



SCHOOL OF COMPUTING

Sacred Heart University

VULNERABILITY ASSESSMENT FOR IOT- BASED SMART HOMES

**A project report submitted for the requirements of computer science master's
degree in cyber security CS670**

Bandar Almutairi
November 2018

CONTENTS

Abstract	3
Introduction	3
Problem statement	4
Literature review.....	5
Vulnerability assessment methodology of IoT devices	6
Standard vulnerability assessment methodology.....	6
Modified vulnerability assessment methodology.....	7
Vulnerability assessment results	9
Printer	9
Smart plug	12
Fire TV	13
Smart TV	15
Smart thermostat.....	16
Conclusion.....	18
References	19
Appendices	20
Appendix 1: Zenmap	20
Appendix 2: Risk score level symbols.....	28
Appendix 3: Vulnerability assessment result of IoT devices.....	28

ABSTRACT

The internet of things (IoT) technology continues to play a critical role in the evolution of society, and it is continually growing and evolving to fit the wants and desires of society. While developing the IoT and improving device capabilities provides the individual with an increased level of connectivity and convenience. However, the introduction of the IoT into our home results to some potential security threats and privacy issues such as the credibility of data and authenticity. These difficulties make smart homes vulnerable to different types of security attacks, resulting in IoT-based smart homes being insecure. For this reason, it is essential to identify the possible security vulnerability to develop a complete picture of the security status of smart homes, most of which are unknown to the users. The purpose of this research is to highlight the security vulnerabilities associated with the IoT based smart home, and it comes up with some recommendations to the users to either remove those weaknesses or reduce below the risk level.

INTRODUCTION

The concept Internet of Things (IoT) does not have a universally accepted definition. Despite being associated with Industry 4.0, different people and schools of thought have bestowed befitting definitions to the term, although its etymology and original usage has been credited to Kevin Ashton [1], a digital innovator. Based on all the versions of its definition, it is apparent that it initially mean data created and collected through conscious human actions, while the latest version implies that the data is created by "things," hence the name, the Internet of Things.

Commonly, IoT refers to and encompasses computers, devices, and objects that interact, exchange and process data so that IoT can be envisaged as a new technology that combines several existing information technologies. The primary objective of IoT, as the definition suggests, is to identify, access and control connected things over the internet using unique identities regardless of time and

location. The network of interconnected devices can create a pool of intelligent and autonomous applications and services that promote personal, professional, and commercial benefits.

The concept of IoT and related technologies can be used to automate and create smart homes that have intelligence services that improve both comfort and quality of life. However, integration of IoT into homes bring with it several new security issues given their connection to the internet. Consequently, smart homes base on IoT requires elevated security levels considering the sensitivity and privacy of the information that can be exploited and abused. Even though modern technologies such as IoT have opportunities, they bear greater risks and smart homes are vulnerable to cyber-attacks with consequences being dire. It should be noted that all the devices on the smart home network are entry points and a hack into one of them can lead to an inversion of privacy, theft of personal information, and illegal spying and monitoring of activities of family members [2]. Hence, smart homes based on IoT requires appropriate security measures including regular vulnerability assessment.

The number of IoT devices has grown at an unprecedented rate from 12.5 billion in 2010 to a projected 50 billion active devices by 2020 [3]. The threat surfaces will increase with such growth and the number of security issues will equally grow. Against the backdrop of this information and considering the growing areas of applications of IoT, the proposed research focuses on security issues facing IoT-based Smart Homes as well as recommendations that can assist end users to avert them.

PROBLEM STATEMENT

Due to the widespread deployment of IoT their security needs to be investigated otherwise the privacy, integrity, and confidentiality of users can be damaged, and eventually, people will lose trust in this technology. The aim of this research is to address the security vulnerabilities for IoT-Based smart home and give the user an overview of the risks associated with IoT.

LITERATURE REVIEW

Nessus is among the leading tools for vulnerability assessment although it stands out because it is comprehensive and has the deepest and broadest tools for scanning vulnerability in the market [4]. However, the Open Web Application Security Project (OWASP) purposes to improve the security of software through provision of information on IoT vulnerability test techniques, guidelines and rules for conducting a test on IoT devices, and an IoT test framework that aid in appraising and understanding IoT security challenges [5].

Besides Nessus, Platforms such as Qualys can also be used during vulnerability assessment. Qualys Cloud Platform focuses on the security of applications on cloud platforms using the same technology or framework. Being a cloud-based assessment tool, Qualys offer round the clock continuous assessment from a global perspective and ensuring compliance with global standards. It provides a second monitoring tool across IT assets and has been described as a complete solution ensuring end-to-end protection. The services available within Qualys Cloud platform including but not limited to continuous monitoring, management of vulnerabilities, policy compliance, PCI compliance, security assessment questionnaire, web application scanning, and web application firewall [6].

In addition, Ali and Awad opine that smart wireless sensors have become extremely valuable devices for monitoring smart home applications. As a result, they have been an attractive target for cyber - attacks. Despite the many benefits associated with IoT, it has many vulnerabilities. The attacker can hack any interconnected devices through the network and having directly accessing the smart home. This means that if the local home network is taken over, the entire household network becomes unsafe [2].

VULNERABILITY ASSESSMENT METHODOLOGY OF IOT DEVICES

Introduction

The research prospect aims at identifying vulnerability points and issues in IoT devices used in smart homes, and such a task requires selection of a methodology including appropriate hardware and software tools. The section provides information on standard methods and techniques used to assess the vulnerability of IoT devices. A subsequent novel vulnerability assessment method developed based on the existing frameworks was introduced and adopted for the research of vulnerabilities within the IoT devices. It is imperative to reiterate the assessment methodology has been modified according to the scope and requirements of this study.

Standard Vulnerability Assessment Methodology

Different scholarly articles and technical sources have described different techniques for assessing vulnerabilities in IoT devices. These methods are slightly different but the most commonly used and widely accepted vulnerability assessment method consists of the phases illustrated in Figure 1.



Figure 1: Standard Vulnerability Assessment Methodology

Figure 1 illustrates the commonly used method for assessing vulnerability in systems. However, while applying such a technique in assessing vulnerabilities in IoT devices, it is mandatory to follow the above steps precisely. In conventional penetration testing, ethical hackers follow the standard methodology but modify parameters to meet their objectives and ensure that the scope of the expected problem is fully understood [7].

Modified Vulnerability Assessment Methodology for IoT Devices

The standard method presented in Figure 1 is adopted with slight changes. Notably, gaining access to systems and concealing such tracks are not within the scope of the research and the phases are subsequently dropped from the standard methodology; hence, the following modified model.

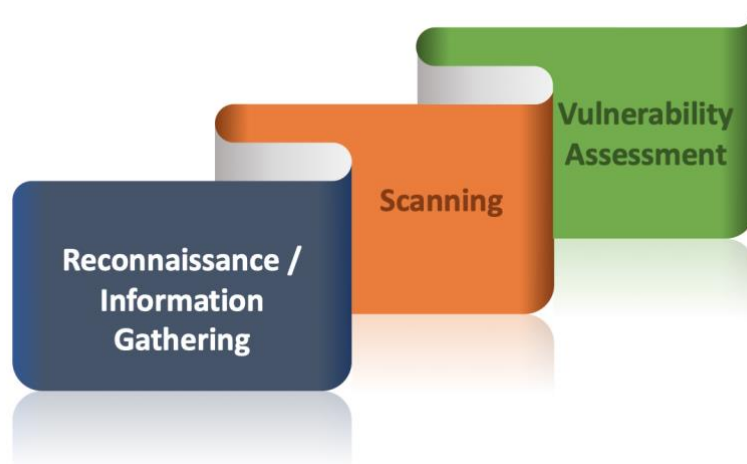


Figure 2: Modified Vulnerability Assessment Methodology

The phases of the assessment method in Figure 2 are discussed as follows:

1. Reconnaissance involves the acquisition of information about the target devices before commencing actual assessment of its security. The phase does identify any underlying security issues, but it is critical for achieving better assessment results. Based on the scope of research, the information that can be retrieved from reconnaissance is limited to hardware, operating systems, default passwords, and web server versions [8].

