Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller

July 31, 2020

Federal Energy Regulatory Commission

North American Electric Reliability Corporation

The opinions and views expressed in this staff White Paper do not necessarily represent those of the Federal Energy Regulatory Commission, its Chairman, or individual Commissioners, and are not binding on the Commission. Similarly, the opinions and views expressed herein do not necessarily represent those of the NERC Board of Trustees, its chair, or any individual trustee, and are not binding on them.

Table of Contents

Executive Summary

In 2012, the House Permanent Select Committee on Intelligence released a bipartisan report assessing the security threat posed by Chinese telecommunication companies. This report recommended against the use of Huawei or ZTE equipment by U.S. government agencies and federal contractors and encouraged the private sector to exclude such equipment as well.[1]

Due to the pervasiveness of these manufacturers throughout the marketplace, the electric sector may unknowingly be using devices from foreign adversaries that could negatively impact the Bulk Power System (BPS). To facilitate the identification of these devices, this report details possible techniques that noninvasively identify one component, the network interface controller (NIC). A NIC generally takes the form of an integrated circuit chip (IC) integrated into a motherboard or upon a host bus adapter card. Research has demonstrated numerous avenues to compromise systems using NICs as a method for undetected access for an attacker. While the techniques described in this report will aid in identifying the NIC vendor, please note that the presence of foreign vendor equipment does not necessarily indicate malicious activity.

This report identifies the noninvasive techniques that security professionals may employ to identify a vendor of a NIC. This approach selects the NIC as a well-known and often-targeted component, and contemplates methods for easy identification of devices often not readily labeled by suspect vendors or that may integrate suspect vendor components. The techniques described are not the only methods of detection nor do they encompass the only concerns industry should have about malicious activity and attacks.

The "Additional Techniques and Considerations" provide high-level examples for other areas a cyber-security professional may consider. Before implementing any approach detailed here, caution dictates complete testing in a non-production network to minimize or eliminate operational impacts. If a vendor of concern is identified, it does not confirm there is malicious activity in the network. Actions should be taken to determine if the device or component exhibits malicious activity.

Purpose

The purpose of this document is to provide example approaches on assessing infrastructure and the deployment of foreign adversary components that could be used to impact the BPS. While there are several noninvasive methods highlighted in the document, industry may have other methods to identify foreign vendor equipment or

[1] Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (Oct. 8, 2012), https://fas.org/irp/congress/2012_rpt/huawei.pdf

components. In addition, industry should consider developing and implementing a process to not only initially identify vendor suppliers, but also to implement an overarching process that could be periodically re-performed and assessed against previous results.

Background – Supply Chain and Huawei and ZTE

Concerns regarding Huawei and ZTE equipment and services used in several sectors and industries have grown over the past decade. The October 2012, House Permanent Select Committee on Intelligence bipartisan report concluded that U.S. government agencies and federal contractors should "exclude ZTE or Huawei equipment in their systems," and "strongly encouraged" private-sector entities "to consider the long-term security risks associated with doing business with either Huawei or ZTE for equipment or services" and "to seek out other vendors for their projects."[2]

In 2013, the Government Accountability Office (GAO) assessed the potential security risks of foreign-manufactured equipment in commercial communications networks and detailed U.S. government efforts to address the risks posed by such equipment.[3] The GAO report found that "[a] potential enemy or criminal group has a number of ways to potentially exploit vulnerabilities in the communications equipment supply chain, such as placing malicious code in the components that could compromise the security and resilience of the networks."[4]

A report by the Defense Innovation Board titled "The 5G Ecosystem: Risks and Opportunities for DoD" highlights the threats posed by China and other nation-state adversaries.[5] The report notes that "evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally" and that many of those vulnerabilities "seem to be related to requirements from the Chinese intelligence community pressuring companies to exfiltrate information."[6] The report also highlights the need for the Department of Defense to "consider options for defending against a compromised supply chain, where Chinese semiconductor components and chipsets are embedded across multiple systems."[7]

[2] Id. at vi, 45.

[3] GAO, Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment (May 21, 2013), https://www.gao.gov/assets/660/654763.pdf.

[4] *Id.* at 3.

[5] https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[6] *Id.* at 25.

[7] *Id.* at 29.

The National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA), among other provisions, bars the Department of Defense from using "telecommunications equipment [or] services produced [or] provided by Huawei Technologies Company or ZTE Corporation" for certain critical programs, including ballistic missile defense and nuclear command, control, and communications.[8]

Example: The Electric Sector Supply Chain Compromise

The electric sector uses networking and telecommunications equipment to operate the Bulk Power System. Many manufacturers of this type of equipment currently exist, but Huawei, ZTE, and their subsidiaries have recently gained the largest market share of networking vendors globally.[9] A portion of this market share dominance stems from embedded Huawei or ZTE components in equipment produced by otherwise unrelated vendors. As such, the probability that electric utilities now use a significant amount of telecommunications equipment with either equipment or components from Huawei or ZTE is high, especially when also factoring in components through subsidiaries branded under a different vendor's label. If these obscurely-labeled (or even unlabeled) components exist in an electric utility's infrastructure, the same risks exist as if the hardware bore the logo of Huawei, ZTE, or one of their well-known subsidiaries.

> Example: An electric utility purchased a network-connected video monitoring system using the *IPv4 TCP/IP protocol* from the vendor ACME.[10] Because most manufacturers integrate parts from many other vendors, the possibility exists that the new video system uses potentially compromised components. By only looking at the label of the video system, the customer may not fully comprehend the source of all internal components. Furthermore, the customer may never know the sources unless the buyer specifically requires the vendor, ACME, to provide details of the purchased internal components. This example illustrates how the installed base of components that are potentially compromised might increase. The complexity of telecommunications products often obfuscates the inclusion of compromised components inside a chassis bearing another vendor's logo.

