXVCJ9\.eyJjc3JmVG9rZW4iOiI0NGJhNDQ1Ny01NDU5LTRhZDctOTY0MC01Nzk4Y
SF:jdiYzFkOTMiLCJpYXQiOjE2MzY5Mjg0MTQsImV4cCI6MTYzNjkzMjAxNH0\.kW541m-l098
SF:pm_Vc3TQCTgImbhzqGHIl8tgqv8tj_3o;\x20path=/;\x20samesite=strict;\x20sec
SF:ure;\x20httponly\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:14\x20G
SF:MT\r\nConnection:\x20close\r\n\r\n\n<!doctype\x20html>\n<html\x20lang=\
SF:"en\">\n<head>\n<meta\x20charset=\"utf-8\">\n<meta\x20name=\"viewport\"
SF:\x20content=\"width=device-width,initial-scale=1\"><link\x20href=\"/ven
SF:dor\.b287c793\.chunk\.css\"\x20rel=\"sty");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,24E,"HTTP/1\.1\x20400\x20\r\nContent-Type:\x20text/html;chars
SF:et=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x20435\r\nDate:\
SF:x20Sun,\x2014\x20Nov\x202021\x2022:20:07\x20GMT\r\nConnection:\x20close
SF:\r\n\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20Sta
SF:tus\x20400\x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20type=\"te
SF:xt/css\">body\x20{font-family:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x
SF:20h3,\x20b\x20{color:white;background-color:#525D76;}\x20h1\x20{font-si
SF:ze:22px;}\x20h2\x20{font-size:16px;}\x20h3\x20{font-size:14px;}\x20p\x2
SF:0{font-size:12px;}\x20a\x20{color:black;}\x20\.line\x20{height:1px;back
SF:ground-color:#525D76;border:none;}</style></head><body><h1>HTTP\x20Stat
SF:us\x20400\x20\xe2\x80\x93\x20Bad\x20Request</h1></body></html>")%r(HTTP
SF:Options,24E,"HTTP/1\.1\x20400\x20\r\nContent-Type:\x20text/html;charset
SF:=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x20435\r\nDate:\x2
SF:0Sun,\x2014\x20Nov\x202021\x2022:20:07\x20GMT\r\nConnection:\x20close\r
SF:\n\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20Statu
SF:s\x20400\x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20type=\"text
SF:/css\">body\x20{font-family:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x20
SF:h3,\x20b\x20{color:white;background-color:#525D76;}\x20h1\x20{font-size
SF::22px;}\x20h2\x20{font-size:16px;}\x20h3\x20{font-size:14px;}\x20p\x20{
SF:font-size:12px;}\x20a\x20{color:black;}\x20\.line\x20{height:1px;backgr
SF:ound-color:#525D76;border:none;}</style></head><body><h1>HTTP\x20Status
SF:\x20400\x20\xe2\x80\x93\x20Bad\x20Request</h1></body></html>")%r(RTSPRe
SF:quest,24E,"HTTP/1\.1\x20400\x20\r\nContent-Type:\x20text/html;charset=u
SF:tf-8\r\nContent-Language:\x20en\r\nContent-Length:\x20435\r\nDate:\x20S
SF:un,\x2014\x20Nov\x202021\x2022:20:08\x20GMT\r\nConnection:\x20close\r\n
SF:\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20Status\
SF:x20400\x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20type=\"text/c
SF:ss\">body\x20{font-family:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x20h3
SF:,\x20b\x20{color:white;background-color:#525D76;}\x20h1\x20{font-size:2
SF:2px;}\x20h2\x20{font-size:16px;}\x20h3\x20{font-size:14px;}\x20p\x20{fo
SF:nt-size:12px;}\x20a\x20{color:black;}\x20\.line\x20{height:1px;backgrou
SF:nd-color:#525D76;border:none;}</style></head><body><h1>HTTP\x20Status\x
SF:20400\x20\xe2\x80\x93\x20Bad\x20Request</h1></body></html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8443-TCP:V=7.92%T=SSL%I=7%D=11/14%Time=61918B9E%P=x86_64-pc-linux-g
SF:nu%r(GetRequest,5C,"HTTP/1\.1\x20404\x20\r\nContent-Length:\x200\r\nDat
SF:e:\x20Sun,\x2014\x20Nov\x202021\x2022:20:14\x20GMT\r\nConnection:\x20cl
SF:ose\r\n\r\n")%r(HTTPOptions,5C,"HTTP/1\.1\x20404\x20\r\nContent-Length:
SF:\x200\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:14\x20GMT\r\nConne
SF:ction:\x20close\r\n\r\n")%r(FourOhFourRequest,5C,"HTTP/1\.1\x20404\x20\
SF:r\nContent-Length:\x200\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:
SF:14\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,24E,"HTTP/1\.