2. Scanning identifies the services and ports running and open on the IoT device of interest. Based on the scope of the research, the scanning stage will identify all open ports and aid in creating the port profile of all IoT devices on the home network [8].
3. Vulnerability assessment phase is the core of this research and it will identify security threats and risks associated with the IoT devices of interest. Some of the predetermined security issues include SQL injection, cross-site scripting (XSS), buffer overflow and password auditing [9].

Tools Used in Vulnerability Assessment

There are several tools used for the Vulnerability assessment of IoT devices. In this section, various tools have been listed for the Vulnerability assessment of IoT devices as follows:

PURPOSE OF TOOLS	TOOLS NAME	DESCRIPTION
Information Gathering and Scanning	Nmap	This tool used to identify the ports opened in IoT devices.
	Zenmap	This tool is a GUI tool of Nmap which provide advance features
Vulnerability Assessment	Nessus	This tool used to identify security issues in IoT devices.
	Qualys	This tool used to identify and assess vulnerabilities in IoT devices so that they can be corrected and prioritized before they are exploited by attackers. It used to scan for vulnerabilities in web applications.
	OWASP ZAP	This tools specifically used to identify vulnerabilities in the web interface of IoT devices. Using multiple tools in finding vulnerabilities is a good practice as this will reduce the number of false positive vulnerabilities.
Supporting Tools	Wireshark	This is a supporting tool and it used to capture network traffic of IoT devices.

Table 1: Tools for Vulnerability Assessment of IoT Devices

These tools have been selected for the assessment process due to the following reasons:

1. The tools have a rapport within the field and they are commonly used for appraising the security status of IoT devices.
2. The tools are open source and leverage budget constraints associated with acquiring security tools.

VULNERABILITY ASSESSMENT RESULTS

Introduction

The scope of this research is to identify threats that can emerge due to the insecure IoT devices. For achieving the goals of this research, a specific vulnerability assessment was conducted on a sample of IoT devices. This section describes the vulnerability assessment results of IoT devices and gives recommendations for their secure usage.

Scope

The following of IoT devices were selected for vulnerability assessment testing:

1. Epson workforce printer
2. Smart Plug
3. Fire TV
4. Smart home TV
5. Nest Thermostat

VULNERABILITY ASSESSMENT OF PRINTER

Introduction

Printers are widely used ranging from homes to big corporates around the globe. Due to the usage of printers in a smart home environment, they have been selected for this research. The Printer selected specifically for this research is Epson workforce printer as it is easy availability in a lab environment. This section presents the detailed Vulnerability issues in Epson workforce printer and gives recommendations for its secure usage. The following table shows the technical specifications of Epson workforce printer that was under testing:

Device Type	Printer
Vendor	Epson Workforce
Model Name	WF-3620
Model Number	C481D
Serial Number	SEDY14707
Device Management Protocol	SSL/TLS
Connectivity	Ethernet

Table 2: Technical Specifications of Printer

Testing Scenario

Epson workforce printer was connected to the local area network in the lab environment. Also, the test machine prepared for the Vulnerability assessment of printer was connected to the same network. All tools were installed in the test machine necessary for the Vulnerability assessment of printer. The tools used for the Vulnerability assessment of Epson workforce printer were Nmap, Nessus, OWASP ZAP and Qualys. For the description of these tools, please refer to Section.

Scope of Work

The scope of the work is to conduct a detailed Vulnerability assessment of Epson workforce with the methodology as mentioned above.

Vulnerability Assessment Findings in Printer

1. **No Password Protection:** The web interface of the printer was not protected with passwords, and as a consequence any authorized or unauthorized user can access the web interface of printer.
2. **SNMP Protocol Version Detected:** SNMP protocol is found enabled on the printer for managing devices on IP networkers. SNMPv1/v2 is an unsecure protocol, and it cannot ensure the confidentiality, integrity, and Authentication of data exchanged between printer and users [10].
3. **SNMP Agent Default Community Name (public):** The default name for SNMP community string on the printer is PUBLIC. This information can be guessed by attacker to gain more knowledge about the printer [11].

4. **SSL Version 2 and 3 Protocol Detection:** The printer accepts connections encrypted using SSL 2.0 and/or SSL 3.0. which is affected by several cryptographic flaws. This is can be a result of a man-in-the-middle or decrypt the communications between the affected printer and users.
5. **SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE):** Since the printer supports SSLv3, which makes it vulnerable to Padding Oracle on Downgraded Legacy Encryption now as POODLE. The attacker tricks the browser into connecting with SSLv3 and gain access to encrypted communication between a printer and users.
6. **SMB Signing Disabled or SMB Signing Not Required:** the printer does not seem to be using SMB (Server Message Block) signing which is a security mechanism to help improve the security of the SMB protocol. When SMB signing is disabled on both the client and server SMB sessions are unauthenticated which can allow man-in-the-middle attacks against the SMB server.
7. **Readable SNMP Information:** Read-access to all SNMP information can give unauthorized users an incredible amount of valuable and sensitive information about your network.
8. **SSL Self-Signed Certificate:** The certificate is not signed by a known certificate authority. This can establish a man-in-the-middle attack against the printer.
9. **HTTP Security Headers:** The following HTTP security headers were not enabled in the web interface of the printer which are X-Frame-Options Header Missing, X-XSS-Protection header and X-Content-Type-Options Header. HTTP security headers protect web applications from various types of web application attacks.
10. **Application Error Disclosure:** The login interface of the printer shows an error/warning message that may disclose sensitive information in case of failed login, which helps attackers in guessing user names of printer's users easily.

Recommendations:

1. Enable password protection on web interface of printer.
2. Disable or remove SNMPv1/2c authentication and Use SNMP version 3 authentication which provides additional security features.

3. Change the default community string.
4. Use TLS 1.1 with recommended cipher suites only for ensuring communication security.
5. Disable SSL 2.0 and 3.0. by Consult the application's documentation to avoid this vulnerability.
6. Enabled SMB sign or it is recommended that SMB signing is enabled and required.
7. Block access to SNMP services at the network perimeter or restrict all SNMP access to separate management networks that are not publicly accessible.
8. Purchase or generate a proper certificate for this service.
9. Enable HTTP security headers on all web pages of printer web interface.
10. Implement password checker at the stage of user accounts creation. Allow complex passwords only.

VULNERABILITY ASSESSMENT OF SMART PLUG

Introduction

Smart plugs belong to the category of IoT devices that used in smart electricity solutions. Smart plugs have huge advantages compared with the traditional plugs including efficient electricity usage, remote management, and safety [12]. In the section below, Vulnerability issues will be identified in the smart plugs. The following table shows the technical specifications of the smart plug that was under testing:

Device Type	Smart Plug
Device Name	Smart WIFI Socket
Model Number	SW A1
Wireless IEEE standards	WIFI 2.4 GHz b/g/n
Security type	WEP64/WEP128/TKIP/CCMP
Security mechanism	WEP/WPA-PSK/WPA2-PSK

Table 3: Technical Specifications of Smart Plug

Testing Scenario

First of all, smart plug was plugged into an electric socket, and then it was configured with some basic settings as per the available user' guide. After that, smart plug gets operational it connects to

the local network. Also, smart plug was controlled with an app called eFamily which was connected to the same WIFI network. A test machine was also connected to the same network of the smart plug. The tools used for the vulnerability assessment of smart plug were Nmap, Nessus, and Qualys. For the description of these tools, please refer to Section.