Unaffiliated vendors integrating or installing compromised components produce the same security risk for the customer as if directly purchased from the manufacturer of the compromised component. The unaffiliated vendor remains unaware of the vulnerability,

[8] National Defense Authorization Act for Fiscal Year 2018, Public Law No. 115–91, § 1656, 131 Stat. 1283 (2017).

[9] Huawei - Statistics & Facts, Statista Research Department, Jul 15, 2019, https://www.statista.com/topics/2305/huawei/

[10] ACME is a fictitious company for the purpose of explanation and is not affiliated with Huawei, ZTE, or any of their subsidiaries.

such as the case with the ACME example above. Since customers can bring compromised components into their network unwittingly, due care must be observed to perform a comprehensive inventory. Accordingly, this non-invasive NIC identification approach serves as an excellent “first-look” method.

Why attack via a Network Interface Controller (NIC)?

Vendors have purposefully created their products or rebranded hardware[11] with backdoors in the past. Many such instances may simply occur while attempting innocently to foster customer service or, not so innocently, to control intellectual property.[12] Vendors may tacitly decide the possible rewards of controlling the customer’s system and intellectual property outweigh the risk of detection and damage to their corporate reputation. Such control could even extend to leveraging malicious access in the pursuit of monetary gain or purposeful misuse for the destruction of customer assets. Regardless of intention, these surreptitious techniques create a great risk of exploitation or misuse and are extremely difficult to discover.

Backdoors serve as gateways for malicious actors to install a wide range of control automation software, rootkits, and tools. These tools not only can command and exfiltrate data from compromised systems, but attackers may also load tools to exploit any vulnerabilities which exist on neighboring hosts. In the presumption that a motivated attacker will utilize any means available, the industry must assume the installation of additional malicious software via all suspect components. As each additional attack vector naturally improves the attacker’s probability of success, more backdoors installed equate to more opportunities to go around a firewall or some other security control to grant inappropriate access to a protected network.

Attackers often employ detection avoidance and malware persistence to improve their chances of success. Detection avoidance means that the component compromised will attempt to hide evidence of the attack and subsequent malicious use. Persistence means the compromised device could remain in service for months to years; therefore, the attacker may have the ability to access the compromised system undetected and perform malicious actions as well. Utilizing common manufacturer components as an attack platform ensures thousands (if not millions) of potential targets. Each compromised device provides an opportunity for a cyber-security control to identify the compromise

[11] Backdoor Found in Lenovo, IBM Switches, Security Week, Eduard Kovacs, January 15, 2018, https://www.securityweek.com/backdoor-found-lenovo-ibm-switches.
[12] Sony BMG Rootkit Scandal: 10 Years Later, Network World, Bob Brown, October 28, 2015, https://www.networkworld.com/article/2998251/sony-bmg-rootkit-scandal-10-years-later.html

and report the discovery to the security community. Selecting the best software or device to compromise becomes a key decision.

A compromised NIC makes a good choice for an attacker "because of its *low-level position* in a computer system, [as] the backdoor is capable of bypassing virtually all commodity *firewall* and *host-based intrusion detection* software."[13] The NIC enables network communications making it nearly ubiquitous. Often the integrator or reseller will use the manufacturer's "reference" NIC driver software without making any changes, thereby increasing the potential to grant access to a malicious actor.

Techniques to Identify NIC Manufacturers[14]

It is important to identify the vendors of components to properly assess risk. The previous sections discussed vendors identified by the U.S. Government with potentially malicious intent. Also discussed were components that are a good selection to compromise with a backdoor. Security professionals thereby possess enough information for a survey plan to discover any of the devices or components existing within their infrastructure. If purchased directly from the manufacturer, the customer should be able to identify the device or component by the labeling. Challenges arise, however, if the device is labeled by a different vendor or integrator. The less-familiar markings or logo may allow such a NIC to escape the customer's notice.

There are several methods for identifying components. One approach involves physically opening the device to inspect for known part numbers from manufacturers and comparing those to a list of potentially malicious components. Such a process would be extremely invasive, likely to void warranties and consume large amounts of time. The physical inspection may furthermore be operationally infeasible since it requires removing the device from production.

Another approach involves automated tools. Fortunately, automated tools already in use by industry may be useful to identify suspect components. System administrators and security professionals routinely use these tools to scan networks for items such as system and network operating health issues, vulnerabilities, missing patches, and malicious activity. The identification methodology put forth by this document will focus specifically on the identification of NIC vendors using information from the *Media Access Control (MAC)* address.

[13] A Chipset Level Network Backdoor: Bypassing Host-Based Firewall & IDS, Sherri Sparks, Shawn Embleton, Cliff C. Zou, 2008, http://www.cs.ucf.edu/~czou/research/Chipset%20Backdoor-AsiaCCS09.pdf.

[14] Any of the suggested techniques should be validated and tested by an IT, OT, and/or cyber security professional to ensure there is no operational impact to the operational environment.

A MAC address is comprised of six (6) numbers, known as hexadecimal octets (e.g., FF:FF:FF:00:00:00). Generally, the first half, FF:FF:FF in this instance identifies the vendor through the IEEE Standards Registration Authority (RA). The IEEE RA refers to these vendor numbers as Organizationally Unique Identifiers (OUI) and ensures that no two vendors use the same numbers.[15] Every device manufactured by that vendor must use the OUI number(s) assigned to them.[16] Numerous organizations provide a web-interface to assist in the identification of vendors. The official IEEE database is provided at http://standards-oui.ieee.org/oui.txt.

