Declaration of Aaron Wagner

Pursuant to 28 U.S.C Section 1746, I, Aaron Wagner, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I have owned since 1997 Net Concepts AZ LLC (Net Concepts), a local IT service company in Arizona. I am a Certified Information Systems Security Professional (CISSP).
3. [redacted]
4. My affidavit highlights wireless network access.
5. Background:

   I wanted to take a moment to outline that the assumptions made in this document are not an exhaustive list of the possibilities and/or vulnerabilities discovered. Without proper authorization no thorough examination could take place. The only examination is based upon what is public and exposed out in the open with no encryption or network isolation. Devices are identified merely by the banner returned during an initial handshake. While some possible vulnerabilities can be demonstrated by more obvious means, some vulnerabilities require thinking outside of traditional norms when discussing election systems. For example: A switch/router that is at the end of life and no longer gets updates would be traditional network vulnerability, allowing USB devices to be plugged in could allow data to be exfiltrated by nontraditional means. Think of a USB stick that communicates on the 900Mhz spectrum vs 2.4 or 5GHz like a traditional wireless network. A great example of that would be https://gotenna.com/.

   In a traditional sense a USB stick the size of a dime may be able to communicate with the MCPublic Wi-Fi or any other several Wi-Fi networks that exists in proximity of the tabulation center. An employee of Dominion has done an extensive talk on how 4G networks can be used with the system which can be a USB stick. Printers have been proven to be an entry point or a place to "hide" on a network. There is a printer on the public Wi-Fi, what would happen if a USB stick allowed a tabulation machine to access that network for whatever reason and now a bad actor may have a way in. An internal bad actor could use the printer hooked to the public to hide use of other printers. The risks and possibilities of election irregularities are limitless with such lax practice of security protocols. In this light, during the investigation it was brought to my attention that mobile devices such as phones were being used in the tabulation area and several times USB sticks were used.

Here is an example, please see 5:29 https://netconcepts.syncedtool.com/shares/file/sXRYTpFsjI9/

It does not appear that encryption keys or passwords were required when inserted and taken out of machines. It is possible that the USB storage devices never leave the tabulation center so on their own not a risk, but given the distance afforded the auditors any stick used on a system would not be caught. The "air gapped" idea with USB devices creates a security issue that would otherwise be discouraged. I have also seen a video with a Dominion employee explaining to county officials that a VPN was optional!

NIST Special Publication 800-124 Revision 1 / Guidelines for Managing the Security of Mobile Devices in the Enterprise page 8 (https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-124r1.pdf)

1. ***General policy**. The centralized technology can enforce enterprise security policies on the mobile device, including (but not limited to) other policy items listed throughout Section 3.2. General policy restrictions of particular interest for mobile device security include the following:*

   a. ***Restrict user and application access to hardware, such as the digital camera, GPS, Bluetooth interface, USB interface, and removable storage.***

   b. *Restrict user and application access to native OS services, such as the built-in web browser, email client, calendaring, contacts, application installation services, etc.*

   c. ***Manage wireless network interfaces (Wi-Fi, Bluetooth, etc.)***

   d. ***Automatically monitor, detect, and report when policy violations occur, such as changes from the approved security configuration baseline, and automatically take action when possible and appropriate.***

   e. *Limit or prevent access to enterprise services based on the mobile device's operating system version (including whether the device has been rooted/jailbroken), vendor/brand, model, or mobile device management software client version (if applicable). Note that this information may be spoofable.*

2. ***Data Communication and Storage***

a. ***Strongly encrypt data communications between the mobile device and the organization. This is most often in the form of a VPN,*** *although it can be established through other uses of secure protocols and encryption.*

b. ***Strongly encrypt stored data on both built-in storage and removable media storage.*** *Removable media can also be "bound" to particular devices such that encrypted information can only be decrypted when the removable media is attached to the device, thereby mitigating the risk of offline attacks on the media.*

See also: The Risks of Using Portable Devices by CISA
https://us-cert.cisa.gov/sites/default/files/publications/RisksOfPortableDevices.pdf
Encryption is mentioned multiple times in this article along with strong recommendations on discouraging use.

NIST Special Publication 800-171 Revision 2
3.1.21 Limit use of portable storage devices on external systems. DISCUSSION Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

Auditors should not be installing software, updating, auditing, etc.

