Cybersecurity Tools

Harry E. López Ubinas
Master in Computer Engineering
Dr. Jeffrey Duffany
Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— The goal of this project is to analyze the effectiveness of different Cybersecurity tools. It will test different techniques such as vulnerability scanning on the network, Wi-Fi hacking, and password cracking.*

Key Terms *— cybersecurity, password cracking, vulnerability scanning, wi-fi-hacking*

INTRODUCTION

Nmap, which stands for Network Mapper, is an open- source tool widely used for network discovery and security auditing. Some of its features are:

- Host discovery
- Port scanning
- Service and version detection
- Operating system detection
- Network mapping

METHODOLOGY

Host Discovery

Host discovery, which is known as "ping scanning," is used in Nmap to see an available host such as computers and devices on a network.

A host discovery scan was ran on the network, which resulted in 6 hosts (figure 1). There are three routers, one printer, and one laptop connected to network 192.168.0.0/24.

```
nmap -sn 192.168.0.1/24

Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 11:45 Eastern Daylight Time
Nmap scan report for 192.168.0.1
Host is up (0.0070s latency).
MAC Address: 24:94:CB:A2:37:5C (Arris Group)
Nmap scan report for 192.168.0.2
Host is up (0.0060s latency).
MAC Address: 34:98:B5:47:AF:8C (Netgear)
Nmap scan report for 192.168.0.3
Host is up (0.096s latency).
MAC Address: 40:B0:34:92:A2:A9 (Hewlett Packard)
Nmap scan report for 192.168.0.6
Host is up (0.083s latency).
MAC Address: D8:12:65:35:C2:71 (Chongqing Fugui Electronics)
Nmap scan report for 192.168.0.252
Host is up (0.0026s latency).
MAC Address: 00:00:CA:01:02:03 (Arris Group)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 7.91 seconds
```

Figure 1
Host discovery scan

Port Scanning

The next step is port scanning, which is critical to identifying open ports on a host.

Figures 2 and 3 show the open ports with their current state and service. This information is valuable because it offers partial information required to start looking more in depth into the ports [1]. SYN scan is the default and most popular scan option, as it quickly scans thousands of ports per second on a fast network.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 11:11 Eastern Daylight Time
Warning: 192.168.0.6 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.0.6
Host is up (0.064s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE
135/tcp open     msrpc
139/tcp open     netbios-ssn
445/tcp open     microsoft-ds
800/tcp filtered mdbs_daemon
MAC Address: D8:12:65:35:C2:71 (Chongqing Fugui Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1728.18 seconds
```

Figure 2
192.168.0.6 open ports

```
nmap -sS 192.168.0.3

Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 12:16 Eastern Daylight Time
Nmap scan report for 192.168.0.3
Host is up (0.014s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
631/tcp  open  ipp
8080/tcp open  http-proxy
9100/tcp open  jetdirect
9220/tcp open  unknown
MAC Address: 40:B0:34:92:A2:A9 (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
```

Figure 3
192.168.0.3 open ports

Most services use the TCP protocol, but UDP services are common, and it is always beneficial to run them for vulnerability scanning [1]. UDP scanning is generally slower and more difficult than TCP. See figures 4 and 5.

```
nmap -sU 192.168.0.6

Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 12:21 Eastern Daylight Time
Nmap scan report for 192.168.0.6
Host is up (0.076s latency).
Not shown: 988 closed udp ports (port-unreach)
PORT      STATE         SERVICE
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open|filtered isakmp
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
5050/udp  open|filtered mmcc
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
18449/udp open|filtered unknown
34855/udp open|filtered unknown
46836/udp open|filtered unknown
58178/udp open|filtered unknown
MAC Address: D8:12:65:35:C2:71 (Chongqing Fugui Electronics)
```

Figure 4

192.168.0.6 UDP Port Scanning