Scope of Work

The scope of the work is to conduct a detailed vulnerability assessment of Smart Plug with the methodology as mentioned above.

Vulnerability Assessment Findings in Smart Plug

Non-Zero Padding Bytes Observed in Ethernet Packets: The service detected that the small packets from the host were padded to the minimum size using non-zero padding bytes which may be exploited to fingerprint the Ethernet cards and device drivers.

Recommendations

Contact the vendor of the Ethernet cards and device drivers for the availability of a patch.

VULNERABILITY ASSESSMENT OF FIRE TV

Introduction

These days, Streaming devices are trending with smart features in home environment. Due to the usage of Streaming devices in a smart home environment, the Fair TV has been identified for this research. This section presents the detailed Vulnerability issues in Fair TV and gives recommendations for its secure usage. The following table shows the technical specifications of Fire TV that were under testing:

Device Type	Streaming devices
Vendor	Amazon
Model number	DV83YM
Serial Number	G070GV01536303E6
Software Version	6.0.9.1-014
Networking	Networking: Wifi 802.11 a/b/g/n/ac; 2x2 MIMO (2.4 GHz and 5.0 GHz dual band) Networking: Ethernet 10/100Mbps
Device Operating System	Fire OS 5 — Based on Android 5.1 (API Level 22)

Table 4: Technical Specifications of Fire TV

Testing Scenario

Fire TV was connected to the local area network in the lab environment. Also, the test machine prepared for the vulnerability assessment of Fire TV was connected to the same network. All tools were installed in the test machine necessary for the vulnerability assessment of Fire TV. The tools used for the vulnerability assessment of Fire TV were Nmap, Nessus, Qualys, and OWASP ZAP. For the description of these tools, please refer to Section.

Scope of Work

The scope of the work is to conduct a detailed vulnerability assessment of Fire TV with the methodology as mentioned above.

Vulnerability Assessment Findings in Fire TV

HTTP Security Headers: HTTP protocol provides security headers for the security of web applications, but it was observed that these headers were not configured on the management interface of the Fire TV. The headers that were not configured include X-frame-options header, X_XSS protection header and X-content-type- options header.

Recommendation:

Enable HTTP security headers on of the Fire TV.

VULNERABILITY ASSESSMENT OF SMART HOME TV

Introduction

Smart TV is considered a necessary entertainment system tailored to the average user which can be placed in a typical home network. [13]. For this reason, Smart home TV has been selected for this research. The Smart home TV selected specifically for this research is Samsung as it is availability in a lab environment. This section presents the detailed Vulnerability issues in Smart home TV and gives recommendations for its secure usage. The following table shows the technical specifications of Smart home TV that was under testing:

Device Type	Smart home TV
Vendor	Samsung
Model Number	UN55JU670D
Serial Number	03PQ3CCG700326P
Software Version	T-HKMAKUC-1530.1, BT-S
Connection	802.11ac Wi-Fi Built In

Table 5: Technical Specifications of Smart home TV

Testing Scenario

Smart home TV was connected to the local area network in the lab environment. Also, the test machine prepared for the vulnerability assessment of Smart TV was connected to the same network. All tools were installed in the test machine necessary for the vulnerability assessment of Smart TV. The tools used for the vulnerability assessment of Smart TV were Nmap, Nessus, and Qualys. For the description of these tools, please refer to Section.

Scope of Work

The scope of the work is to conduct a detailed vulnerability assessment of Smart home TV with the methodology as mentioned above.

Vulnerability Assessment Findings in Smart home TV

1. **Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows**

RCE: The Portable SDK for UPnP TV (libupnp) library contains multiple buffer overflow vulnerabilities. Smart home TV use (libupnp) may accept UPnP queries over the WAN interface, thus exposing this vulnerability allow an unauthenticated hacker to execute arbitrary code on the device or cause a denial of service.

2. **SSL Self-Signed Certificate:** The certificate is not signed by a known certificate authority. This can establish a man-in-the-middle attack against the Smart TV.

VULNERABILITY ASSESSMENT OF SMART THERMOSTAT

Introduction

The Smart Thermostat is the next generation of temperature control, and It offers more control over your home's climate and temperature [14]. The Smart Thermostat selected specifically for this research is Nest as it is easy availability in a lab environment. This section presents the detailed Vulnerability issues in Smart Thermostat and gives recommendations for its secure usage. The following table shows the technical specifications of Smart Thermostat that was under testing:

Device Type	Thermostat
Vendor	Nest
Model	Display-3.4
Backplate Model	C481D
Serial Number	09AA01AC161708G1
Software Version	5.8.2-1
Connectivity	Wi-Fi: 802.11b/g/n 2.4GHz

Table 6: Technical Specifications of Smart Thermostat

Testing Scenario

Thermostat was connected to the local area network in the lab environment. Also, the test machine prepared for the vulnerability assessment of Thermostat was connected to the same network. All tools were installed in the test machine necessary for the vulnerability assessment of Thermostat. The tools used for the vulnerability assessment of Thermostat were Nmap, Nessus, and Qualys. For the description of these tools, please refer to Section.

Scope of Work

The scope of the work is to conduct a detailed vulnerability assessment of Thermostat with the methodology as mentioned above.

Vulnerability Assessment Findings in Thermostat

Smart Thermostat was subjected to vulnerability assessment using different methods, but interestingly no vulnerabilities have been classified in Smart Thermostat. The reason was that smart Thermostat had not opened any ports for its operation. Interestingly Smart Thermostat was found to be fully operational even without running any service in it. From the consequences of lab experimentation it can be concluded that if any IoT device can deliver its services without opening its ports (services), then the possibility of its hacking gets reduced.

Recommendations

Every IoT devices should try to deliver its services without opening ports, if possible. If opening ports are necessary for the function and operation of any IoT device, then least ports should be opened. As opening ports open additional attack vectors for insiders, hackers, and outsiders.

CONCLUSION

The use of IoT technology in the smart home has yielded both benefit and risks. The devices are efficient and fun to use. However, they are highly vulnerable to security risks in a smart home environment.

In this research, significant issues in some of the IoT devices based smart homes were identified by achieving a comprehensive vulnerability assessment and document all the findings in one place. In order to make these objectives, multiple IoT devices were subjected to in detailed vulnerability assessment using the latest tools and methodologies.

The first objective of the research has been successful as this research provides a comprehensive vulnerability assessment which will serve as a starting point for users who need to investigate in the security of their IoT devices without wasting time. The second objective of this research was to provide the best recommendations for securing IoT devices. Considering the identified security issues in IoT devices, best recommendations have been derived, and hence the last objective of the research was also achieved successfully.

This research concludes that insecurities in IoT devices seriously affect the privacy of the user, and in order to get broad acceptance among users, security must be better, and trust is essential to implement this technology in their home. Thus, security is one of the areas that must be put into the highest priority when performing the smart home technology.