SF:1\x20400\x20\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-Lan
SF:guage:\x20en\r\nContent-Length:\x20435\r\nDate:\x20Sun,\x2014\x20Nov\x2
SF:02021\x2022:20:20\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20ht
SF:ml><html\x20lang=\"en\"><head><title>HTTP\x20Status\x20400\x20\xe2\x80\
SF:x93\x20Bad\x20Request</title><style\x20type=\"text/css\">body\x20{font-
SF:family:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x20h3,\x20b\x20{color:wh
SF:ite;background-color:#525D76;}\x20h1\x20{font-size:22px;}\x20h2\x20{fon
SF:t-size:16px;}\x20h3\x20{font-size:14px;}\x20p\x20{font-size:12px;}\x20a
SF:\x20{color:black;}\x20\.line\x20{height:1px;background-color:#525D76;bo
SF:rder:none;}</style></head><body><h1>HTTP\x20Status\x20400\x20\xe2\x80\x
SF:93\x20Bad\x20Request</h1></body></html>")%r(RPCCheck,24E,"HTTP/1\.1\x20
SF:400\x20\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-Language
SF::\x20en\r\nContent-Length:\x20435\r\nDate:\x20Sun,\x2014\x20Nov\x202021
SF:\x2022:20:20\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20html><h
SF:tml\x20lang=\"en\"><head><title>HTTP\x20Status\x20400\x20\xe2\x80\x93\x
SF:20Bad\x20Request</title><style\x20type=\"text/css\">body\x20{font-famil
SF:y:Tahoma,Arial,sans-serif;}\x20h1,\x20h2,\x20h3,\x20b\x20{color:white;b
SF:ackground-color:#525D76;}\x20h1\x20{font-size:22px;}\x20h2\x20{font-siz
SF:e:16px;}\x20h3\x20{font-size:14px;}\x20p\x20{font-size:12px;}\x20a\x20{
SF:color:black;}\x20\.line\x20{height:1px;background-color:#525D76;border:
SF:none;}</style></head><body><h1>HTTP\x20Status\x20400\x20\xe2\x80\x93\x2
SF:0Bad\x20Request</h1></body></html>");
Aggressive OS guesses: Linux 3.2 - 4.9 (97%), Linux 3.2 - 3.16 (93%), Linux 3.16 (92%), Linux 2.6.32 (92%), Android 4.1.1 (92%), Android 4.2.2 (Linux 3.4) (92%), DD-WRT v3.0 (Linux 4.4.2) (92%), Linux 2.6.32 - 3.10 (92%), Android 4.1.2 (91%), Linux 3.18 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

<u>This is my home DNS Server:</u>
Nmap scan report for PiHole (192.168.1.2)
Host is up (0.011s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.9p1 Raspbian 10+deb10u2+rpt1 (protocol 2.0)
53/tcp open domain (generic dns response: REFUSED)
80/tcp open http   lighttpd 1.4.53
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.92%I=7%D=11/14%Time=61918B9C%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,30,"\0\.\0\x06\x85\x80\0\x01\0\x01\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x01\0\x01\0\0\0\x02\0\x04\0\0\0\0")%r(
SF:DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x85\0\0\0\0\0\0\0\0");
Aggressive OS guesses: Linux 5.0 - 5.3 (96%), Linux 2.6.32 (93%), Linux 3.2 - 4.9 (93%), Linux 4.15 - 5.6 (93%), Linux 2.6.32 - 3.10 (93%), Linux 5.3 - 5.4 (93%), Sony X75CH-series Android

TV (Android 5.0) (93%), Netgear ReadyNAS 2100 (RAIDiator 4.2.24) (93%), Netgear ReadyNAS device (RAIDiator 4.2.21 - 4.2.27) (91%), Linux 3.1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Apple HomePod:
Nmap scan report for 192.168.1.20
Host is up (0.010s latency).
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE VERSION
5000/tcp open rtsp
7000/tcp open rtsp
7100/tcp open rtsp AirTunes rtspd 595.15.41
49152/tcp open unknown
62078/tcp open tcpwrapped
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,49,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\
SF:r\nServer:\x20AirTunes/595\.15\.41\r\n\r\n")%r(RTSPRequest,D7,"RTSP/1\.
SF:0\x20200\x20OK\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:08\x20GMT
SF:\r\nContent-Length:\x200\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x
SF:20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PA
SF:RAMETER,\x20POST,\x20GET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\n
SF:\r\n")%r(HTTPOptions,D7,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sun,\x2014\
SF:x20Nov\x202021\x2022:20:13\x20GMT\r\nContent-Length:\x200\r\nPublic:\x2
SF:0ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPT
SF:IONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20GET,\x20PUT\r\nSe
SF:rver:\x20AirTunes/595\.15\.41\r\n\r\n")%r(FourOhFourRequest,49,"HTTP/1\
SF:.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20AirTune
SF:s/595\.15\.41\r\n\r\n")%r(SIPOptions,E9,"RTSP/1\.0\x20200\x20OK\r\nDate
SF::\x20Sun,\x2014\x20Nov\x202021\x2022:20:13\x20GMT\r\nContent-Length:\x2
SF:00\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20
SF:TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20G
SF:ET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\nCSeq:\x2042\x20OPTIONS
SF:\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7000-TCP:V=7.92%I=7%D=11/14%Time=61918BAB%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,49,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\