```
nmap -sU 192.168.0.3

Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-27 12:42 Eastern Daylight Time
Nmap scan report for 192.168.0.3
Host is up (0.029s latency).
Not shown: 995 closed udp ports (port-unreach)
PORT      STATE         SERVICE
137/udp   open          netbios-ns
161/udp   open          snmp
3702/udp open|filtered ws-discovery
5353/udp open          zeroconf
5355/udp open|filtered llmnr
MAC Address: 40:B0:34:92:A2:A9 (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 88.17 seconds
```

Figure 5

192.168.0.3 UDP Port Scanning

Service and Version Detection

Being aware of the version is beneficial for vulnerability scanning, which assists in knowing specific vulnerabilities that may affect each version, tailoring exploits, and improving security measures.

Based on the search for service and version, a printer with various ports open is shown (figure 6), while there are a few open ports running Microsoft NetBIOS and Microsoft Windows RPC (figure 7).

```
Nmap scan report for 192.168.0.3
Host is up (0.016s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
80/tcp   open  http       HP OfficeJet 4650 series printer http config (Serial TH72I4B14N0662)
443/tcp  open  ssl/http   HP OfficeJet 4650 series printer http config (Serial TH72I4B14N0662)
631/tcp  open  http       HP OfficeJet 4650 series printer http config (Serial TH72I4B14N0662)
8080/tcp open  http       HP OfficeJet 4650 series printer http config (Serial TH72I4B14N0662)
9100/tcp open  jetdirect?
9220/tcp open  hp-gsg     HP Generic Scan Gateway 1.0
MAC Address: 40:B0:34:92:A2:A9 (Hewlett Packard)
Service Info: Device: printer; CPE: cpe:/h:hp:officejet_4650_series
```

Figure 6

192.168.0.3 service and version

```
Nmap scan report for 192.168.0.6
Host is up (0.0040s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: D8:12:65:35:C2:71 (Chongqing Fugui Electronics)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 964.42 seconds
```

Figure 7

192.168.0.6 Service and Version

Operating System Detection

The -O command in Nmap was used to find operating systems utilized by equipment on specific IP addresses.

The scan showed no exact matches for host (figure 8), which is expected for a printer. It showed that the operating system is Microsoft Windows 10 (figure 9).

```
MAC Address: 40:B0:34:92:A2:A9 (Hewlett Packard)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=3/27%OT=80%CT=1%CU=44376%PV=Y%DS=1%DC=D%G=Y%M=40B034%T
OS:M=66049571%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=10A%TI=RI%TS=A
OS:)SEQ(CI=I%II=I)SEQ(SP=102%GCD=1%ISR=10A%TI=RD%CI=I%II=I%TS=D)SEQ(SP=102%
OS:GCD=1%ISR=10A%TI=RI%CI=RI%TS=A)OPS(O1=M5B4NW0NNT11%O2=M578NW0NNSNNT11%O3
OS:=M280NW0NNT11%O4=M5B4NW0NNSNNT11%O5=M218NW0NNSNNT11%O6=M109NNSNNT11)WIN(
OS:W1=21F0%W2=2088%W3=2258%W4=21F0%W5=20C0%W6=209D)ECN(R=Y%DF=N%T=40%W=2238
OS:%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R
OS:=N)T4(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%
OS:DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=FF%CD=S)