REFERENCES

- [1] En.wikipedia.org. (2018). Kevin Ashton. [online] Available https://en.wikipedia.org/wiki/Kevin_Ashton [Accessed 13 Nov. 2018].
- [2] Mdpi.com. (2018). [online] Available at: <https://www.mdpi.com/1424-8220/18/3/817/pdf> [Accessed 13 Nov. 2018].
- [3] Cisco.com. (2018). [online] Available at: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Accessed 13 Nov. 2018].
- [4] Tenable®. (2018). Nessus Professional. [online] Available at: <https://www.tenable.com/products/nessus/nessus-professional> [Accessed 15 Nov. 2018].
- [5] Owasp.org. (2018). OWASP Internet of Things Project - OWASP. [online] Available at: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project [Accessed 15 Nov. 2018].
- [6] Qualys.com. (2018). Information Security and Compliance | Qualys, Inc.. [online] Available at: <https://www.qualys.com/> [Accessed 13 Nov. 2018].
- [7] TechRepublic. (2018). News, Tips, and Advice for Technology Professionals - TechRepublic. [online] Available at: <https://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/> [Accessed 13 Nov. 2018].
- [8] SearchITChannel. (2018). Penetration testing reconnaissance -- Footprinting, scanning and enumerating. [online] Available at: <https://searchitchannel.techtarget.com/tip/Penetration-testing-reconnaissance-Footprinting-scanning-and-enumerating> [Accessed 13 Nov. 2018].
- [9] Veracode. (2018). Vulnerability Assessment and Penetration Testing. [online] Available at: <https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing> [Accessed 13 Nov. 2018].
- [10] Inc, B. (2018). Finding and Fixing Vulnerabilities in SNMP Protocol Version Detection, a Low Risk Vulnerability. [online] Beyondsecurity.com. Available at: https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_snmp_protocol_version_detection [Accessed 13 Nov. 2018].
- [11] Ee.ucl.ac.uk. (2018). [online] Available at: <http://www.ee.ucl.ac.uk/lcs/previous/LCS2003/102.pdf> [Accessed 13 Nov. 2018].
- [12] SafeWise. (2018). SafeWise | Your Guide to Home Security and Safety. [online] Available at: <https://www.safewise.com/> [Accessed 13 Nov. 2018].
- [13] Delaat.net. (2018). [online] Available at: <http://delaat.net/rp/2012-2013/p39/report.pdf> [Accessed 13 Nov. 2018].
- [14] Bob's Heating & Air Conditioning. (2018). Benefits of Switching to a Smart Thermostat. [online] Available at: <https://www.bobsheating.com/blog/benefits-of-switching-to-a-smart-thermostat/> [Accessed 13 Nov. 2018].
- [15] Sectools.org. (2018). SecTools.Org Top Network Security Tools. [online] Available at: <https://sectools.org/> [Accessed 13 Nov. 2018].