3.1.4 SECURITY REQUIREMENT Separate the duties of individuals to reduce the risk of malevolent activity without collusion. DISCUSSION Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span

> *systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.*
>
> **It appears way too easy for a person to walk in and out of camera without entering a code or using a prox card due to the doors left open and hallways exiting the room.** https://netconcepts.syncedtool.com/shares/file/vhvmnEdSh2U/
>
> *3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.*
> *DISCUSSION Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors. Derived Security Requirements*
> *3.10.3 Escort visitors and monitor visitor activity.*
> *DISCUSSION Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.*

This is just a sampling of the issues that can be noted watching the captured videos. Obviously, many issues would need to be investigated to understand context and possible explanations that are plausible. It appears that many security procedures are not followed as outlined in NIST or by CISA. I believe the “air gapped” system combined with an overly complicated system create an issue that is hard to manage securely. I have now watched several people use wireless devices in the ballot tabulation room. It is clear to me that there are no wireless blocks in place.

I drove to the MCTEC and arrived around 10:40pm and met with Ryan Hartwig. Staying on public property, I scanned the public wifi and assessed the vulnerabilities on the public Wi-Fi. I did NOT attempt to hack into or penetrate the hidden networks whatsoever. I simply connected to MCPublic since it was an open network.

I was able to see an Apple TV, Xbox, and Nintendo Switch on the public county Wi-Fi Network. At our location, there were no other buildings nearby except the election center, and there was an empty lot to our southwest and an electrical substation to our southeast.

In my discovery scan I found a 3Com SuperStack 3 Switch device on the network, which is an outdated piece of equipment from 2014, very vulnerable to manipulation by cyber-attacks because of EOL (end of life). If it is managed internally that could also be a risk.

I did a Google search for a CVE and found the listed as vulnerable to DoS attacks (Denial of Service). Port 80 and 443 were open, but not tested due to that would require authorization. Other observations included:

1. There are a large number of wireless networks. A corporate network should not be “Netgearxx”. There were two “Mcxx” networks (Maricopa County).
2. Who created the “fuckyou” SSIDI Wi-Fi network name?
3. Who would control APs (Access Points) during an audit? Is that network still up? Who would create a network like that in a county building or business?
4. The issue of the old equipment from 2014 (3Com superstack)
5. Why would gaming systems be connected to a network at a tabulation center? It is likely the networks are on HP equipment (3com being acquired by HP). Why are Foreign (other manufacturers) APs (access points) allowed to be installed?
6. Consumer Routers are notorious for having vulnerabilities. Consumer routers appear to be in use along with “main” network. Old un-patched wireless access points are vulnerable. Corporate wireless products can suffer the same issues. https://routersecurity.org/bugs.php
7. I very confident they are not just using the HP equipment. I am fairly certain those other wireless networks were coming from the tabulation center.
8. All networks were encrypted aside from guest and one hidden. It is not likely tabulation machines on those networks. Getting into those networks would not be legal. Network accessed was public and open for anyone and everyone. Network isolation not configured. Point is, are there wireless networks? YES
9. There was a printer connected to the public Wi-Fi.

Aaron Wagner

2-7-2021

NMAP Scan:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-05 22:40 US Mountain Standard Time

NSE: Loaded 153 scripts for scanning.
```

```
NSE: Script Pre-scanning.

Initiating NSE at 22:40

Completed NSE at 22:40, 0.00s elapsed

Initiating NSE at 22:40

Completed NSE at 22:40, 0.00s elapsed

Initiating NSE at 22:40

Completed NSE at 22:40, 0.00s elapsed

Initiating ARP Ping Scan at 22:40

Scanning 256 hosts [1 port/host]

Completed ARP Ping Scan at 22:40, 2.32s elapsed (256 total hosts)

Initiating Parallel DNS resolution of 13 hosts. at 22:40

Nmap scan report for 10.3.160.25 [host down]

 at 22:40, 5.53s elapsed




Initiating SYN Stealth Scan at 22:40

Scanning 13 hosts [1000 ports/host]

Discovered open port 80/tcp on 10.3.160.165

Discovered open port 80/tcp on 10.3.160.130

Discovered open port 443/tcp on 10.3.160.130

Discovered open port 16113/tcp on 10.3.160.5

Increasing send delay for 10.3.160.130 from 0 to 5 due to 11 out of 11 dropped probes since last increase.