The remaining half of three (3) octets of a MAC address, the network ID, works somewhat like a serial number. The manufacturer strives to ensure the uniqueness of this portion of the address, since if two NICs attempt to communicate with the same address on the same network, neither will function reliably.

Ideally, if each manufacturer uses their correct OUI and carefully assigns a unique "serial" number, no two MAC addresses should ever match. Even if two manufacturers happen to use the same network identifier octets, then OUI should still be different.

> Example: *FC:E3:3C*:5B:BA:92 (Huawei Tech Co Ltd) is a MAC address for a Huawei NIC. The first three (3) octets *FC:E3:3C* identify Huawei, and the last three octets, 5B:BA:92, are a unique number identifying the NIC on the network.

This approach performs common passive scanning techniques to identify the NIC MAC address and, specifically, the associated OUI. Passive scanning reduces the risk of communication interruption within an operational network and possibly impacting BES reliability.

While the four techniques and tools described below are designed to be noninvasive, entities are encouraged to consider use at their own risk, as there may be a negative impact on their network or environment.

Technique 1 – NMAP Passive ARP Scan

[15] IEEE RA Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID), IEEE Standards Registration Authority, https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf

[16] Approximately 39,000 OUIs exist as of March, 2020, Gitlab – OUI list, March 2020, https://gitlab.com/wireshark/wireshark/raw/master/manuf

Nmap (“Network Mapper”) is an open-source tool for network exploration and security auditing.[17] With the proper parameters, Nmap can scan a *local network* to identify all the devices, their associated MAC addresses, and OUIs.

> *Please Note: This approach does not use port scanning on the Network Layer (Layer 3 – TCP/IP/UDP). Layer 3 Port interrogation against production networks may yield deleterious results to systems. The command-line parameters (switches) are used to restrict the tool to the Data Link Layer (Layer 2) for MAC address harvesting only.*
>
> *Nmap is a very powerful tool and can adversely impact production systems. SMEs who are familiar with its capabilities should be consulted prior to use on production systems.*

All hosts connected via Ethernet rely on MAC addresses to transfer messages (data frames) to other nodes within the subnet. In addition, since all connected nodes send and receive reflexively as an innate requirement of the defined standards of Ethernet,[18] an Nmap scan makes ARP requests to discover all the devices on the local network. Using these types of scans should provide a reliable listing of all connected devices.

Once complete, the scan output associates the node’s IP address with its MAC address. Nmap then attempts to determine the assigned manufacturer from an internal list of OUIs. For best results, users should update the file called “nmap-mac-prefixes” to the most current version available. This example scan used an updated file with the OUI list from Wireshark, which has approximately 39,000 entries, compared to Nmap’s 27,000.[19]

```
C:\Users\HP-84>nmap -sn -PR 192.168.101.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-16 12:39 Eastern Standard Time
Nmap scan report for 192.168.101.1
MAC Address: 2C:30:33:FF:FF:FF (Netgear)
Nmap scan report for 192.168.101.2
MAC Address: BC:DD:C2:FF:FF:FF (Espressif Inc)
Nmap scan report for 192.168.101.4
MAC Address: BC:DD:C2:FF:FF:FF (Espressif Inc)
Nmap scan report for 192.168.101.5
MAC Address: B0:2A:43:FF:FF:FF (Google  Inc)
Nmap scan report for 192.168.101.6
MAC Address: EC:FA:BC:FF:FF:FF (Espressif Inc)
Nmap scan report for 192.168.101.7
MAC Address: 6C:E8:5C:FF:FF:FF (Apple  Inc)
Nmap scan report for 192.168.101.9
MAC Address: FC:E3:3C:5B:BA:92 (Huawei Tech Co  Ltd)
Nmap scan report for 192.168.101.14
MAC Address: 3C:18:A0:FF:FF:FF (Luxshare Precision Industry Co Ltd)
Nmap scan report for 192.168.101.16
MAC Address: C4:9A:02:FF:FF:FF (LG Electronics (Mobile Communications))
```

[17] Nmap definition, March 2020, https://nmap.org/book/man.html#man-description.

[18] IEEE Standard Authority, 802.3-2018 – IEEE Standard for Ethernet, Standard Details, https://standards.ieee.org/standard/802_3-2018.html

[19] OUI list: The file nmap-mac-prefixes file should be updated with the OUI list from Wireshark, https://gitlab.com/wireshark/wireshark/raw/master/manuf. (There are other vendors with a similar list).

```
Nmap scan report for 192.168.101.17
MAC Address: 30:4B:07:FF:FF:FF (Motorola Mobility Llc  a Lenovo Co)
Nmap scan report for 192.168.101.19
MAC Address: E8:9E:B4:FF:FF:FF (Hon Hai Precision Ind. Co  Ltd)
Nmap scan report for 192.168.101.25
MAC Address: 68:17:29:FF:FF:FF (Intel Corp)
Nmap scan report for 192.168.101.28
MAC Address: 68:DB:F5:FF:FF:FF (Amazon Tech Inc)
Nmap scan report for 192.168.101.33
MAC Address: 8C:AE:4C:FF:FF:FF (Plugable Tech)
Nmap scan report for 192.168.101.38
MAC Address: 00:22:A1:83:08:00 (Huawei Symantec Tech Co  Ltd)
Nmap scan report for 192.168.101.40
MAC Address: 00:08:96:FF:FF:FF (Printronix  Inc)
Nmap scan report for 192.168.101.44
MAC Address: B0:C1:9E:83:08:04 (zte Corp)
Nmap scan report for 192.168.101.45
MAC Address: A4:AD:B8:FF:FF:FF (Vitec Group  Camera Dynamics Ltd)
Nmap scan report for 192.168.101.46
MAC Address: 00:0F:1A:FF:FF:FF (Gaming Support B.V.)
Nmap scan report for 192.168.101.50
MAC Address: B0:70:2D:FF:FF:FF (Apple  Inc)
Nmap scan report for 192.168.101.52
MAC Address: 70:11:24:FF:FF:FF (Apple  Inc)
Nmap scan report for 192.168.101.53
MAC Address: 2C:B0:5D:FF:FF:FF (Netgear)
Nmap scan report for 192.168.101.55
MAC Address: 3C:8B:FE:FF:FF:FF (Samsung Electronics Co  Ltd)
Nmap scan report for 192.168.101.99
MAC Address: 48:F8:B3:FF:FF:FF (Cisco-Linksys  Llc)
Nmap scan report for 192.168.101.8
Host is up.
Nmap done: 256 IP addresses (25 hosts up) scanned in 22.92 seconds
```