APPENDICES

Appendix 1: Zenmap

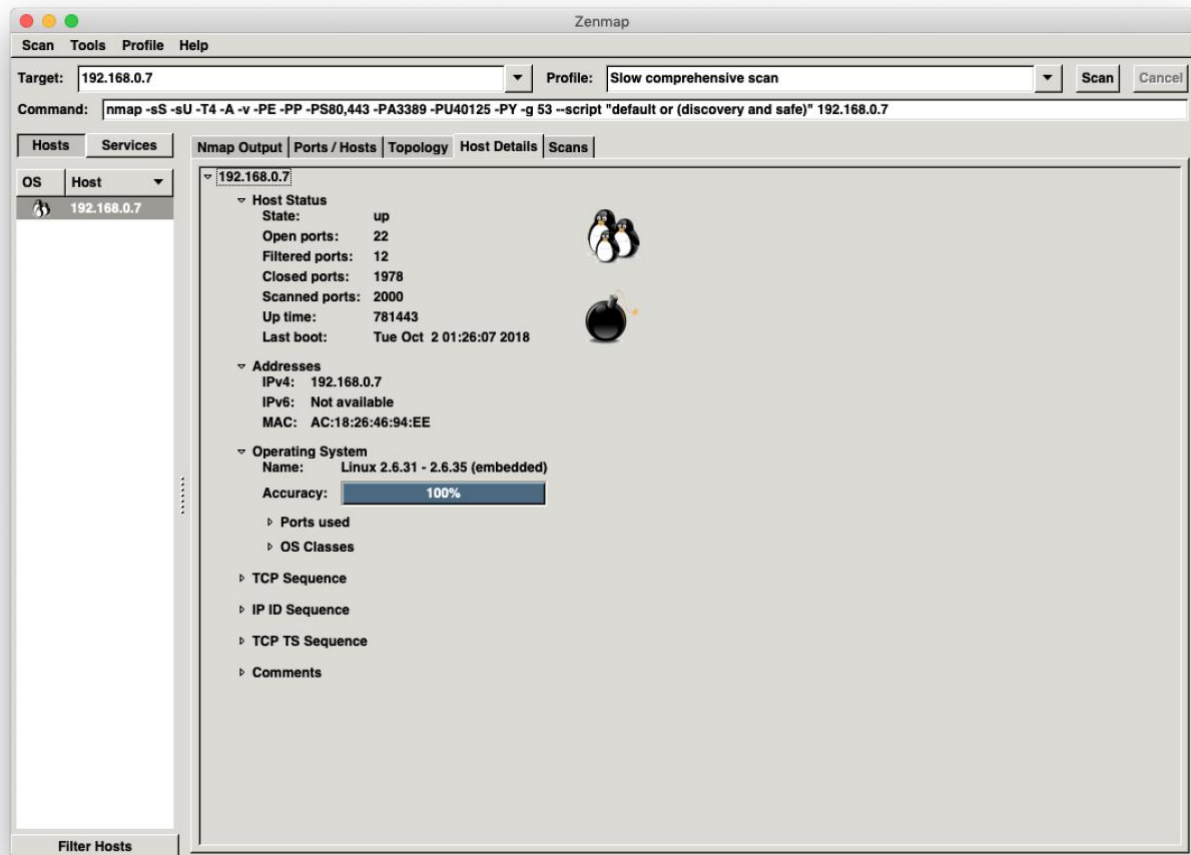


Figure 3: Information Gathering of Printer

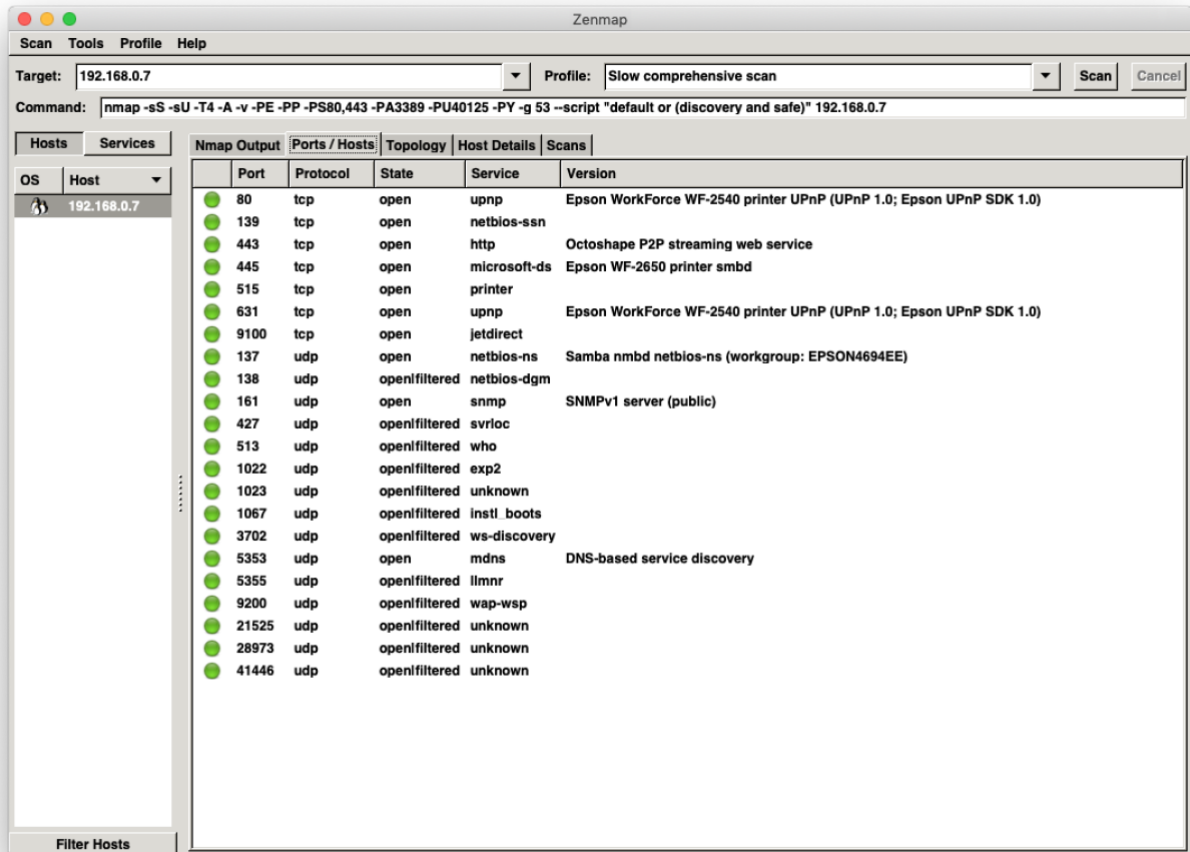


Figure 4: Information Gathering of Printer

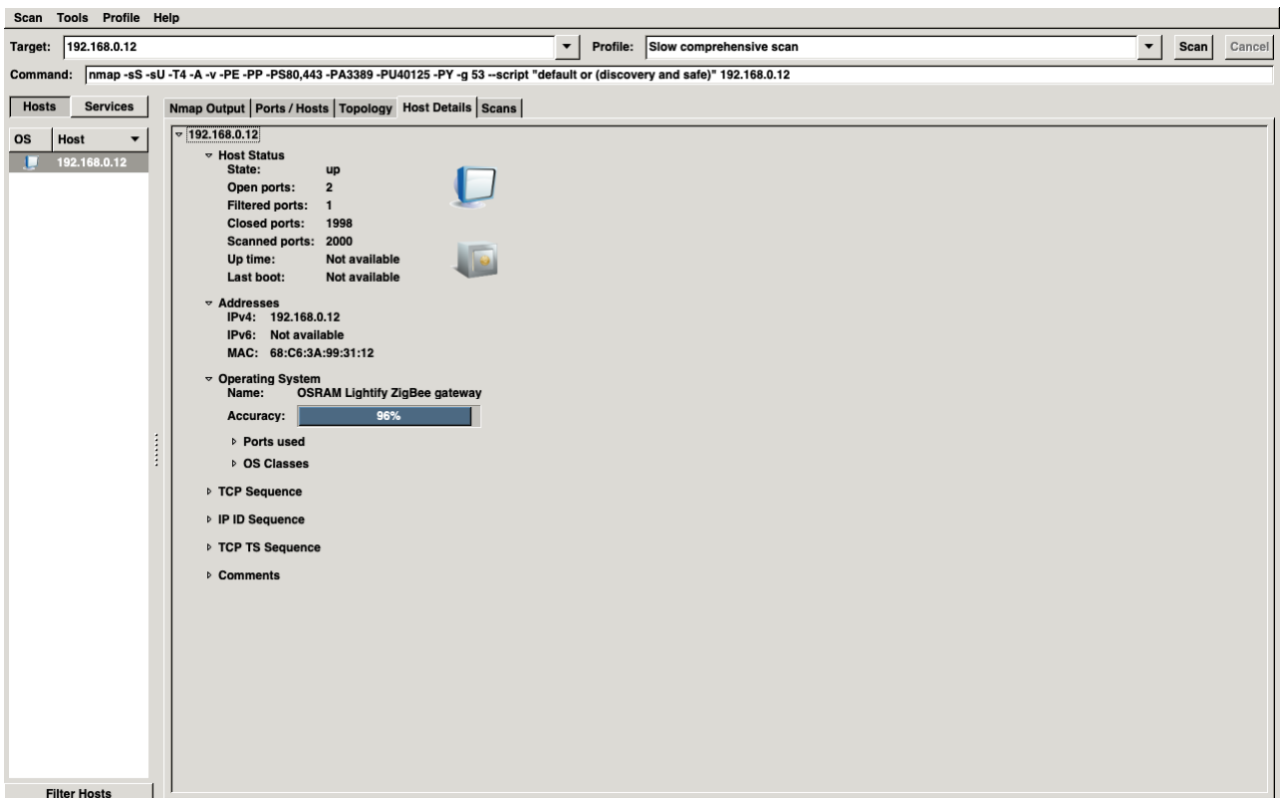


Figure 5: Information Gathering of Smart Plug

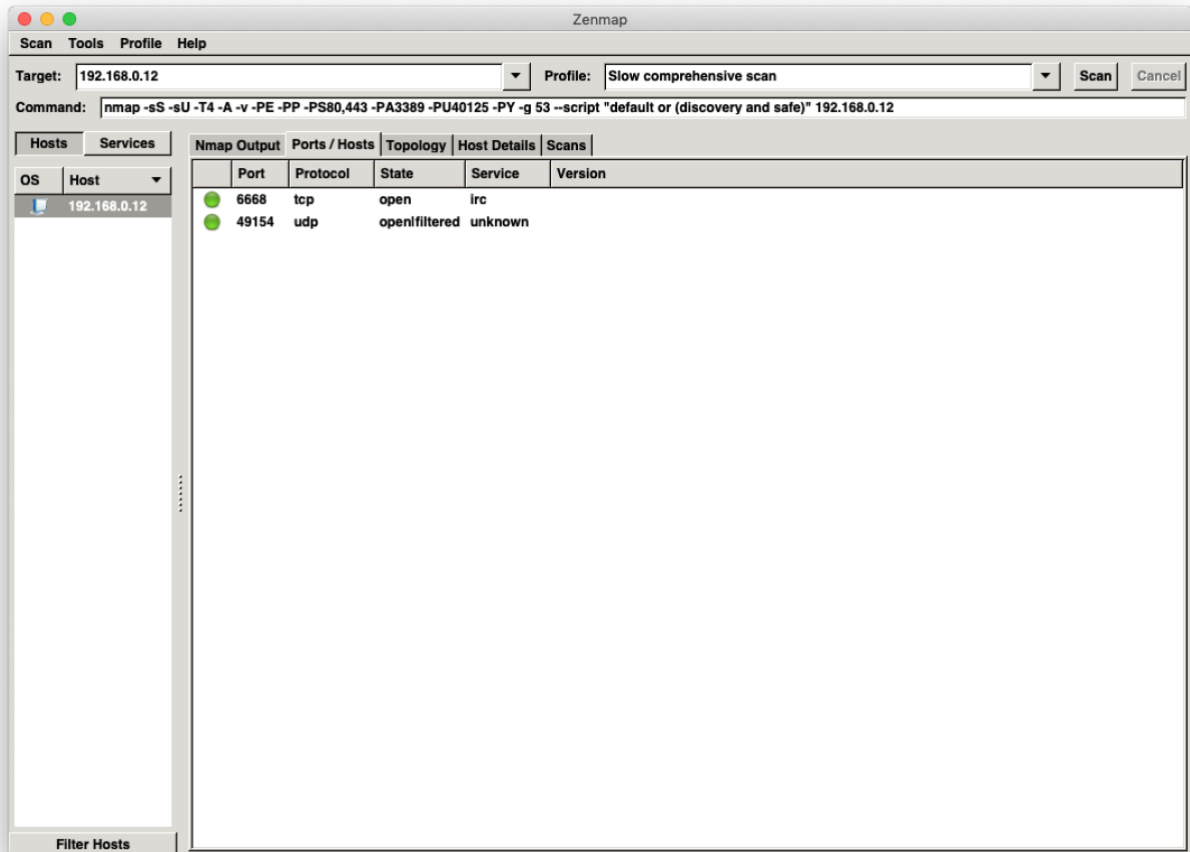


Figure 6: Information Gathering of Smart Plug

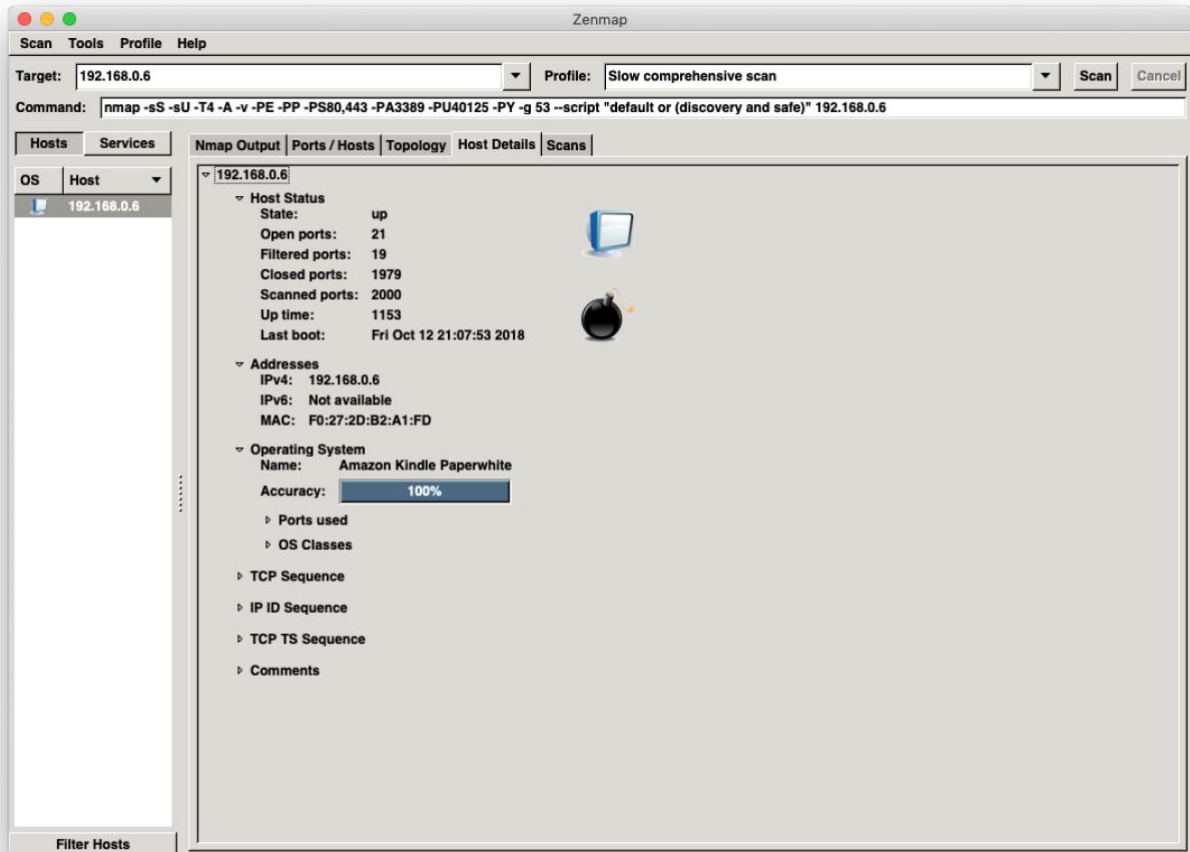


Figure 7: Information Gathering of Fire TV

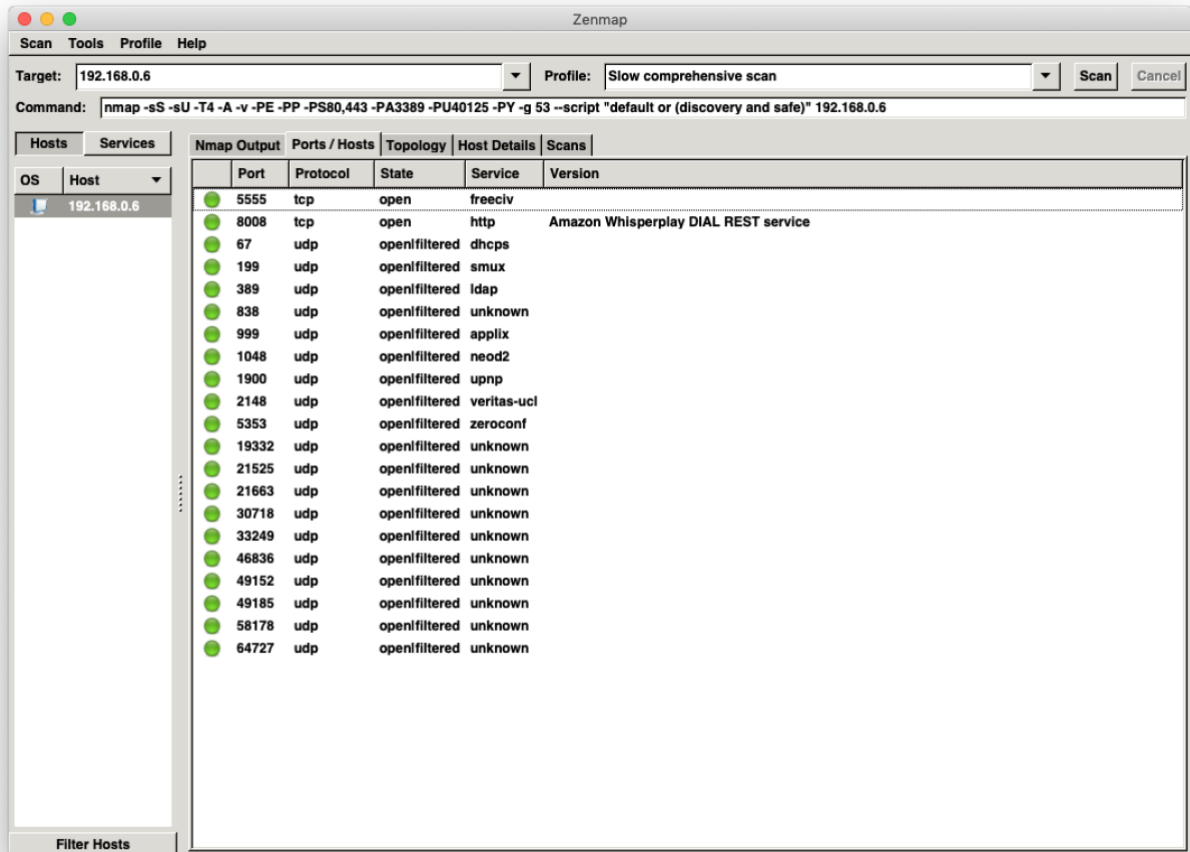


Figure 8: Information Gathering of Fire TV

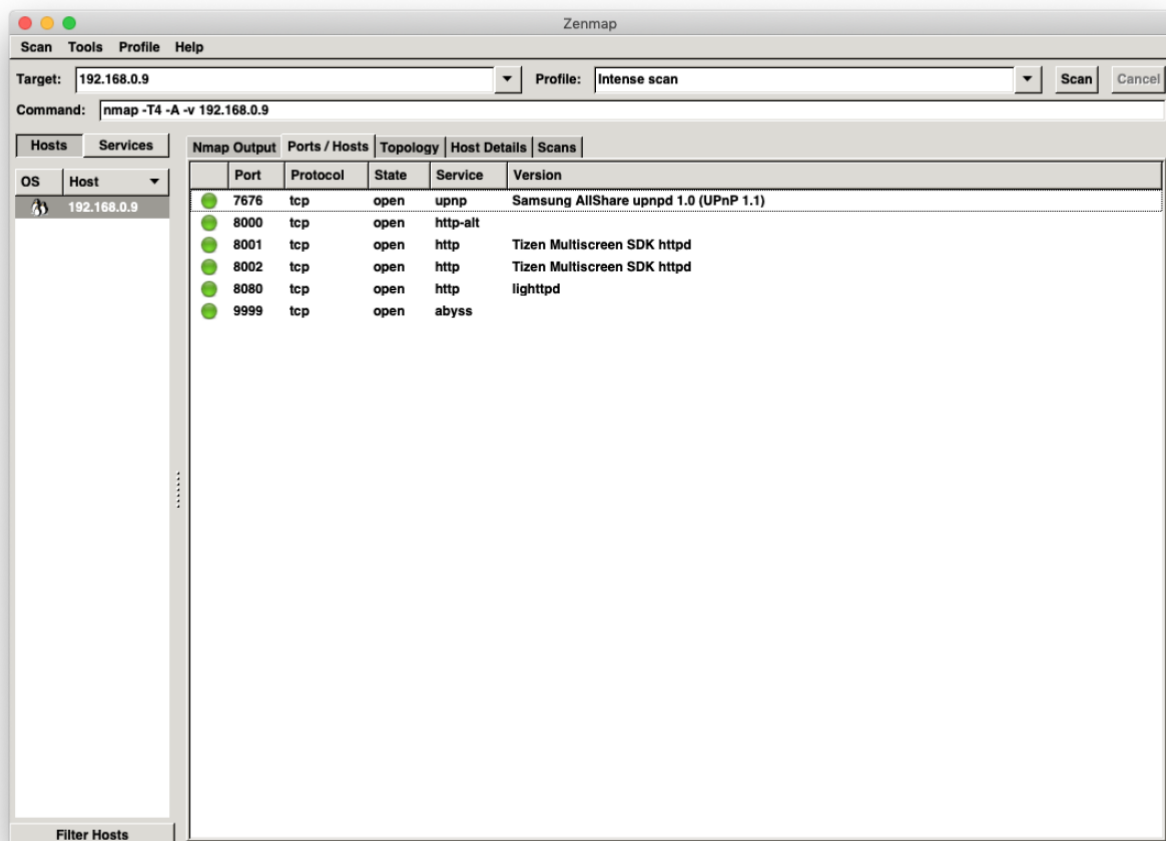


Figure 9: Information Gathering of Smart TV

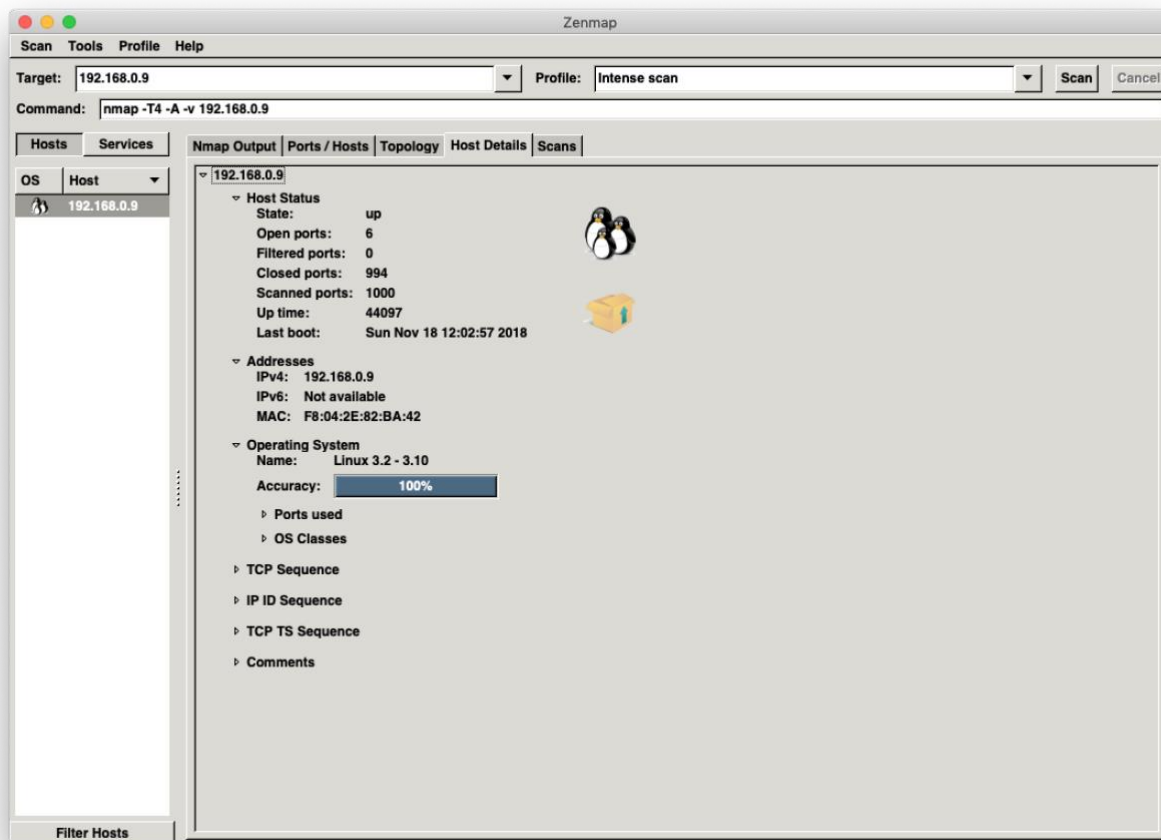


Figure 10: Information Gathering of Smart TV

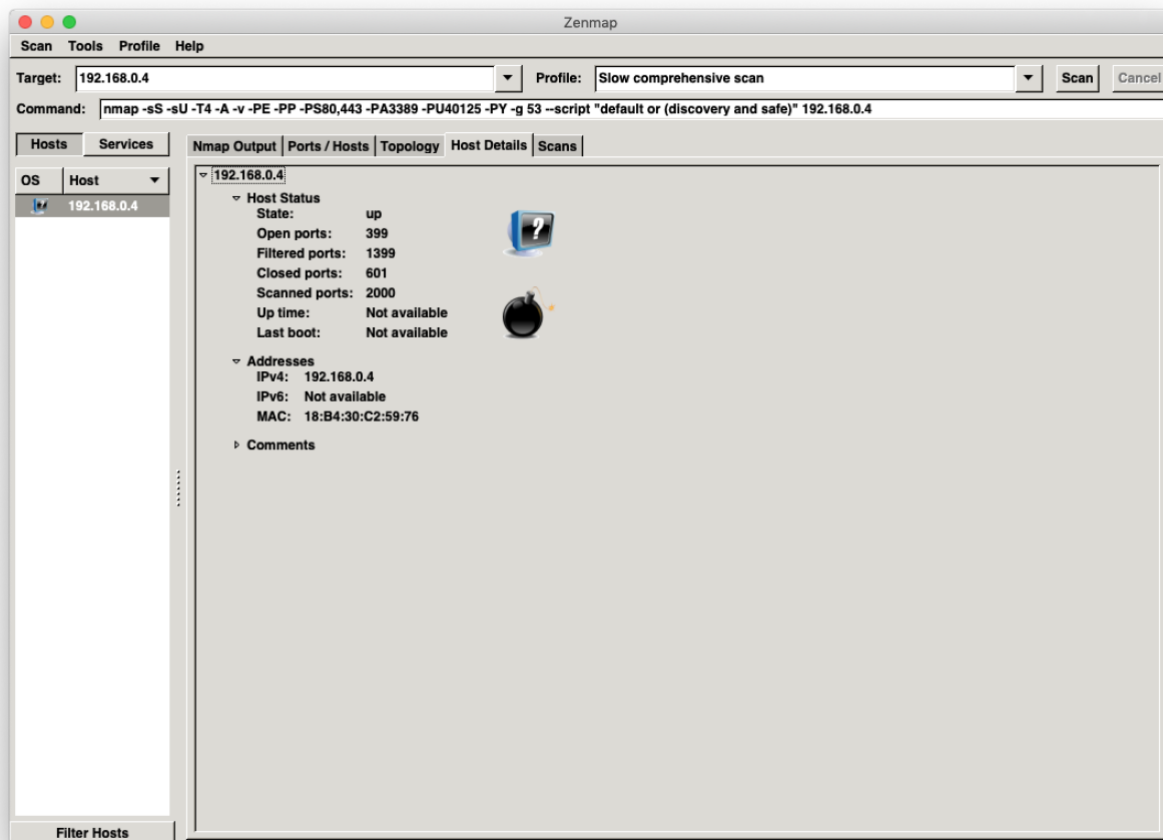
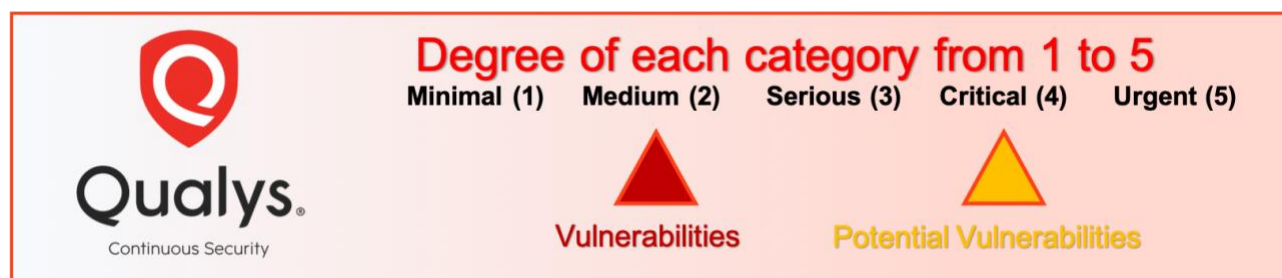
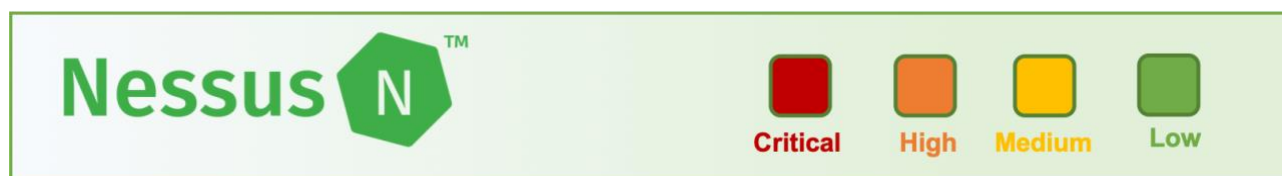






Figure 11: Information Gathering of Thermostat

Appendix 2: Risk score level symbols:













Appendix 3: Vulnerability assessment result of IoT devices:

 Vulnerability assessment of printer			
No	Issue	Security level	Recommendation
1	No Password Protection: The web interface of the printer was not protected with passwords, and as a consequence any authorized or unauthorized user can access the web interface of printer.	 High	Enable password protection on web interface of printer.
2	SNMP Protocol Version Detected: SNMP protocol is found enabled on the printer for managing devices on IP networkers. SNMPv1/v2 is an unsecure protocol, and it cannot ensure the confidentiality, integrity, and Authentication of data exchanged between printer and users.	 Vulnerability	Disable or remove SNMPv1/2c authentication and Use SNMP version 3 authentication which provides additional security features.