SF:r\nServer:\x20AirTunes/595\.15\.41\r\n\r\n")%r(HTTPOptions,D7,"HTTP/1\.
SF:1\x20200\x20OK\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:29\x20GMT
SF:\r\nContent-Length:\x200\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x
SF:20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_P
A
SF:RAMETER,\x20POST,\x20GET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\n
SF:\r\n")%r(RTSPRequest,D7,"RTSP/1\.0\x20200\x20OK\r\nDate:\x20Sun,\x2014\
SF:x20Nov\x202021\x2022:20:29\x20GMT\r\nContent-Length:\x200\r\nPublic:\x2
SF:0ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OP
T
SF:IONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20GET,\x20PUT\r\nSe
SF:rver:\x20AirTunes/595\.15\.41\r\n\r\n")%r(FourOhFourRequest,49,"HTTP/1\
SF:.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20AirTune
SF:s/595\.15\.41\r\n\r\n")%r(SIPOptions,E9,"RTSP/1\.0\x20200\x20OK\r\nDate
SF::\x20Sun,\x2014\x20Nov\x202021\x2022:20:34\x20GMT\r\nContent-Length:\x2
SF:00\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20
SF:TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x2
0G
SF:ET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\nCSeq:\x2042\x20OPTIONS
SF:\r\n\r\n");
Aggressive OS guesses: Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0) (94%), Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0) (93%), Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.0 (Darwin 15.6.0 - 19.0.0) (92%), Apple iOS 9.0 (Darwin 15.0.0) (92%), Apple OS X 10.11 (El Capitan) - 10.12 (Sierra) or iOS 10.1 - 10.2 (Darwin 15.4.0 - 16.6.0) (91%), Apple iPad tablet computer (iOS 4.3.2) (90%), Apple iPad tablet computer or iPhone mobile phone (iOS 4.0 - 4.1) (90%), Apple iPhone mobile phone (iOS 4.3.2) (90%), Apple Mac OS X 10.5 (Leopard) - 10.6.8 (Snow Leopard) or iOS 4.0 - 4.2.1 (Darwin 9.0.0b5 - 10.8.0) (90%), Apple iOS 5.0.1 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Apple HomePod:
Nmap scan report for 192.168.1.21
Host is up (0.020s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: NOTIMP)
5000/tcp open rtsp
7000/tcp open rtsp
7100/tcp open rtsp AirTunes rtspd 595.15.41
49152/tcp open unknown
62078/tcp open tcpwrapped
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=11/14%Time=61918B9C%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,2B,"\0\)\0\x06\x80\x80\0\x01\0\0\0\0\0\x01\x07version
SF:\x04bind\0\0\x10\0\x03\0\0\)\x10\0\0\0\0\0\0\0")%r(DNSStatusRequestTCP,
SF:E,"\0\x0c\0\0\x90\x04\0\0\0\0\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,49,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\
SF:r\nServer:\x20AirTunes/595\.15\.41\r\n\r\n")%r(RTSPRequest,D7,"RTSP/1\.
SF:0\x20200\x20OK\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:08\x20GMT
SF:\r\nContent-Length:\x200\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x
SF:20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_P
A
SF:RAMETER,\x20POST,\x20GET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\n
SF:\r\n")%r(HTTPOptions,D7,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sun,\x2014\
SF:x20Nov\x202021\x2022:20:13\x20GMT\r\nContent-Length:\x200\r\nPublic:\x2
SF:0ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OP
T
SF:IONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20GET,\x20PUT\r\nSe
SF:rver:\x20AirTunes/595\.15\.41\r\n\r\n")%r(FourOhFourRequest,49,"HTTP/1\
SF:.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20AirTune
SF:s/595\.15\.41\r\n\r\n")%r(SIPOptions,E9,"RTSP/1\.0\x20200\x20OK\r\nDate
SF::\x20Sun,\x2014\x20Nov\x202021\x2022:20:13\x20GMT\r\nContent-Length:\x2
SF:00\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20
SF:TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x2
0G
SF:ET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\nCSeq:\x2042\x20OPTIONS
SF:\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7000-TCP:V=7.92%I=7%D=11/14%Time=61918BAB%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,49,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\
SF:r\nServer:\x20AirTunes/595\.15\.41\r\n\r\n")%r(HTTPOptions,D7,"HTTP/1\.
SF:1\x20200\x20OK\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:28\x20GMT
SF:\r\nContent-Length:\x200\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x
SF:20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_P
A
SF:RAMETER,\x20POST,\x20GET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\n
SF:\r\n")%r(RTSPRequest,D7,"RTSP/1\.0\x20200\x20OK\r\nDate:\x20Sun,\x2014\
SF:x20Nov\x202021\x2022:20:28\x20GMT\r\nContent-Length:\x200\r\nPublic:\x2
SF:0ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OP
T
SF:IONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20GET,\x20PUT\r\nSe
SF:rver:\x20AirTunes/595\.15\.41\r\n\r\n")%r(FourOhFourRequest,49,"HTTP/1\
SF:.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20AirTune

SF:s/595\.15\.41\r\n\r\n")%r(SIPOptions,E9,"RTSP/1\.0\x20200\x20OK\r\nDate
SF::\x20Sun,\x2014\x20Nov\x202021\x2022:20:33\x20GMT\r\nContent-Length:\x2
SF:00\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20
SF:TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x2
0G
SF:ET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\nCSeq:\x2042\x20OPTIONS
SF:\r\n\r\n");
Aggressive OS guesses: Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0) (94%), Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.0 (Darwin 15.6.0 - 19.0.0) (93%), Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0) (92%), Apple OS X 10.11 (El Capitan) - 10.12 (Sierra) or iOS 10.1 - 10.2 (Darwin 15.4.0 - 16.6.0) (91%), Apple iOS 9.0 (Darwin 15.0.0) (90%), Apple iPad tablet computer (iOS 4.3.2) (90%), Apple iPad tablet computer or iPhone mobile phone (iOS 4.0 - 4.1) (90%), Apple iPhone mobile phone (iOS 4.3.2) (90%), Apple Mac OS X 10.5 (Leopard) - 10.6.8 (Snow Leopard) or iOS 4.0 - 4.2.1 (Darwin 9.0.0b5 - 10.8.0) (90%), Apple iOS 5.0.1 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Apple HomePod:
Nmap scan report for 192.168.1.23
Host is up (0.0087s latency).
Not shown: 994 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: NOTIMP)
5000/tcp open rtsp
7000/tcp open rtsp
7100/tcp open rtsp AirTunes rtspd 595.15.41
49152/tcp open unknown
62078/tcp open tcpwrapped
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=11/14%Time=61918B9C%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,2B,"\0\)\0\x06\x80\x80\0\x01\0\0\0\0\0\x01\x07version
SF:\x04bind\0\0\x10\0\x03\0\0\)\x10\0\0\0\0\0\0\0")%r(DNSStatusRequestTCP,
SF:E,"\0\x0c\0\0\x90\x04\0\0\0\0\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,49,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\
SF:r\nServer:\x20AirTunes/595\.15\.41\r\n\r\n")%r(RTSPRequest,D7,"RTSP/1\.
SF:0\x20200\x20OK\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:08\x20GMT
SF:\r\nContent-Length:\x200\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x
SF:20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_P
A