Figure 1: NMAP ARP scan

The example utilized the following command:

```
nmap -sn -PR 192.168.101.0/24
```

Using this technique benefits from the fact that it should have minimal impact on an operational network using TCP/IP, as the scan uses commands expected in the normal operations for the local network.[20] As previously discussed, an ARP scan should identify all devices on the local network and list the devices with the IP, MAC address, and the OUI. ARP scans can only be performed in the local network.

`Nmap scan report for 192.168.101.9:` The results of this scan indicated 25 devices were connected in the local network. The IP address for this device is 192.168.101.9 and was identified by the scan.

`MAC Address: FC:E3:3C:5B:BA:92 (Huawei Tech Co Ltd):` The scan provided the MAC address paired with its associated IP address.

[20] While an Nmap ARP scan should have minimal impacts to network operations, users are advised to fully vet this technique in a development or test network.

Technique 2 – List ARP Cache Table

Computing devices typically have an installed command that can list the MAC addresses associated with the IP address in a local network as shown in Figure 2.

```
C:\Users\HP-84>arp -a
Interface: 192.168.101.8 --- 0x7
  Internet Address    Physical Address      Type
  192.168.101.1        2c-30-33-ff-ff-ff     dynamic
  192.168.101.2        bc-dd-c2-ff-ff-ff     dynamic
  192.168.101.4        bc-dd-c2-ff-ff-ff     dynamic
  192.168.101.5        b0-2a-43-ff-ff-ff     dynamic
  192.168.101.6        ec-fa-bc-ff-ff-ff     dynamic
  192.168.101.7        6c-e8-5c-ff-ff-ff     dynamic
  192.168.101.9        fc-e3-3c-5b-ba-92     dynamic
  192.168.101.14       3c-18-a0-ff-ff-ff     dynamic
  192.168.101.16       c4-9a-02-ff-ff-ff     dynamic
  192.168.101.17       30-4b-07-ff-ff-ff     dynamic
  192.168.101.19       e8-9e-b4-ff-ff-ff     dynamic
  192.168.101.25       68-17-29-ff-ff-ff     dynamic
  192.168.101.28       68-db-f5-ff-ff-ff     dynamic
  192.168.101.33       8c-ae-4c-ff-ff-ff     dynamic
  192.168.101.38       00-22-a1-83-08-00     dynamic
  192.168.101.40       00-08-96-ff-ff-ff     dynamic
  192.168.101.44       b0-c1-9e-83-08-04     dynamic
  192.168.101.45       a4-ad-b8-ff-ff-ff     dynamic
  192.168.101.46       00-0f-1a-ff-ff-ff     dynamic
  192.168.101.50       b0-70-2d-ff-ff-ff     dynamic
  192.168.101.52       70-11-24-ff-ff-ff     dynamic
  192.168.101.53       2c-b0-5d-ff-ff-ff     dynamic
  192.168.101.55       3c-8b-fe-ff-ff-ff     dynamic
  192.168.101.99       48-f8-b3-ff-ff-ff     dynamic
  192.168.101.255      ff-ff-ff-ff-ff-ff     static
```

Figure 2: Windows ARP Cache Table

The ARP Command (Figure 2.):

Typing the “arp -a” command, Figure 2., which is standard in the Windows operating system environment, will display the entries that have been cached by the operating system. The cache table may not contain all the entries since it is dynamic and will change over time.[21] However, using this command is an operationally safe option to collect the MAC addresses and compare them to the OUI list to determine if there is a component from a specific vendor.[22]

Devices other than Windows typically have a command similar to the “ARP” command. Switches are good devices to list the ARP cache, and a network administrator should have the ability to retrieve the ARP cache table. Regardless of the device, retrieval of the ARP cache table should not impact the operation of the system since the query is passive and consistent with normal network operations. (Most networking devices have a method to view the ARP cache table, but depending on the device, it may not be fully populated

[21] A network administrator should know what commands populate the ARP cache for the device in the local network.

[22] Staff that manage the networked system can write a script to identify the MAC address using the OUI list.