Network Distance: 1 hop
```

Figure 8

192.168.0.3 OS detection

```
MAC Address: D8:12:65:35:C2:71 (Chongqing Fugui Electronics)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 961.18 seconds
```

Figure 9

192.168.0.6 OS detection

Network Mapping

An overall view of the devices on the network, connections among them, and the services they are offering can be seen. Host discovery, port scanning, version, service detection, and operating system detection were performed.

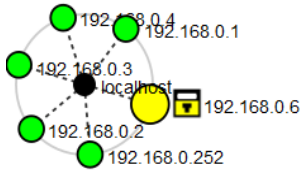


Figure 10

Network topology

Figure 10 shows a star topology because each node is connected to a central hub. This information could seem unimportant, but it assists in vulnerability scanning of the system.

Vulnerable Devices

After an extensive vulnerability scanning, possible vulnerable devices may be analyzed. After watching port opens and their available services (figures 6 and 7), it was noticed that the printer has various ports open and that the service is http, which means direct connection would yield no issues.

The interface printer, which is connected in the network, is visible (figure 11). Since http is unsecure, connecting to was simple by typing and IP address into the web browser. Information such as ink levels, scan, fax, web services, network, tools, and setting may be seen.

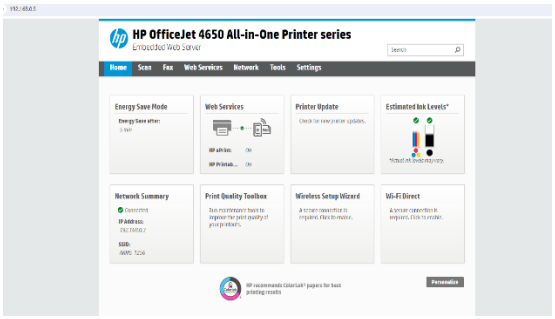


Figure 11
HP OfficeJet

It was possible to enter the https service directly to the password settings (figure 12). It was noticed that the printer is still on default settings with the username "admin." We had the option to set a new password. We ere able to print test pages and obtain information about recent usage from the printer itself.

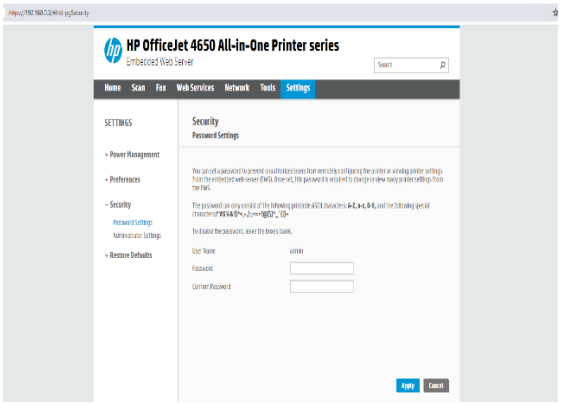


Figure 12
Password settings

We were able to capture the name of the printer network and the password (figure 13). This is valuable information, since it enables for remote printing through this printer from any device. Because the printer is unsecured, with this information, all we would need is to be in range of the device to be able to use it.

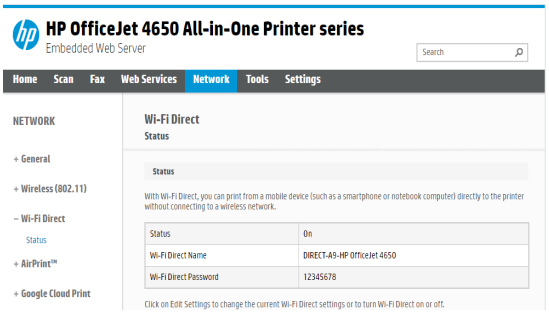


Figure 13
Wi-fi direct

Password Cracking

We attempted to crack a password-protected file for a case that forensic department cannot access. John the Ripper was used to attempt to crack passwords for seven Word documents and one video document.