SF:RAMETER,\x20POST,\x20GET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\n
SF:\r\n")%r(HTTPOptions,D7,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Sun,\x2014\
SF:x20Nov\x202021\x2022:20:13\x20GMT\r\nContent-Length:\x200\r\nPublic:\x2
SF:0ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OP
T
SF:IONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20GET,\x20PUT\r\nSe
SF:rver:\x20AirTunes/595\.15\.41\r\n\r\n")%r(FourOhFourRequest,49,"HTTP/1\
SF:.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20AirTune
SF:s/595\.15\.41\r\n\r\n")%r(SIPOptions,E9,"RTSP/1\.0\x20200\x20OK\r\nDate
SF::\x20Sun,\x2014\x20Nov\x202021\x2022:20:13\x20GMT\r\nContent-Length:\x2
SF:00\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20
SF:TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x2
0G
SF:ET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\nCSeq:\x2042\x20OPTIONS
SF:\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port7000-TCP:V=7.92%I=7%D=11/14%Time=61918BAB%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,49,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\
SF:r\nServer:\x20AirTunes/595\.15\.41\r\n\r\n")%r(HTTPOptions,D7,"HTTP/1\.
SF:1\x20200\x20OK\r\nDate:\x20Sun,\x2014\x20Nov\x202021\x2022:20:28\x20GMT
SF:\r\nContent-Length:\x200\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x
SF:20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_P
A
SF:RAMETER,\x20POST,\x20GET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\n
SF:\r\n")%r(RTSPRequest,D7,"RTSP/1\.0\x20200\x20OK\r\nDate:\x20Sun,\x2014\
SF:x20Nov\x202021\x2022:20:28\x20GMT\r\nContent-Length:\x200\r\nPublic:\x2
SF:0ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20TEARDOWN,\x20OP
T
SF:IONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x20GET,\x20PUT\r\nSe
SF:rver:\x20AirTunes/595\.15\.41\r\n\r\n")%r(FourOhFourRequest,49,"HTTP/1\
SF:.1\x20404\x20Not\x20Found\r\nContent-Length:\x200\r\nServer:\x20AirTune
SF:s/595\.15\.41\r\n\r\n")%r(SIPOptions,E9,"RTSP/1\.0\x20200\x20OK\r\nDate
SF::\x20Sun,\x2014\x20Nov\x202021\x2022:20:33\x20GMT\r\nContent-Length:\x2
SF:00\r\nPublic:\x20ANNOUNCE,\x20SETUP,\x20RECORD,\x20PAUSE,\x20FLUSH,\x20
SF:TEARDOWN,\x20OPTIONS,\x20GET_PARAMETER,\x20SET_PARAMETER,\x20POST,\x2
0G
SF:ET,\x20PUT\r\nServer:\x20AirTunes/595\.15\.41\r\nCSeq:\x2042\x20OPTIONS
SF:\r\n\r\n");
Aggressive OS guesses: Apple OS X 10.11 (El Capitan) - 10.12 (Sierra) or iOS 10.1 - 10.2 (Darwin 15.4.0 - 16.6.0) (94%), Apple TV 5 (92%), Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0) (92%), Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0) (91%), Apple TV 5.2.1 or 5.3 (89%), Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.0 (Darwin 15.6.0 - 19.0.0) (89%), Apple Mac OS X 10.6.5 (Snow Leopard) (Darwin 10.5.0) (89%), FreeBSD 11.1-STABLE (89%), Apple

Mac OS X Server 10.5 (Leopard) pre-release build 9A284 (87%), Apple macOS 10.12.5 (Sierra) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Belkin Smart Outlet:

```
Nmap scan report for 192.168.1.24
Host is up (0.0099s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
53/tcp    open     domain  (generic dns response: REFUSED)
5961/tcp  filtered unknown
49153/tcp open     upnp
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=11/14%Time=61918B9C%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,30,"\0\.\0\x06\x85\x80\0\x01\0\x01\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x01\0\x01\0\0\0\x02\0\x04\0\0\0\0")%r(
SF:DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x85\0\0\0\0\0\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port49153-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(
SF:mongodb,BD,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVER:\x20Unspecifie
SF:d,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2050\r\nAccept-Rang
SF:es:\x20bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>400\x
SF:20Bad\x20Request</h1></body></html>")%r(GetRequest,B9,"HTTP/1\.0\x20404
SF:\x20Not\x20Found\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecifie
SF:d\r\nCONTENT-LENGTH:\x2048\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\
SF:x20text/html\r\n\r\n<html><body><h1>404\x20Not\x20Found</h1></body></ht
SF:ml>")%r(HTTPOptions,C5,"HTTP/0\.0\x20501\x20Not\x20Implemented\r\nSERVE
SF:R:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x205
SF:4\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html
SF:><body><h1>501\x20Not\x20Implemented</h1></body></html>")%r(RTSPRequest
SF:,BD,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVER:\x20Unspecified,\x20U
SF:PnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2050\r\nAccept-Ranges:\x20
SF:bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x
SF:20Request</h1></body></html>")%r(RPCCheck,BD,"HTTP/0\.0\x20400\x20Bad\x
SF:20Request\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCO
SF:NTENT-LENGTH:\x2050\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text
SF:/html\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1></body></html>")
SF:%r(DNSVersionBindReqTCP,BD,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVE
SF:R:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x205
SF:0\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html
SF:><body><h1>400\x20Bad\x20Request</h1></body></html>")%r(FourOhFourReque
```