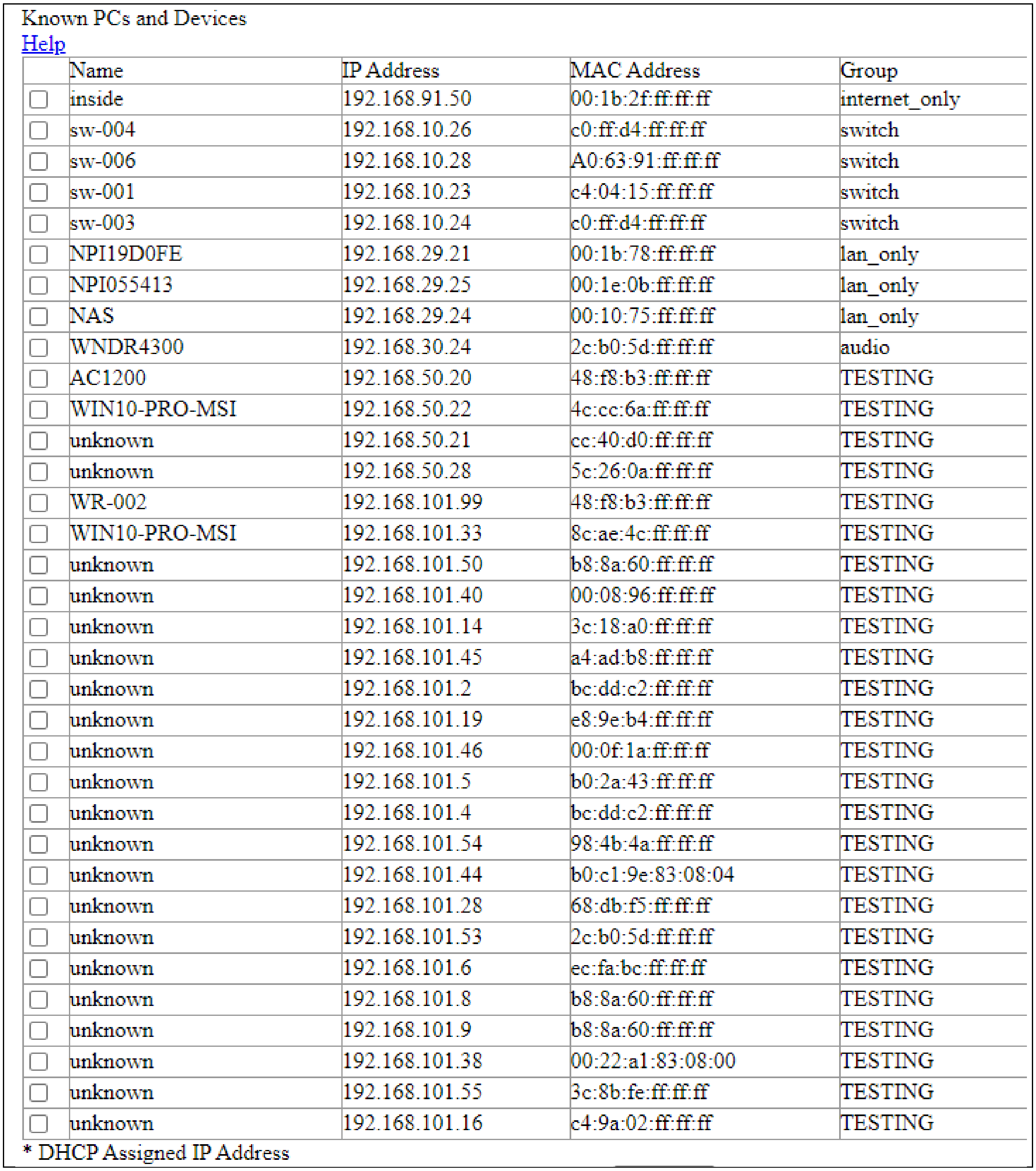
with MAC addresses. The utility's network security professional should have the ability to retrieve the MAC addresses.)

Technique 3 – DHCP Client Table

The Dynamic Host Configuration Protocol (DHCP) is a networking protocol used to assign IP addresses to devices. A DHCP server delivers the assigned IP address in response to client requests. A DHCP server can be a standalone server such as a computer or integrated within the network device. Regardless of the location, the DHCP server will contain a list of devices, the pool of configured IP addresses, and the associated MAC address within the network referred to as a DHCP client table, Figure 3. The OUI list from the Wireshark tool can be used to look up the MAC address vendors listed in the DHCP client table. Retrieving the DHCP client table is a passive technique and is noninvasive; however, it should be noted not all networked systems use a DHCP server and this technique may not always be a reliable option when collecting valid NIC MAC addresses on the network.

Additionally, if a *static IP*[23] is used for a device in the network, the IP may or may not be listed in the DHCP client table. The results will vary based on the DHCP server type and implementation. A network administrator can verify the values, which are stored in a client table. The benefit of using the DHCP client table over the previous techniques described is that the result will be a broader sweep of the IP and MAC addresses. The IP and MAC addresses listed may contain devices from all the local networks if the DHCP server is configured to allocate IP addresses to all the segments. The previous techniques described require the command to be run within each local network. Figure 3. shows a client table for IP and MAC addresses for several local networks that were allocated by the DHCP server, the third set of numbers is the local network address, e.g., 192.168.***10***.x, 192.168.***29***.x, 192.168.***30***.x, 192.168.***50***.x, 192.168.***91***.x, 192.168.***101***.x, and 192.168.***120***.x.

[23] A Static IP is an IP address that is manually entered in a networking device and is not automatically assigned by a DHCP server.