3	SNMP Agent Default Community Name (public): The default name for SNMP community string on the printer is PUBLIC. This information can be guessed by attacker to gain more knowledge about the printer.	 High	Change the default community string.




Vulnerability assessment of printer

No	Issue	Security level	Recommendation
4	SSL Version 2 and 3 Protocol Detection: The printer accepts connections encrypted using SSL 2.0 and/or SSL 3.0. which is affected by several cryptographic flaws. This is can be a result of a man-in-the-middle or decrypt the communications between the affected printer and users.	 High	Use TLS 1.1 with recommended cipher suites only for ensuring communication security.
5	SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE): Since the printer supports SSLv3, which makes it vulnerable to Padding Oracle on Downgraded Legacy Encryption now as POODLE. The attacker tricks the browser into connecting with SSLv3 and gain access to encrypted communication between a printer and users.	 Medium  5 Vulnerability	Disable SSL 2.0 and 3.0. by Consult the application's documentation to avoid this vulnerability.
6	SMB Signing Disabled or SMB Signing Not Required: the printer does not seem to be using SMB (Server Message Block) signing which is a security mechanism to help improve the security of the SMB protocol. When SMB signing is disabled on both the client and server SMB sessions are unauthenticated which can allow man-in-the-middle attacks against the SMB server.	 Medium  3 Potential Vulnerability	Enabled SMB sign or it is recommended that SMB signing is enabled and required.