SYN Stealth Scan Timing: About 26.79% done; ETC: 22:42 (0:01:25 remaining)

Increasing send delay for 10.3.160.130 from 5 to 10 due to 11 out of 24 dropped probes since last increase.
```

```
Completed SYN Stealth Scan against 10.3.160.1 in 60.38s (12 hosts left)
Completed SYN Stealth Scan against 10.3.160.165 in 60.67s (11 hosts left)
Completed SYN Stealth Scan against 10.3.160.115 in 64.94s (10 hosts left)
Completed SYN Stealth Scan against 10.3.160.11 in 65.05s (9 hosts left)
Completed SYN Stealth Scan against 10.3.160.43 in 65.05s (8 hosts left)
Completed SYN Stealth Scan against 10.3.160.106 in 65.05s (7 hosts left)
Completed SYN Stealth Scan against 10.3.160.13 in 65.48s (6 hosts left)
Completed SYN Stealth Scan against 10.3.160.45 in 65.48s (5 hosts left)
Completed SYN Stealth Scan against 10.3.160.14 in 65.70s (4 hosts left)
Completed SYN Stealth Scan against 10.3.160.5 in 65.80s (3 hosts left)
Completed SYN Stealth Scan against 10.3.160.26 in 65.80s (2 hosts left)
Completed SYN Stealth Scan against 10.3.160.83 in 65.81s (1 host left)
Completed SYN Stealth Scan at 22:42, 136.71s elapsed (13000 total ports)
Initiating Service scan at 22:42
Scanning 4 services on 13 hosts
Completed Service scan at 22:42, 12.63s elapsed (4 services on 13 hosts)
Initiating OS detection (try #1) against 13 hosts
Retrying OS detection (try #2) against 12 hosts
WARNING: OS didn't match until try #2
NSE: Script scanning 13 hosts.
Initiating NSE at 22:43
Completed NSE at 22:44, 5.13s elapsed
Initiating NSE at 22:44
Completed NSE at 22:44, 0.15s elapsed
Initiating NSE at 22:44
Completed NSE at 22:44, 0.00s elapsed
```

```
Nmap scan report for 10.3.160.1

Host is up (0.0040s latency).


All 1000 scanned ports on 10.3.160.1 are filtered


MAC Address: 34:E5:EC:F6:B6:10 (Palo Alto Networks)


Too many fingerprints match this host to give specific OS details


Network Distance: 1 hop




TRACEROUTE


HOP RTT     ADDRESS


1   4.00 ms 10.3.160.1




Nmap scan report for 10.3.160.5


Host is up (0.016s latency).


Not shown: 997 filtered ports
```

```
PORT      STATE  SERVICE    VERSION

3128/tcp  closed squid-http

8080/tcp  closed http-proxy

16113/tcp open   tcpwrapped
MAC Address: C4:F7:D5:E4:D6:0B (Cisco Systems)
Device type: printer|WAP|specialized
Running (JUST GUESSING): HP embedded (87%), Netgear embedded (87%), Crestron 2-Series (86%)
OS CPE: cpe:/h:netgear:wgr614v7 cpe:/o:crestron:2_series
Aggressive OS guesses: HP PSC 2400-series Photosmart printer (87%), Netgear WGR614v7 wireless broadband router (87%), Crestron XPanel control system (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop


TRACEROUTE
HOP RTT      ADDRESS
1   16.49 ms 10.3.160.5


Nmap scan report for 10.3.160.11
Host is up (0.0030s latency).
All 1000 scanned ports on 10.3.160.11 are filtered
```

```
MAC Address: 08:A6:BC:15:CE:98 (Amazon Technologies)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop



TRACEROUTE

HOP RTT     ADDRESS


1   3.00 ms 10.3.160.11



Nmap scan report for 10.3.160.13

Host is up (0.0040s latency).

All 1000 scanned ports on 10.3.160.13 are filtered

MAC Address: 18:B4:30:DF:D1:82 (Nest Labs)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop



TRACEROUTE


HOP RTT     ADDRESS
```

```
1   4.00 ms 10.3.160.13


Nmap scan report for 10.3.160.14

Host is up (0.0040s latency).