Known PCs and Devices

Help

	Name	IP Address	MAC Address	Group
☐	inside	192.168.91.50	00:1b:2f:ff:ff:ff	internet_only
☐	sw-004	192.168.10.26	c0:ff:d4:ff:ff:ff	switch
☐	sw-006	192.168.10.28	A0:63:91:ff:ff:ff	switch
☐	sw-001	192.168.10.23	c4:04:15:ff:ff:ff	switch
☐	sw-003	192.168.10.24	c0:ff:d4:ff:ff:ff	switch
☐	NPI19D0FE	192.168.29.21	00:1b:78:ff:ff:ff	lan_only
☐	NPI055413	192.168.29.25	00:1e:0b:ff:ff:ff	lan_only
☐	NAS	192.168.29.24	00:10:75:ff:ff:ff	lan_only
☐	WNDR4300	192.168.30.24	2c:b0:5d:ff:ff:ff	audio
☐	AC1200	192.168.50.20	48:f8:b3:ff:ff:ff	TESTING
☐	WIN10-PRO-MSI	192.168.50.22	4c:cc:6a:ff:ff:ff	TESTING
☐	unknown	192.168.50.21	cc:40:d0:ff:ff:ff	TESTING
☐	unknown	192.168.50.28	5c:26:0a:ff:ff:ff	TESTING
☐	WR-002	192.168.101.99	48:f8:b3:ff:ff:ff	TESTING
☐	WIN10-PRO-MSI	192.168.101.33	8c:ae:4c:ff:ff:ff	TESTING
☐	unknown	192.168.101.50	b8:8a:60:ff:ff:ff	TESTING
☐	unknown	192.168.101.40	00:08:96:ff:ff:ff	TESTING
☐	unknown	192.168.101.14	3c:18:a0:ff:ff:ff	TESTING
☐	unknown	192.168.101.45	a4:ad:b8:ff:ff:ff	TESTING
☐	unknown	192.168.101.2	bc:dd:c2:ff:ff:ff	TESTING
☐	unknown	192.168.101.19	e8:9e:b4:ff:ff:ff	TESTING
☐	unknown	192.168.101.46	00:0f:1a:ff:ff:ff	TESTING
☐	unknown	192.168.101.5	b0:2a:43:ff:ff:ff	TESTING
☐	unknown	192.168.101.4	bc:dd:c2:ff:ff:ff	TESTING
☐	unknown	192.168.101.54	98:4b:4a:ff:ff:ff	TESTING
☐	unknown	192.168.101.44	b0:c1:9e:83:08:04	TESTING
☐	unknown	192.168.101.28	68:db:f5:ff:ff:ff	TESTING
☐	unknown	192.168.101.53	2c:b0:5d:ff:ff:ff	TESTING
☐	unknown	192.168.101.6	ec:fa:bc:ff:ff:ff	TESTING
☐	unknown	192.168.101.8	b8:8a:60:ff:ff:ff	TESTING
☐	unknown	192.168.101.9	b8:8a:60:ff:ff:ff	TESTING
☐	unknown	192.168.101.38	00:22:a1:83:08:00	TESTING
☐	unknown	192.168.101.55	3c:8b:fe:ff:ff:ff	TESTING
☐	unknown	192.168.101.16	c4:9a:02:ff:ff:ff	TESTING