7	Readable SNMP Information: Read-access to all SNMP information can give unauthorized users an incredible amount of valuable and sensitive information about your network.	 3 Vulnerability	Block access to SNMP services at the network perimeter or restrict all SNMP access to separate management networks that are not publicly accessible.
8	SSL Self-Signed Certificate: The certificate is not signed by a known certificate authority. This can establish a man-in-the-middle attack against the printer.	 Medium	Purchase or generate a proper certificate for this service.
9	HTTP Security Headers: The following HTTP security headers were not enabled in the web interface of the printer which are X-Frame-Options Header Missing, X-XSS-Protection header and X-Content-Type-Options Header. HTTP security headers protect web applications from various types of web application attacks.	 2 Vulnerability  Low	Enable HTTP security headers on all web pages of printer web interface.
10	Application Error Disclosure: Application Error Disclosure: The login interface of the printer shows an error/warning message that may disclose sensitive information in case of failed login, which helps attackers in guessing user names of printer's users easily.	 Medium	Implement password checker at the stage of user accounts creation. Allow complex passwords only.





Vulnerability assessment of Smart plug

No	Issue	Security level	Recommendation
1.	Non-Zero Padding Bytes Observed in Ethernet Packets: The service detected that the small packets from the host were padded to the minimum size using non-zero padding bytes which may be exploited to fingerprint the Ethernet cards and device drivers.	 Vulnerability	Contact the vendor of the Ethernet cards and device drivers for the availability of a patch.