SF:st,B9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nSERVER:\x20Unspecified,\x20U
SF:PnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2048\r\nAccept-Ranges:\x20
SF:bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>404\x20Not\x
SF:20Found</h1></body></html>")%r(SIPOptions,BD,"HTTP/0\.0\x20400\x20Bad\x
SF:20Request\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCO
SF:NTENT-LENGTH:\x2050\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text
SF:/html\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1></body></html>");
Aggressive OS guesses: OpenWrt Kamikaze - Backfire or SuperMicro BMC (Linux 2.6.19 - 2.6.32) (97%), Linux 2.6.18 - 2.6.32 (96%), Thecus 4200 or N5500 NAS device (Linux 2.6.33) (96%), Vilar IP Camera (Linux 2.6) (95%), Cisco WAE-512 Wide Area Application Engine (ACNS 5.5.5.4) (95%), OpenWrt (Linux 2.4.32) (94%), OpenWrt White Russian 0.9 (Linux 2.4.30) (94%), OpenWrt Backfire 10.03 (Linux 2.6.32) (94%), OpenWrt (Linux 2.4.30 - 2.4.34) (94%), OpenWrt Kamikaze 8.09 (Linux 2.6.26) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Harmony TV Controller:
Nmap scan report for 192.168.1.53
Host is up (0.010s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
8088/tcp open radan-http?
8222/tcp open unknown
Aggressive OS guesses: Linux 2.6.17 - 2.6.36 (97%), Linux 2.6.32 - 2.6.35 (95%), D-Link DIR-600 or DIR-645 WAP (Linux 2.6.33) (94%), Linux 2.6.16 - 2.6.35 (embedded) (94%), Linux 2.6.24 - 2.6.36 (94%), Linux 2.6.13 - 2.6.32 (94%), AXIS 207W Network Camera (93%), Linux 2.6.18 - 2.6.32 (93%), Linux 2.6.22 - 2.6.23 (93%), Linux 2.4.20 (Red Hat 7.2) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Phillips Hue Bridge:
Nmap scan report for 192.168.1.79
Host is up (0.0050s latency).
Not shown: 840 closed tcp ports (reset), 157 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http nginx
443/tcp open ssl/http nginx
8080/tcp open http Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
Aggressive OS guesses: Philips Hue Bridge 2.0 (Linux) (97%), OpenWrt (Linux 3.3) (93%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (91%), OpenWrt (Linux 2.4.32) (91%), OpenWrt White Russian 0.9 (Linux 2.4.30) (91%), Asus RT-N10 router or AXIS 211A Network Camera (Linux 2.6) (91%), Linux 2.6.18 (91%), AXIS 211A Network Camera (Linux 2.6.20) (91%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (91%), Linux 2.6.16 (90%)

No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

iPad:
Nmap scan report for 192.168.1.80
Host is up (0.0093s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE VERSION
49152/tcp open unknown
62078/tcp open tcpwrapped
Device type: phone|general purpose
Running: Apple iOS 11.X|12.X|13.X, Apple macOS 10.13.X|10.14.X|10.15.X
OS CPE: cpe:/o:apple:iphone_os:11 cpe:/o:apple:iphone_os:12 cpe:/o:apple:iphone_os:13 cpe:/o:apple:mac_os_x:10.13 cpe:/o:apple:mac_os_x:10.14 cpe:/o:apple:mac_os_x:10.15
OS details: Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS 11.0 - 13.4 (Darwin 17.0.0 - 19.2.0)
Network Distance: 2 hops

SmartThings Hub:
Nmap scan report for 192.168.1.88
Host is up (0.0062s latency).
All 1000 scanned ports on 192.168.1.88 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Citrix Access Gateway VPN gateway (95%), Linksys WRT610Nv3 WAP (95%), 3Com OfficeConnect 3CRWER100-75 wireless broadband router (94%), Adtran 424RG FTTH gateway (94%), Aerohive HiveOS 3.4 (94%), Aerohive HiveOS 5.1 (94%), Aerohive HiveOS 7.1 (94%), AirMagnet SmartEdge wireless sensor; or Foscam FI8904W, FI8910W, or FI8918W, or Instar IN-3010 surveillance camera (Linux 2.4) (94%), Alcatel-Lucent OmniPCX GD3 PBX (Linux 2.6.23) (94%), Allnet 2210 webcam, Cisco MDS 9124 or 9216i switch (SAN-OS 3.1 - 3.2), or Nortel IP Phone 1535 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

iPhone:
Nmap scan report for 192.168.1.119
Host is up (0.0044s latency).
Not shown: 999 closed tcp ports (reset)
PORT STATE SERVICE VERSION
62078/tcp open tcpwrapped
Device type: firewall
Running (JUST GUESSING): Fortinet embedded (87%)

OS CPE: cpe:/h:fortinet:fortigate_100d
Aggressive OS guesses: Fortinet FortiGate 100D firewall (87%)
No exact OS matches for host (test conditions non-ideal).