We attempted to crack the passwords of two Word documents found in the Business folder that were password-protected (figure 14).

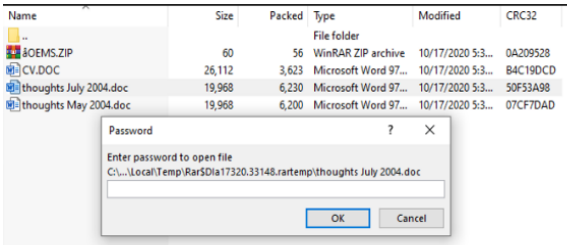


Figure 14
Password-protected Word documents

The password-cracking attempt was done with John the Ripper, primarily a password cracker used during pen-testing exercises that can help staff spot weak passwords and poor password policies [2].

An "office2john.py" command was used to create a hash from the password-protected file (figure 15). All that was I needed was the location of the document, and the program generated the hash file "hashfile1."

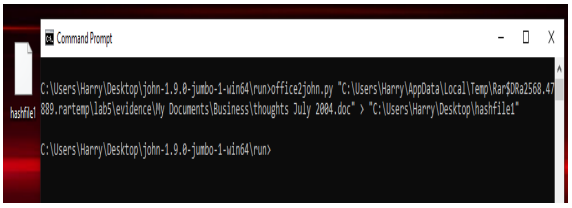


Figure 15
Generating the hash file

John the Ripper was used to decode the generated hash file 15, with which we obtained the password "smoke" for the document named "thoughts July 2004" and the password "fire" for the document named "thoughts May 2004" (figures 16 and 17).

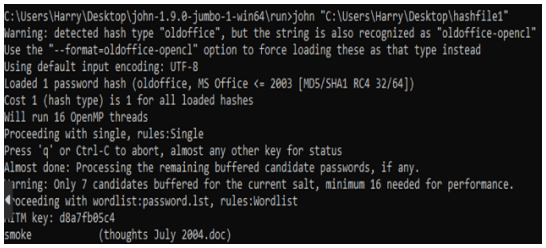


Figure 16
Decoding hash file 1

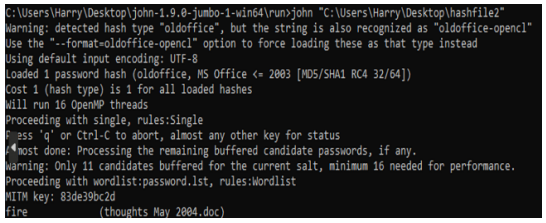


Figure 17
Decoding hash file 2

We were able to open both documents. Documents show the creator's displease with the government, firemen, and insurance companies, claiming all they do is collect one's money and that people need to start "waking up."

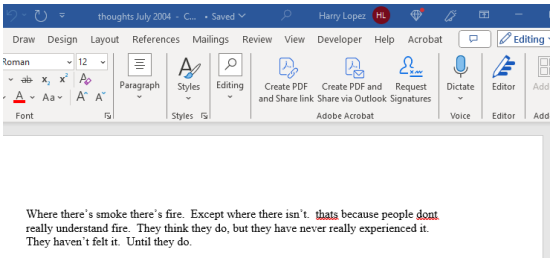
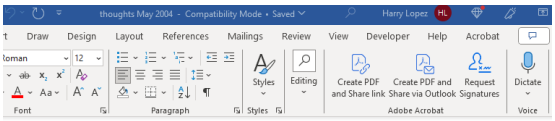


Figure 18
Document named "thoughts July 2004.doc," opened



The problem with these government people is like "firemen" is that they sit around all day watching their big screen tvs that my tax dollars bought. They're supposed to be fighting fires but they're too busy burning up my money. What they need is something to do. They need to burn a few more calories instead. What about that. What about these insurance guys too. All they do is collect your money every month. Hows about if they start paying out a little bit more. People need to wake up.

Figure 19
Document named "thoughts May 2004.doc," opened

The same process using John the Ripper to attempt and get passwords was repeated with two new password-protected documents (figure 20).

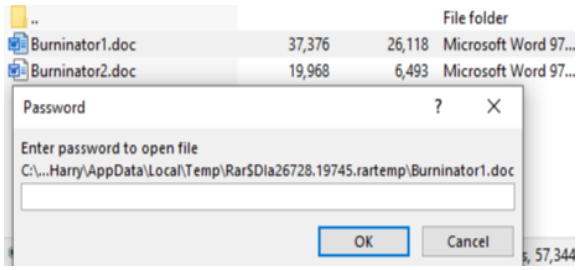


Figure 20
Password-protected documents

Hashes were generated for documents "Burninator1.doc" and Burminator2.doc." Figure 21 shows both hashes values containing the passwords. Figure 22 shows John the Ripper's crack process.

Figure 21
Generating the hashes

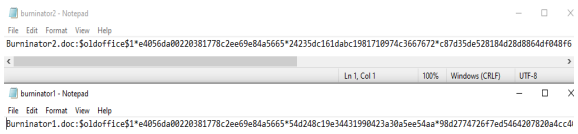


Figure 22
Password crack process