Vulnerability assessment of Amazon Fire TV

No	Issue	Security level	Recommendation
1.	HTTP Security Headers: HTTP protocol provides security headers for the security of web applications, but it was observed that these headers were not configured on the management interface of the Fire TV. The headers that were not configured include X-frame-options header, X_XSS protection header and X-content-type- options header.	 Vulnerability  Low	Enable HTTP security headers on of the Fire TV.



Vulnerability assessment of Smart TV

No	Issue	Security level	Recommendation
1.	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE: The Portable SDK for UPnP TV (libupnp) library contains multiple buffer overflow vulnerabilities. Smart home TV use (libupnp) may accept UPnP queries over the WAN interface, thus exposing this vulnerability allow an unauthenticated hacker to execute arbitrary code on the device or cause a denial of service.	 Critical	Apply an update to libupnp version 1.6.18 or later.
2.	SSL Self-Signed Certificate: The certificate is not signed by a known certificate authority. This can establish a man-in-the-middle attack against the Smart TV.	 Medium	Purchase or generate a proper certificate for this service.
3.	SSL Certificate Cannot Be Trusted: This can happen in three various ways: <ol style="list-style-type: none"> 1. Self-signed certificate. 2. The certificate is not valid at the time of the scan. 3. The certificate may contain a signature didn't match the certificate's information or could not be verified. This could cause man in the middle attacks against the remote host.	 Medium	Purchase or generate a proper certificate for this service.