All 1000 scanned ports on 10.3.160.14 are filtered
MAC Address: 18:B4:30:E3:F0:1F (Nest Labs)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop


TRACEROUTE
HOP RTT     ADDRESS
1   4.00 ms 10.3.160.14



Nmap scan report for 10.3.160.26
Host is up (0.0030s latency).
All 1000 scanned ports on 10.3.160.26 are filtered
MAC Address: A0:6A:44:C6:C9:B3 (Vizio)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE

HOP RTT     ADDRESS

1   3.00 ms 10.3.160.26



Nmap scan report for 10.3.160.43

Host is up (0.0030s latency).

All 1000 scanned ports on 10.3.160.43 are filtered


MAC Address: AC:2B:6E:2D:C5:49 (Intel Corporate)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop



TRACEROUTE


HOP RTT     ADDRESS

1   3.00 ms 10.3.160.43



Nmap scan report for 10.3.160.45

Host is up (0.0030s latency).

All 1000 scanned ports on 10.3.160.45 are filtered

MAC Address: 34:F1:50:2F:AD:44 (Hui Zhou Gaoshengda Technology)

Too many fingerprints match this host to give specific OS details
```

```
Network Distance: 1 hop


TRACEROUTE

HOP RTT     ADDRESS

1   3.00 ms 10.3.160.45



Nmap scan report for 10.3.160.83

Host is up (0.0040s latency).

All 1000 scanned ports on 10.3.160.83 are filtered

MAC Address: 9C:30:5B:D7:C0:A9 (Hon Hai Precision Ind.)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop


TRACEROUTE
```

```
HOP RTT     ADDRESS

1   4.00 ms 10.3.160.83



Nmap scan report for 10.3.160.106

Host is up (0.0030s latency).

All 1000 scanned ports on 10.3.160.106 are filtered

MAC Address: 4C:36:4E:0A:22:2B (Panasonic  Connected Solutions Company)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop



TRACEROUTE

HOP RTT     ADDRESS

1   3.00 ms 10.3.160.106
```

```
Nmap scan report for 10.3.160.115

Host is up (0.0030s latency).

All 1000 scanned ports on 10.3.160.115 are filtered

MAC Address: D2:72:92:A6:2A:B3 (Unknown)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop


TRACEROUTE


HOP RTT     ADDRESS


1   3.00 ms 10.3.160.115




Nmap scan report for 10.3.160.130


Host is up (0.32s latency).


Not shown: 998 filtered ports


PORT    STATE SERVICE VERSION
```

```
80/tcp  open  http

| fingerprint-strings:

|   FourOhFourRequest:

|     HTTP/1.1 200 OK

|     Location: https://dt3-03310-0bzwc1-
dmz.maricopa.gov/fs/customwebauth/login_pass.html?switch_url=https://dt3-03310-0bzwc1-
dmz.maricopa.gov/login.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPu
blic&redirect=/nice%20ports%2C/Tri%6Eity.txt%2ebak

|     Content-Type: text/html

|     Content-Length: 505

|_    <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="no-cache"><META http-equiv="Expires"
content="-1"><META http-equiv="refresh" content="1; URL=https://dt3-03310-0bzwc1-
dmz.maricopa.gov/fs/customwebauth/login_pass.html?switch_url=https://dt3-03310-0bzwc1-
dmz.maricopa.gov/login.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPu
blic&redirect=/nice%20ports%2C/Tri%6Eity.txt%2ebak"></HEAD></HTML>

443/tcp open  https

| fingerprint-strings:

|   FourOhFourRequest:
```

```
|    HTTP/1.1 200 OK

|    Location: https://dt3-03310-0bzwc1-dmz.maricopa.gov/fs/customwebauth/login_pass.html?switch_url=https://dt3-03310-0bzwc1-dmz.maricopa.gov/login.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/nice%20ports%2C/Tri%6Eity.txt%2ebak

|    Content-Type: text/html

|    Content-Length: 505

|    <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma" content="no-cache"><META http-equiv="Expires" content="-1"><META http-equiv="refresh" content="1; URL=https://dt3-03310-0bzwc1-dmz.maricopa.gov/fs/customwebauth/login_pass.html?switch_url=https://dt3-03310-0bzwc1-dmz.maricopa.gov/login.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/nice%20ports%2C/Tri%6Eity.txt%2ebak"></HEAD></HTML>