Belkin Smart Outlet:
Nmap scan report for 192.168.1.139
Host is up (0.011s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: REFUSED)
85/tcp filtered mit-ml-dev
144/tcp filtered news
2045/tcp filtered cdfunc
2135/tcp filtered gris
5960/tcp filtered unknown
9071/tcp filtered unknown
9110/tcp filtered unknown
9917/tcp filtered unknown
9943/tcp filtered unknown
49153/tcp open upnp Belkin Wemo upnpd (UPnP 1.0)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.92%I=7%D=11/14%Time=61918B9C%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,30,"\0\.\0\x06\x85\x80\0\x01\0\x01\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x01\0\x01\0\0\0\x02\0\x04\0\0\0\0")%r(
SF:DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x85\0\0\0\0\0\0\0\0");
Aggressive OS guesses: OpenWrt Kamikaze - Backfire or SuperMicro BMC (Linux 2.6.19 - 2.6.32) (97%), Linux 2.6.18 - 2.6.32 (96%), Thecus 4200 or N5500 NAS device (Linux 2.6.33) (96%), Vilar IP Camera (Linux 2.6) (95%), Cisco WAE-512 Wide Area Application Engine (ACNS 5.5.5.4) (95%), OpenWrt (Linux 2.4.32) (94%), OpenWrt White Russian 0.9 (Linux 2.4.30) (94%), OpenWrt (Linux 2.4.30 - 2.4.34) (94%), OpenWrt Kamikaze 8.09 (Linux 2.6.26) (94%), OpenWrt Backfire 10.03 (Linux 2.6.32) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Device: power-misc

Belkin Smart Outlet:
Nmap scan report for 192.168.1.179
Host is up (0.011s latency).
Not shown: 970 closed tcp ports (reset), 28 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain (generic dns response: REFUSED)
49153/tcp open upnp

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port53-TCP:V=7.92%I=7%D=11/14%Time=61918B9C%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,30,"\0\.\0\x06\x85\x80\0\x01\0\x01\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03\xc0\x0c\0\x01\0\x01\0\0\0\x02\0\x04\0\0\0\0")%r(
SF:DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x85\0\0\0\0\0\0\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port49153-TCP:V=7.92%I=7%D=11/14%Time=61918B97%P=x86_64-pc-linux-gnu%r(
SF:mongodb,BD,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVER:\x20Unspecifie
SF:d,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2050\r\nAccept-Rang
SF:es:\x20bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>400\x
SF:20Bad\x20Request</h1></body></html>")%r(GetRequest,B9,"HTTP/1\.0\x20404
SF:\x20Not\x20Found\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecifie
SF:d\r\nCONTENT-LENGTH:\x2048\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\
SF:x20text/html\r\n\r\n<html><body><h1>404\x20Not\x20Found</h1></body></ht
SF:ml>")%r(HTTPOptions,C5,"HTTP/0\.0\x20501\x20Not\x20Implemented\r\nSERVE
SF:R:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x205
SF:4\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html
SF:><body><h1>501\x20Not\x20Implemented</h1></body></html>")%r(RTSPRequest
SF:,BD,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVER:\x20Unspecified,\x20U
SF:PnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2050\r\nAccept-Ranges:\x20
SF:bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x
SF:20Request</h1></body></html>")%r(RPCCheck,BD,"HTTP/0\.0\x20400\x20Bad\x
SF:20Request\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCO
SF:NTENT-LENGTH:\x2050\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text
SF:/html\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1></body></html>")
SF:%r(DNSVersionBindReqTCP,BD,"HTTP/0\.0\x20400\x20Bad\x20Request\r\nSERVE
SF:R:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x205
SF:0\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html
SF:><body><h1>400\x20Bad\x20Request</h1></body></html>")%r(FourOhFourReque
SF:st,B9,"HTTP/1\.0\x20404\x20Not\x20Found\r\nSERVER:\x20Unspecified,\x20U
SF:PnP/1\.0,\x20Unspecified\r\nCONTENT-LENGTH:\x2048\r\nAccept-Ranges:\x20
SF:bytes\r\nCONTENT-TYPE:\x20text/html\r\n\r\n<html><body><h1>404\x20Not\x
SF:20Found</h1></body></html>")%r(SIPOptions,BD,"HTTP/0\.0\x20400\x20Bad\x
SF:20Request\r\nSERVER:\x20Unspecified,\x20UPnP/1\.0,\x20Unspecified\r\nCO
SF:NTENT-LENGTH:\x2050\r\nAccept-Ranges:\x20bytes\r\nCONTENT-TYPE:\x20text
SF:/html\r\n\r\n<html><body><h1>400\x20Bad\x20Request</h1></body></html>");
Aggressive OS guesses: OpenWrt Kamikaze - Backfire or SuperMicro BMC (Linux 2.6.19 - 2.6.32) (97%), Thecus 4200 or N5500 NAS device (Linux 2.6.33) (97%), Linux 2.6.18 - 2.6.32 (96%), Vilar IP Camera (Linux 2.6) (95%), Cisco WAE-512 Wide Area Application Engine (ACNS 5.5.5.4) (95%), OpenWrt (Linux 2.4.32) (94%), OpenWrt White Russian 0.9 (Linux 2.4.30) (94%), OpenWrt Backfire 10.03 (Linux 2.6.32) (94%), Pirelli AV4202N wireless ADSL modem (94%), Huawei HG8240 GPON ONT (94%)