John the Ripper successfully hashed the files and cracked the passwords. Both documents had the same password: "trogdor" (figures 23 and 24).

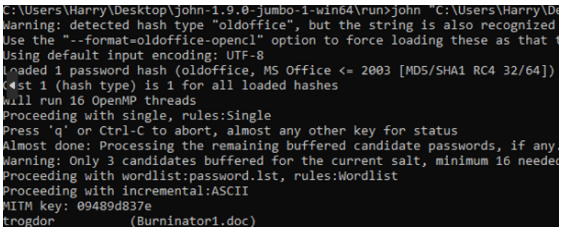


Figure 23
Decoding Burninator1.doc

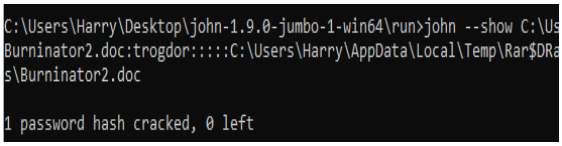
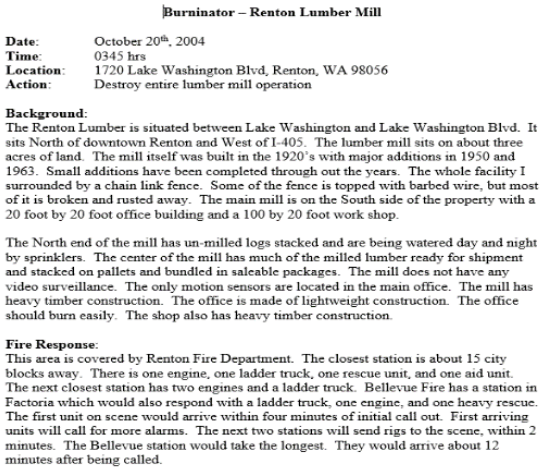


Figure 24
Decoding Burninator2.doc

Once opened, the "Burninator1" document reveals a background on a Renton Lumber Mill, information on a local fire response team, and timelines to burn lumber and an evacuation plan (figure 25).



Burninator – Renton Lumber Mill

Date: October 20th, 2004
Time: 0345 hrs
Location: 1720 Lake Washington Blvd, Renton, WA 98056
Action: Destroy entire lumber mill operation

Background:
The Renton Lumber is situated between Lake Washington and Lake Washington Blvd. It sits North of downtown Renton and West of I-405. The lumber mill sits on about three acres of land. The mill itself was built in the 1920's with major additions in 1950 and 1963. Small additions have been completed through out the years. The whole facility I surrounded by a chain link fence. Some of the fence is topped with barbed wire, but most of it is broken and rusted away. The main mill is on the South side of the property with a 20 foot by 20 foot office building and a 100 by 20 foot work shop.

The North end of the mill has un-milled logs stacked and are being watered day and night by sprinklers. The center of the mill has much of the milled lumber ready for shipment and stacked on pallets and bundled in saleable packages. The mill does not have any video surveillance. The only motion sensors are located in the main office. The mill has heavy timber construction. The office is made of lightweight construction. The office should burn easily. The shop also has heavy timber construction.

Fire Response:
This area is covered by Renton Fire Department. The closest station is about 15 city blocks away. There is one engine, one ladder truck, one rescue unit, and one aid unit. The next closest station has two engines and a ladder truck. Bellevue Fire has a station in Factoria which would also respond with a ladder truck, one engine, and one heavy rescue. The first unit on scene would arrive within four minutes of initial call out. First arriving units will call for more alarms. The next two stations will send rigs to the scene, within 2 minutes. The Bellevue station would take the longest. They would arrive about 12 minutes after being called.