|   GetRequest:

|    HTTP/1.1 200 OK

|    Location: https://dt3-03310-0bzwc1-dmz.maricopa.gov/fs/customwebauth/login_pass.html?switch_url=https://dt3-03310-0bzwc1-dmz.maricopa.gov/login.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/

|    Content-Type: text/html
|     Content-Length: 470

|_    <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma" content="no-cache"><META http-equiv="Expires" content="-1"><META http-equiv="refresh" content="1; URL=https://dt3-03310-0bzwc1-dmz.maricopa.gov/fs/customwebauth/login_pass.html?switch_url=https://dt3-03310-0bzwc1-dmz.maricopa.gov/login.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/"></HEAD></HTML>

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-Port80-TCP:V=7.91%I=7%D=2/5%Time=601E2C51%P=i686-pc-windows-windows%r(F

SF:ourOhFourRequest,342,"HTTP/1\.1\x20200\x20OK\r\nLocation:\x20https://dt

SF:3-03310-0bzwc1-dmz\.maricopa\.gov/fs/customwebauth/login_pass\.html\?sw

SF:itch_url=https://dt3-03310-0bzwc1-dmz\.maricopa\.gov/login\.html&ap_mac

SF:=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=

SF:/nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\nContent-Type:\x20text/html\r\n

SF:Content-Length:\x20505\r\n\r\n<HTML><HEAD><TITLE>\x20Web\x20Authenticat
```

```
SF:ion\x20Redirect</TITLE><META\x20http-equiv=\"Cache-control\"\x20content
SF:=\"no-cache\"><META\x20http-equiv=\"Pragma\"\x20content=\"no-cache\"><M
SF:ETA\x20http-equiv=\"Expires\"\x20content=\"-1\"><META\x20http-equiv=\"r
SF:efresh\"\x20content=\"1;\x20URL=https://dt3-03310-0bzwc1-dmz\.maricopa\
SF:.gov/fs/customwebauth/login_pass\.html\?switch_url=https://dt3-03310-0b
SF:zwc1-dmz\.maricopa\.gov/login\.html&ap_mac=d8:b1:90:aa:54:d0&client_mac
SF:=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/nice%20ports%2C/Tri%6Eity\.t
SF:xt%2ebak\"></HEAD></HTML>\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.91%I=7%D=2/5%Time=601E2C51%P=i686-pc-windows-windows%r(
SF:GetRequest,2FC,"HTTP/1\.1\x20200\x20OK\r\nLocation:\x20https://dt3-0331
SF:0-0bzwc1-dmz\.maricopa\.gov/fs/customwebauth/login_pass\.html\?switch_u
SF:rl=https://dt3-03310-0bzwc1-dmz\.maricopa\.gov/login\.html&ap_mac=d8:b1
```

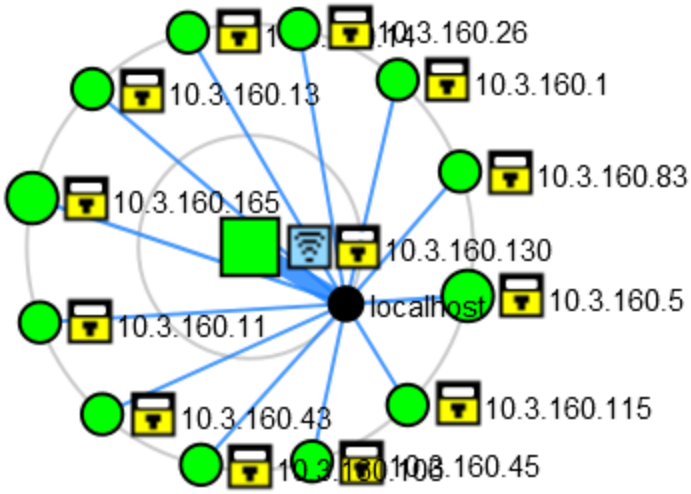
```
SF::90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/\r\nC

