

AFSL Audit Report

Report #36

|  |  |
| --- | --- |
| **PREPARED FOR**UW ASFL | **PREPARED DATE**May 8, 2018 |

# 

# 

# SCOPE OF AUDIT

This audit covers the following IP addresses. Any further systems owned by the AFSL will not be tested for security flaws. Specific ports for key services are listed below.

1. 128.95.35.199
2. 128.95.35.200
3. 199:1666 -> Perforce
4. 200:5000 -> Synology

# RECONNAISSANCE

Our analysis of the attack surface consisted of the following:

1. Opening with a ping request to both servers.
   1. 200 IP successfully delivered packets.
   2. 199 IP returned a “Request timeout for icmp\_seq #” indicating the presence of a Firewall
   3. Both of these indicate the server is online and accessible
2. A SYN Scan of both IPs in the maximum port range (1-65535) with UDP services included.
   1. 200 IP - Illuminated the following services are running.

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

548/tcp open afp

1723/tcp open pptp

3261/tcp open winshadow

3262/tcp open necp

3263/tcp open ecolor-imager

3264/tcp open ccmail

5000/tcp open upnp

5001/tcp open commplex-link

5005/tcp open avt-profile-2

5006/tcp open wsm-server

6281/tcp open unknown

6690/tcp open cleverdetect

* 1. 199 IP - Showed all ports as filtered at a cursory scan, upon further review the only open port is 1666/tcp

1. A SYN ACK scan on all of the ports running services. This was only run on the 200 machine. Additional information was discovered for each of the running services including the Version and Operating System.

PORT STATE SERVICE REASON VERSION

53/tcp open domain syn-ack ttl 255 ISC BIND DNSServer

80/tcp open http syn-ack ttl 255 nginx

139/tcp open netbios-ssn syn-ack ttl 255 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

443/tcp open ssl/http syn-ack ttl 255 nginx

445/tcp open netbios-ssn syn-ack ttl 255 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

548/tcp open afp syn-ack ttl 255 Netatalk 3.1.8 (name: AIARGDS; protocol 3.4)

1723/tcp open pptp syn-ack ttl 255 cananian (Firmware: 1)

3261/tcp open winshadow? syn-ack ttl 255

3262/tcp open necp? syn-ack ttl 255

3263/tcp open ecolor-imager? syn-ack ttl 255

3264/tcp open ccmail? syn-ack ttl 255

5000/tcp open http syn-ack ttl 255 nginx

5001/tcp open ssl/http syn-ack ttl 255 nginx

5005/tcp open http syn-ack ttl 255 Apache httpd

5006/tcp open ssl/http syn-ack ttl 255 Apache httpd

6281/tcp open unknown syn-ack ttl 255

6690/tcp open cleverdetect? syn-ack ttl 255

Service Info: Hosts: AIARGDS, local; OS: Unix

1. A Window Scan
   1. 200 - Returned all ports as open, which is behavior of a Firewall
   2. 199 - Returned all ports as open, which is behavior of a Firewall
2. An aggressive Operating System check, which produced the following:

Aggressive OS guesses: Grandstream GXP1105 VoIP phone (92%), Garmin Virb Elite action camera (89%), 2N Helios IP VoIP doorbell (89%), FireBrick FB2700 firewall (87%), NodeMCU firmware (lwIP stack) (86%), Cognex DataMan 200 ID reader (lwIP TCP/IP stack) (86%), Sony PlayStation 2 game console (86%), Philips Hue Bridge (lwIP stack v1.4.0) (85%), Rigol DSG3060 signal generator (85%)

No exact OS matches for host (test conditions non-ideal).

1. An nmblookup on the 200 IP, which returned no reply
2. Metasploit exploit review for each service

# RISK ANALYSIS

Based on our analysis of the attack surface, we’ve determined the AFSL systems are at a

low risk for intrusion. 200 has multiple services running that show up in our scans, however these services are up to date with recent patches and 0 publically available exploits were found for these particular service versions in the Metasploit Framework.

Additional scans to determine the Operating System running on the machine returned

inaccurate information, which was likely obfuscated by the Firewall. Even an nmblookup was

unsuccessful, making it difficult to determine any additional information about the Samba

instance running on the machine.

Although it’s not recommended for your use case, your DNS server is not vulnerable to zone transfers.

# MITIGATIONS & RECOMMENDATIONS

On the 128.95.35.200 server, it’s dangerous to leave netbois-ssn services open to the internet, those services should only even be visible to the internal network. Also, the synology and samba services seem up to date, but be aware that in past versions of those programs malicious actors could easily gain remote code execution through those services. Note that with synology and the associated nginx program, you can set it up such that nginx acts as a reverse proxy. furthermore you should disable the non encrypted version of both of those services, after all you are already serving the non-encrypted version.

For data availability you should look into conducting regular backups and store your files (perforce, and the smb share) on a RAID array for data security should a drive fail.

Regarding the 128.95.35.199 server, this server is much more secure and only allows the one port to talk to the outside world, but keep the service updated as in previous versions malicious actors were able to arbitrarily overwrite files without authentication, also look into tunneling this through TLS via nginx, that way the information stays confidential and maintains its integrity.

You can use IP tables on your Linux instance to close/open ports.