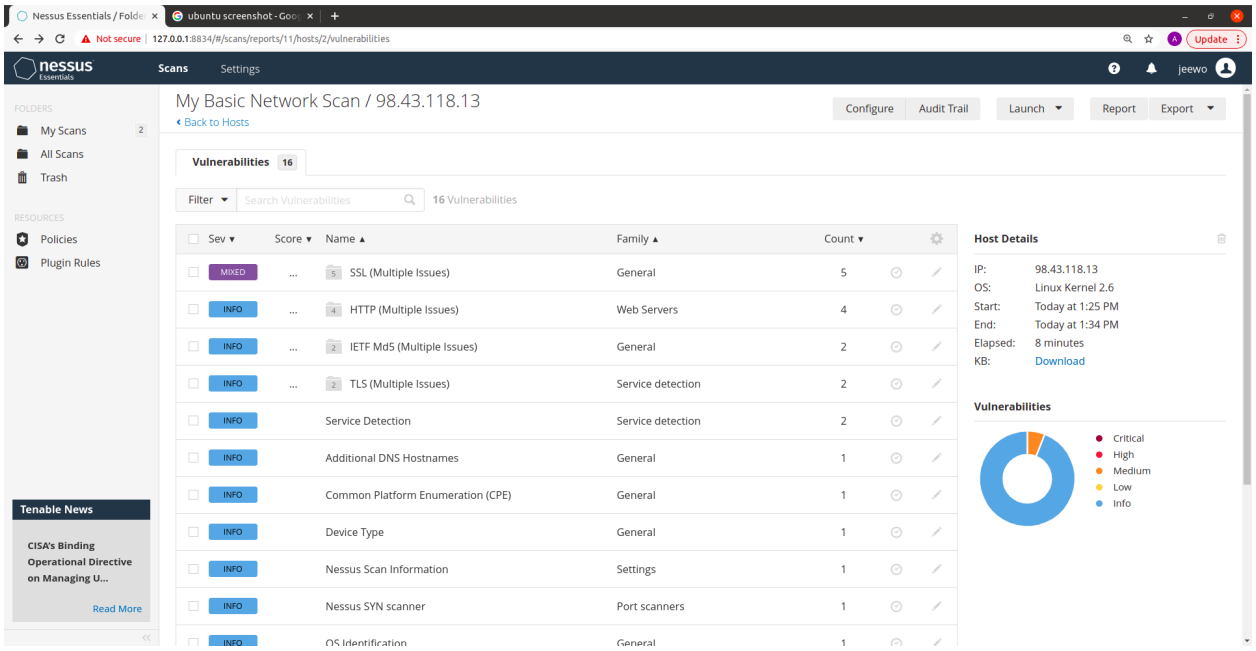
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

Smart Home Controller (Home Assistant):
Nmap scan report for homeassistant (192.168.1.230)
Host is up (0.0048s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.4 (protocol 2.0)
Aggressive OS guesses: Linux 4.15 - 5.6 (97%), Linux 5.0 - 5.3 (96%), Linux 5.0 - 5.4 (94%), Linux 2.6.32 (93%), Linux 3.2 - 4.9 (93%), Linux 2.6.32 - 3.10 (93%), Linux 5.3 - 5.4 (93%), Linux 5.4 (93%), Linux 3.4 - 3.10 (92%), Synology DiskStation Manager 5.2-5644 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (14 hosts up) scanned in 228.48 seconds

Part 2: Vulnerability Analysis

The scan was performed remotely by Aryan on Tim's network to find the vulnerability remotely. Screenshot of the Nessus scan:



<u>The top five vulnerabilities are:</u>

1) SSL
2) HTTP
3) IETF Md5
4) TLS
5) Service Detection

According to the cve database, For SSL (certificate could not be trusted) issue was discovered in Erlang/OTP before 23.2.2. The ssl application 10.2 accepts and trusts an invalid X.509 certificate chain to a trusted root Certification Authority. In this vulnerability, an attacker could be using a fake certificate from a non-public certificate provider to fraudulently get into the system pretending to be an authorized party.

In HTTP(HSTS Missing From HTTPS Server) it is due to using an affected version of tensorflow (machine learning platform). According to the CVE database this problem is currently being resolved and will soon be released with an updated version without this vulnerability.

IETF Md5 (SSL Certificate Signed Using Weak Hashing Algorithm (Known CA) is a vulnerability that was found in the postgresql-jdbc before version 42.2.5. To use this vulnerability, It was possible to provide an SSL Factory and not check the hostname if a

host name verifier was not provided to the driver. A man in the middle attack could be a possibility by using this vulnerability.

TLS(TLS Version 1.2 Protocol Detection), this is a vulnerability in the mozilla firefox where the browser does not reject the MD5 signatures in Server Key Exchange messages in TLS 1.2 Handshake Protocol traffic, which makes it vulnerable for the man in the middle attack.

Service Detection is a vulnerability where multiple cisco products were affected which led into the causing DOS to many of the users. This vulnerability is due to improper memory resource management.

Part 3: ARP and DNS Queries

3.2

The DNS queries and responses used UDP, which is labeled as Decimal 17 in the header.

3.4

ARP Queries:

(3.1) Wireshark Filter: arp

Source IP/MAC Address

Destination IP/MAC Address

Address Resolution Protocol (request)

Opcode: request (1)

Sender MAC address: Technico_1b:32:17 (80:b2:34:1b:32:17)

Sender IP address: 10.0.0.1 (10.0.0.1)

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

(Target MAC is all 00.* because we are seeking that MAC address with this ARP query)

Target IP address: 10.0.0.232 (10.0.0.232)

Address Resolution Protocol (reply)

Opcode: reply (2)

Sender MAC address: IntelCor_d5:41:89 (7c:b2:7d:d5:41:89)

Sender IP address: 10.0.0.232 (10.0.0.232)

Target MAC address: Technico_1b:32:17 (80:b2:34:1b:32:17)`

Target IP address: 10.0.0.1 (10.0.0.1)

DNS Queries:

(3.3) WireShark Filter: dns

(192.168.1.2 is a home implementation of a DNS server running PiHole on a RaspberryPi)

Source IP/MAC Address

Destination IP/MAC Address

Additional Relevant Information

Who Asked and Answered (Same for Both):