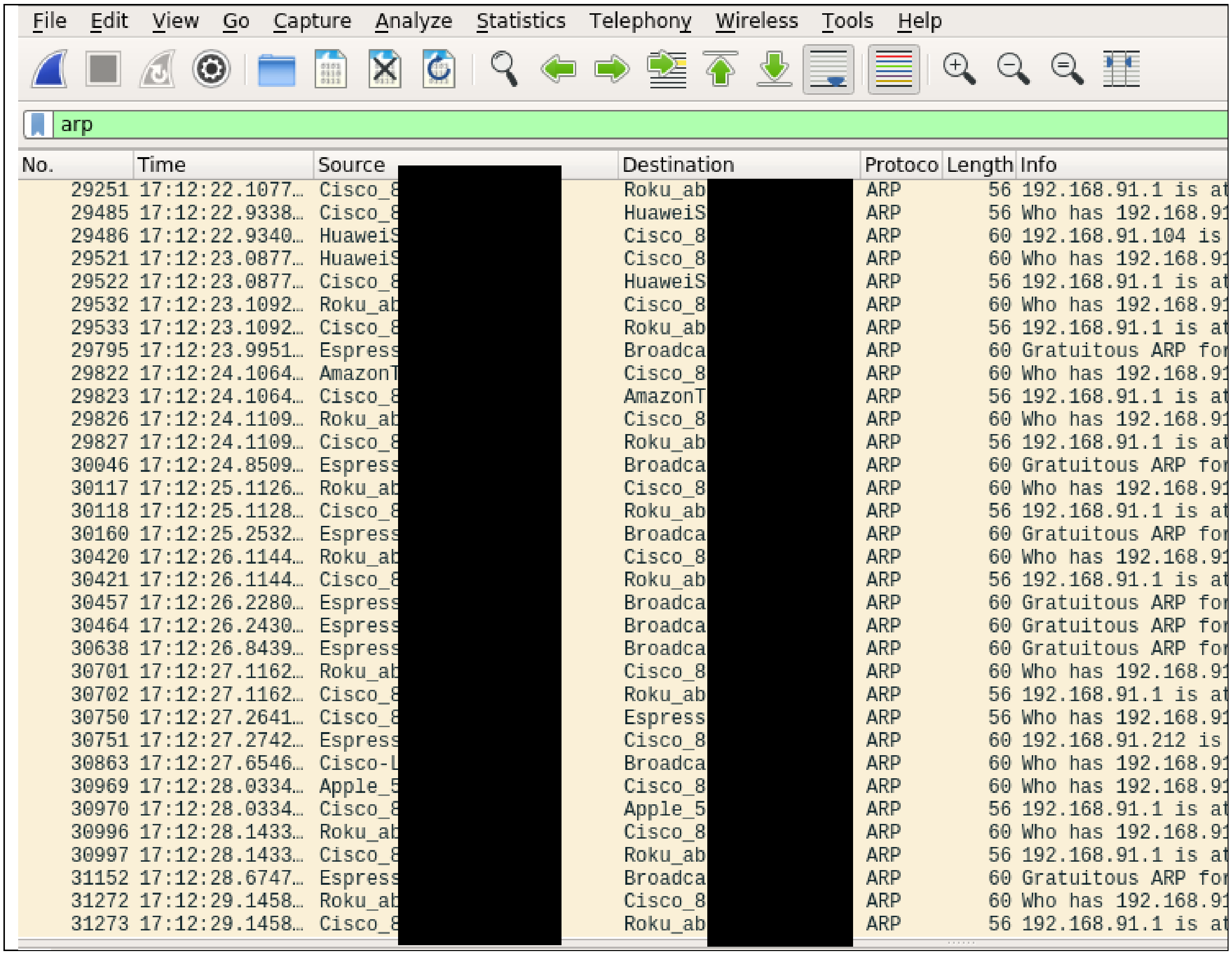
* DHCP Assigned IP Address

Figure 3: Router DHCP List

Technique 4 – Port Mirroring

Network and security professionals routinely use a technique called "port mirroring," [24] which is used to send a copy of network traffic passing through a *switch port(s)*[25] to a *mirrored port* for analysis. It is common practice to use port mirroring to monitor traffic for devices such as an Intrusion Detection System (IDS). Traffic sent to a mirrored port is read-only and used by the monitoring device or software. It should be noted that this monitoring device cannot introduce new traffic into the network. The OUI list from the Wireshark tool can be used to look up the MAC address. Tools like Wireshark may automatically identify the MAC address OUI as the traffic is captured, Figure 4. This passive, noninvasive technique of port mirroring does have limitations because not all of the device traffic may pass through the switch port that is being monitored. Additionally, it will take time to build a list of the devices as the traffic is captured. These conditions can be accounted for by capturing traffic in multiple locations. In addition, most tools allow for filtering on keywords during the capture. For example, a filter can be configured to only show a MAC address for specific OUIs listed, e.g., filter for B0:C1:9E, which is the ZTE OUI. This process will be time-consuming since many vendors have more than one MAC address OUI registered to their company, resulting in potentially thousands of filter entries. Once the list is created, the process can run for extended periods of time and allow for the detection of devices as they are added to the network.

[24] There are many techniques to passively capture network traffic.
[25] A switch port is a physical port in a network switch where a networking cable is connected.



arp

No.	Time	Source	Destination	Protoco	Length	Info
29251	17:12:22.1077…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
29485	17:12:22.9338…	Cisco_8 [redacted]	HuaweiS [redacted]	ARP	56	Who has 192.168.91
29486	17:12:22.9340…	HuaweiS [redacted]	Cisco_8 [redacted]	ARP	60	192.168.91.104 is
29521	17:12:23.0877…	HuaweiS [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
29522	17:12:23.0877…	Cisco_8 [redacted]	HuaweiS [redacted]	ARP	56	192.168.91.1 is at
29532	17:12:23.1092…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
29533	17:12:23.1092…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
29795	17:12:23.9951…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
29822	17:12:24.1064…	AmazonT [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
29823	17:12:24.1064…	Cisco_8 [redacted]	AmazonT [redacted]	ARP	56	192.168.91.1 is at
29826	17:12:24.1109…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
29827	17:12:24.1109…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
30046	17:12:24.8509…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
30117	17:12:25.1126…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
30118	17:12:25.1128…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
30160	17:12:25.2532…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
30420	17:12:26.1144…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
30421	17:12:26.1144…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
30457	17:12:26.2280…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
30464	17:12:26.2430…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
30638	17:12:26.8439…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
30701	17:12:27.1162…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
30702	17:12:27.1162…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
30750	17:12:27.2641…	Cisco_8 [redacted]	Espress [redacted]	ARP	56	Who has 192.168.91
30751	17:12:27.2742…	Espress [redacted]	Cisco_8 [redacted]	ARP	60	192.168.91.212 is
30863	17:12:27.6546…	Cisco-L [redacted]	Broadca [redacted]	ARP	60	Who has 192.168.91
30969	17:12:28.0334…	Apple_5 [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
30970	17:12:28.0334…	Cisco_8 [redacted]	Apple_5 [redacted]	ARP	56	192.168.91.1 is at
30996	17:12:28.1433…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
30997	17:12:28.1433…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at
31152	17:12:28.6747…	Espress [redacted]	Broadca [redacted]	ARP	60	Gratuitous ARP for
31272	17:12:29.1458…	Roku_ab [redacted]	Cisco_8 [redacted]	ARP	60	Who has 192.168.91
31273	17:12:29.1458…	Cisco_8 [redacted]	Roku_ab [redacted]	ARP	56	192.168.91.1 is at