SF:ontent-Type:\x20text/html\r\nContent-Length:\x20470\r\n\r\n<HTML><HEAD>

SF:<TITLE>\x20Web\x20Authentication\x20Redirect</TITLE><META\x20http-equiv

SF:=\"Cache-control\"\x20content=\"no-cache\"><META\x20http-equiv=\"Pragma

SF:\"\x20content=\"no-cache\"><META\x20http-equiv=\"Expires\"\x20content=\

SF:"-1\"><META\x20http-equiv=\"refresh\"\x20content=\"1;\x20URL=https://dt

SF:3-03310-0bzwc1-dmz\.maricopa\.gov/fs/customwebauth/login_pass\.html\?sw

SF:itch_url=https://dt3-03310-0bzwc1-dmz\.maricopa\.gov/login\.html&ap_mac

SF:=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=

SF:/\"></HEAD></HTML>\r\n")%r(FourOhFourRequest,342,"HTTP/1\.1\x20200\x20O

SF:K\r\nLocation:\x20https://dt3-03310-0bzwc1-dmz\.maricopa\.gov/fs/custom

SF:webauth/login_pass\.html\?switch_url=https://dt3-03310-0bzwc1-dmz\.mari

SF:copa\.gov/login\.html&ap_mac=d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:f
```

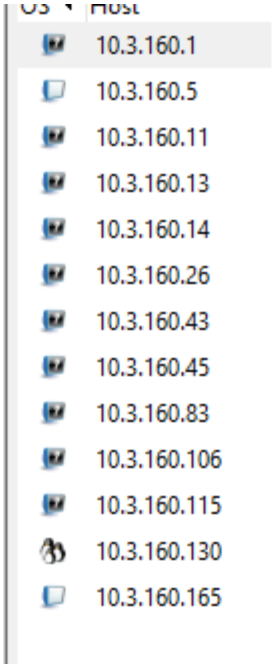
```
SF:d:18&wlan=MCPublic&redirect=/nice%20ports%2C/Tri%6Eity\.txt%2ebak\r\nCo
SF:ntent-Type:\x20text/html\r\nContent-Length:\x20505\r\n\r\n<HTML><HEAD><
SF:TITLE>\x20Web\x20Authentication\x20Redirect</TITLE><META\x20http-equiv=
SF:\"Cache-control\"\x20content=\"no-cache\"><META\x20http-equiv=\"Pragma\
SF:"\x20content=\"no-cache\"><META\x20http-equiv=\"Expires\"\x20content=\"
SF:-1\"><META\x20http-equiv=\"refresh\"\x20content=\"1;\x20URL=https://dt3
SF:-03310-0bzwc1-dmz\.maricopa\.gov/fs/customwebauth/login_pass\.html\?swi
SF:tch_url=https://dt3-03310-0bzwc1-dmz\.maricopa\.gov/login\.html&ap_mac=
SF:d8:b1:90:aa:54:d0&client_mac=7c:a7:b0:bb:fd:18&wlan=MCPublic&redirect=/
SF:nice%20ports%2C/Tri%6Eity\.txt%2ebak\"></HEAD></HTML>\r\n");
MAC Address: 50:13:95:60:1A:D2 (SichuanAI-LinkTechnologyCo.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
```

```
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
Network Distance: 1 hop

TRACEROUTE
HOP RTT       ADDRESS
1   320.14 ms 10.3.160.130

Nmap scan report for 10.3.160.165
Host is up (0.013s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE    VERSION
```

```
80/tcp open  tcpwrapped
MAC Address: B4:B6:86:AB:5C:1D (Hewlett Packard)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: media device|specialized
Running: Crestron embedded, Wago Kontakttechnik embedded
OS CPE: cpe:/h:crestron:mpc-m5 cpe:/h:wago_kontakttechnik:750-852
OS details: Crestron MPC-M5 AV controller or Wago Kontakttechnik 750-852 PLC
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   13.38 ms 10.3.160.165
```

```
NSE: Script Post-scanning.

Initiating NSE at 22:44

Completed NSE at 22:44, 0.00s elapsed

Initiating NSE at 22:44

Completed NSE at 22:44, 0.00s elapsed

Initiating NSE at 22:44

Completed NSE at 22:44, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (13 hosts up) scanned in 239.81 seconds
```





OS	Host
	10.3.160.1
	10.3.160.5
	10.3.160.11
	10.3.160.13
	10.3.160.14
	10.3.160.26
	10.3.160.43
	10.3.160.45
	10.3.160.83
	10.3.160.106
	10.3.160.115
	10.3.160.130
	10.3.160.165