Ethernet II, Src: IntelCor_aa:74:27 (**20:79:18:aa:74:27**), Dst: Raspberr_ca:b0:bf (**b8:27:eb:ca:b0:bf**)

Destination: Raspberr_ca:b0:bf (b8:27:eb:ca:b0:bf)

Source: IntelCor_aa:74:27 (20:79:18:aa:74:27)

Type: IPv4 (0x0800)

This is an IPv6 DNS Query to find Wikipedia.org:

1681 2.642240 192.168.1.97 192.168.1.2 DNS 77 Standard query 0x2493 AAAA www.wikipedia.org

Domain Name System (query)
Queries
www.wikipedia.org: type AAAA, class IN
Name: www.wikipedia.org
[Name Length: 17]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 1701]

This is an IPv4 DNS Query to find Wikipedia.org:

1683 2.642402 192.168.1.97 192.168.1.2 DNS 77 Standard query 0x8dc8 A www.wikipedia.org

Domain Name System (query)
Queries
www.wikipedia.org: type A, class IN
Name: www.wikipedia.org
[Name Length: 17]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 1702]

DNS Responses:

WireShark Filter: dns

(192.168.1.2 is a home implementation of a DNS server running PiHole on a RaspberryPi)

Source IP/MAC Address

Destination IP/MAC Address

Additional Relevant Information

Who Asked and Answered (Same for Both):

Ethernet II, Src: Raspberr_ca:b0:bf (**b8:27:eb:ca:b0:bf**), Dst: IntelCor_aa:74:27 (**20:79:18:aa:74:27**)
Destination: IntelCor_aa:74:27 (20:79:18:aa:74:27)
Source: Raspberr_ca:b0:bf (b8:27:eb:ca:b0:bf)
Type: IPv4 (0x0800)

This is an IPv6 DNS Response for Wikipedia.org:

1701 2.677182 192.168.1.2 192.168.1.97 DNS 134 Standard query response 0x2493 AAAA www.wikipedia.org CNAME dyna.wikimedia.org AAAA 2620:0:860:ed1a::1

Domain Name System (response)
Queries
www.wikipedia.org: type AAAA, class IN
Name: www.wikipedia.org
[Name Length: 17]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
www.wikipedia.org: type CNAME, class IN, cname dyna.wikimedia.org
Name: www.wikipedia.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 86231 (23 hours, 57 minutes, 11 seconds)
Data length: 17
CNAME: dyna.wikimedia.org
dyna.wikimedia.org: type AAAA, class IN, addr 2620:0:860:ed1a::1
Name: dyna.wikimedia.org
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 431 (7 minutes, 11 seconds)
Data length: 16
AAAA Address: 2620:0:860:ed1a::1
[Request In: 1681]
[Time: 0.034942000 seconds]

This is an IPv4 DNS Response for Wikipedia.org:
1702 2.680366 192.168.1.2 192.168.1.97 DNS 122 Standard query response 0x8dc8 A www.wikipedia.org CNAME dyna.wikimedia.org A 208.80.153.224

Domain Name System (response)
Queries
www.wikipedia.org: type A, class IN
Name: www.wikipedia.org
[Name Length: 17]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.wikipedia.org: type CNAME, class IN, cname dyna.wikimedia.org
Name: www.wikipedia.org

Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 85870 (23 hours, 51 minutes, 10 seconds)
Data length: 17
CNAME: dyna.wikimedia.org
dyna.wikimedia.org: type A, class IN, addr 208.80.153.224
Name: dyna.wikimedia.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 70 (1 minute, 10 seconds)
Data length: 4
Address: 208.80.153.224
[Request In: 1683]
[Time: 0.037964000 seconds]

TCP Questions:

(3.5/6) WireShark Filter: tcp.flags.syn==1 && tcp.flags.ack ==0

Questions:

Local TCP Port Number
Remote TCP Port Number
Remote IP Address
Destination MAC Address
Source MAC Address

(3.7/3.8.2)

Connection 1:

1707 2.687932 2601:282:1a7f:f81a:108d:830f:526b:c929 2620:0:860:ed1a::1 TCP 86 51372 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1

Ethernet II, Src: IntelCor_aa:74:27 (20:79:18:aa:74:27), Dst: 6a:d7:9a:41:2e:c1 (6a:d7:9a:41:2e:c1)
Destination: 6a:d7:9a:41:2e:c1 (6a:d7:9a:41:2e:c1)
Source: IntelCor_aa:74:27 (20:79:18:aa:74:27)
Type: IPv6 (0x86dd)

Transmission Control Protocol, Src Port: 51372, Dst Port: 443, Seq: 0, Len: 0

Connection 2:

2241 3.326463 2601:282:1a7f:f81a:108d:830f:526b:c929 2620:0:860:ed1a::1 TCP 86 51375 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1

Ethernet II, Src: IntelCor_aa:74:27 (20:79:18:aa:74:27), Dst: 6a:d7:9a:41:2e:c1 (6a:d7:9a:41:2e:c1)
Destination: 6a:d7:9a:41:2e:c1 (6a:d7:9a:41:2e:c1)

Source: IntelCor_aa:74:27 (20:79:18:aa:74:27)
Type: IPv6 (0x86dd)

Transmission Control Protocol, Src Port: 51375, Dst Port: 443, Seq: 0, Len: 0

(3.8.1)

Why are all the outgoing packets going to this particular MAC address?

Packets are going to the 6a:d7:9a:41:2e:c1 address, as that was resolved in the ARP/DNS queries. These resolved Wikipedia.org to a specific IP address, which then resolved to a hardware address of what we assume is a wikipedia server.