Figure 4: Mirroring Port Capture using Wireshark

Key Takeaways

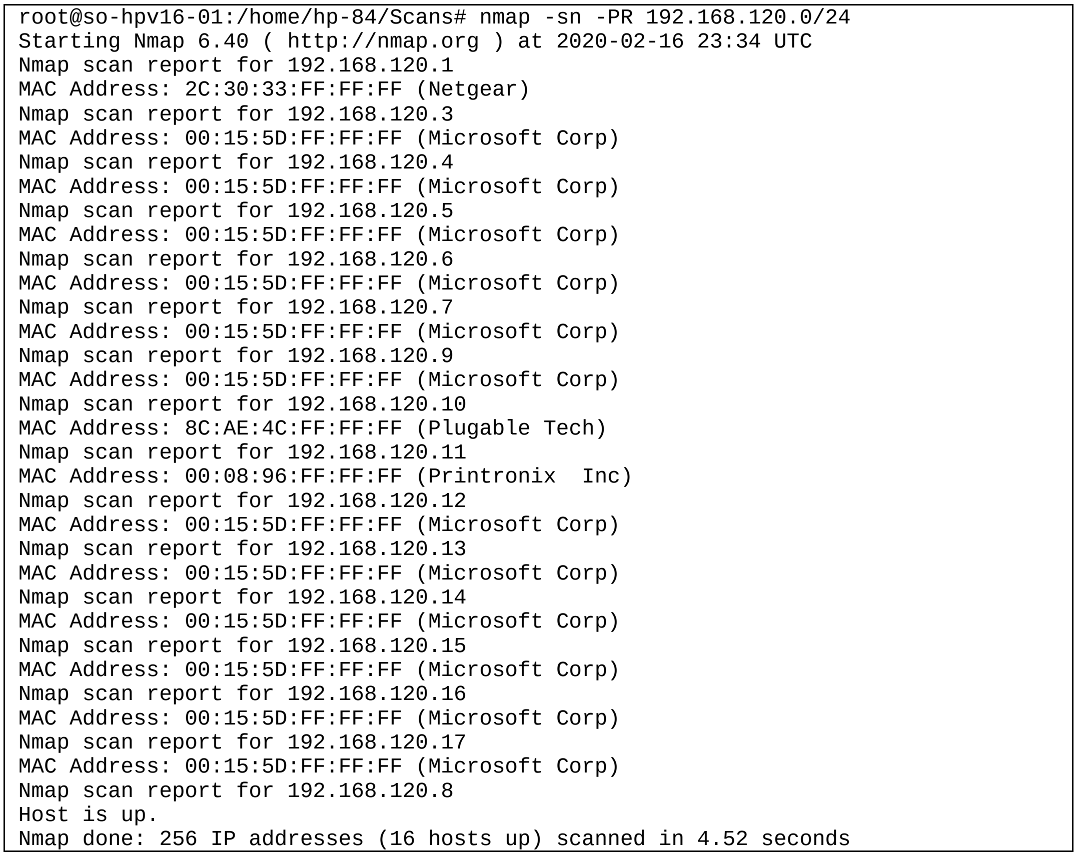
The techniques described above identify a NIC vendor, but there are other passive techniques available to identify NICs and other components. All methods previously described, as well as those below, should be tested to ensure there is no operational impact to the production environment. A network or cybersecurity professional may know what options are appropriate for the operating environment.

Key takeaways:

- Many entities have a testbed or development network that is a representation of the production network. Perform the scans in these environments before using the techniques described. Also, use caution when developing automated processes in the production environment.
- Most networked devices, such as routers, can list the ARP cache table saved, and the list can be compared with an OUI list. This may not produce a complete list of all the MAC addresses in a local network.
- Write signatures for IDSs that can detect the MAC address and OUI for a specific vendor. This approach has an advantage because it operates continuously, but the disadvantage is it may also require many signatures to be written for all the OUIs. Writing a subset of OUIs may be more appropriate.
- Many systems have routine or continuous scans to monitor system health and/or check for vulnerabilities. The tool(s) used for these scans can typically be configured to capture the MAC address and identify the vendor based on the OUI. Additionally, the same tools can examine other components in the system and identify the vendor, i.e., CPU, GPU, and driver vendors may be identified using these tools.
- Many devices have a method to manually change the MAC address. As a result, a vendor may have changed the MAC OUI to obfuscate the identity of the vendor, e.g., Huawei is changed to a Cisco OUI. Comparing the discovered OUI to the expected OUI may indicate abnormal activity. If a Cisco OUI is identified in a Dell system, the security professional may want to perform additional research as to why the OUI was not identified as expected. Please note, this may be a time-consuming task.
- A *Virtual Machine (VM)* MAC address may be identified as the vendor of the *hypervisor* and not the actual physical MAC address of the NIC that is installed in the device such as a server. Figure 5. shows 12 Microsoft MAC addresses that are associated with Microsoft's "Hyper-V" hypervisor; each of the 12 MAC addresses

start with the first three octets of 00:15:5D, which is an OUI for Microsoft. The physical NIC for the Hyper-V server has the first three octets of 8C:AE:4C, which is for “Pluggable Tech” with an IP address of 192.168.120.10. How the MAC address for a hypervisor is identified may vary between vendors and should be tested. It should not be assumed the physical NIC for the hypervisor's physical machine will be identified when a scan is performed.

- IPv6 networks use a Neighbor Table (also known as IPv6 Neighbor Discovery Cache) to display the MAC addresses for an IPv6 network.
- Other tools to consider consist of:
    - arp-watch
    - arp-scan
    - snmp discovery
    - hping3
- There are additional components, beyond those identified in this report, which a malicious actor may use to install a backdoor. Entities that are concerned should discuss this with their cybersecurity professionals and cybersecurity vendors and partners, as well as state and federal partners that have details of compromised devices and techniques.



```
root@so-hpv16-01:/home/hp-84/Scans# nmap -sn -PR 192.168.120.0/24
Starting Nmap 6.40 ( http://nmap.org ) at 2020-02-16 23:34 UTC
Nmap scan report for 192.168.120.1
MAC Address: 2C:30:33:FF:FF:FF (Netgear)
Nmap scan report for 192.168.120.3
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.4
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.5
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.6
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.7
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.9
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.10
MAC Address: 8C:AE:4C:FF:FF:FF (Plugable Tech)
Nmap scan report for 192.168.120.11
MAC Address: 00:08:96:FF:FF:FF (Printronix  Inc)
Nmap scan report for 192.168.120.12
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.13
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.14
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.15
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.16
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.17
MAC Address: 00:15:5D:FF:FF:FF (Microsoft Corp)
Nmap scan report for 192.168.120.8
Host is up.
Nmap done: 256 IP addresses (16 hosts up) scanned in 4.52 seconds
```

Figure 5: Nmap scan of network with multiple virtual machines.