Figure 25
Document named "Burminator1.doc," opened

Once opened, the "Burninator2" document reveals the title "Burninator – Ballard Lumber Mill."

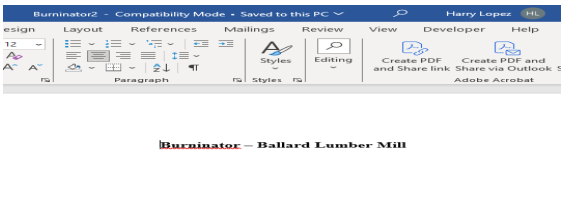


Figure 26
Document named "Burminator2.doc," opened

Another document to password-crack was also a Word document in the Documents folder named "PRKs_world.doc" (figure 27). As with the previous documents, John the Ripper was used to generate the hash that would be used to crack the password and gain access to the document.

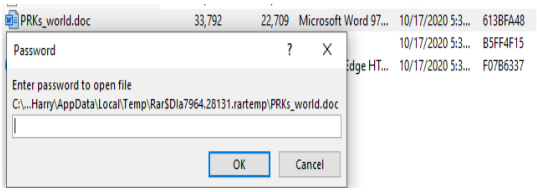


Figure 27
Password-protected document

John the Ripper was given a directory of where protected document was, and it generated the hash file that will be used crack the password (figure 28).

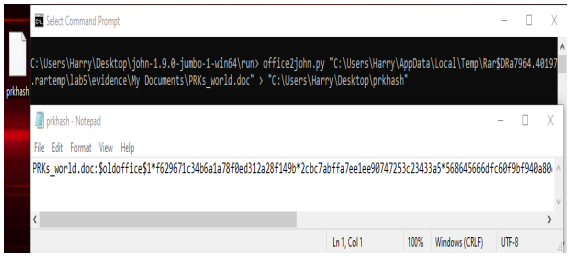


Figure 28
Generating the hashes

The attempt to crack the document's password with the hash file generated by Jack the Ripper was successful (figure 29). The password for the document was "art."

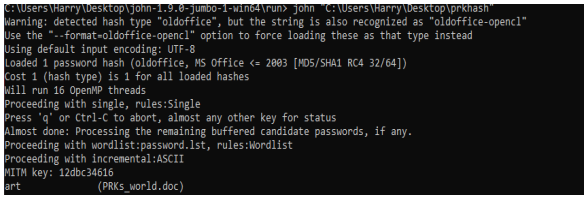
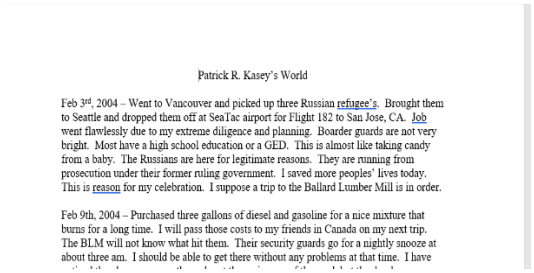


Figure 29
Decoding the hashes

Once opened, the document shows proof of a series of activities that suggest criminal behavior, specifically arson (figure 30).



Patrick R. Kasey's World

Feb 3rd, 2004 – Went to Vancouver and picked up three Russian refugee's. Brought them to Seattle and dropped them off at SeaTac airport for Flight 182 to San Jose, CA. Job went flawlessly due to my extreme diligence and planning. Boarder guards are not very bright. Most have a high school education or a GED. This is almost like taking candy from a baby. The Russians are here for legitimate reasons. They are running from prosecution under their former ruling government. I saved more peoples' lives today. This is reason for my celebration. I suppose a trip to the Ballard Lumber Mill is in order.

Feb 9th, 2004 – Purchased three gallons of diesel and gasoline for a nice mixture that burns for a long time. I will pass those costs to my friends in Canada on my next trip. The BLM will not know what hit them. Their security guards go for a nightly snooze at about three am. I should be able to get there without any problems at that time. I have

Figure 30
Document named "PRKs_world.doc," opened

A password-protected video (figure 31) was cracked by John the Ripper. The password was "firefly." I utilized the command "zip2john" for the video (figure 32).

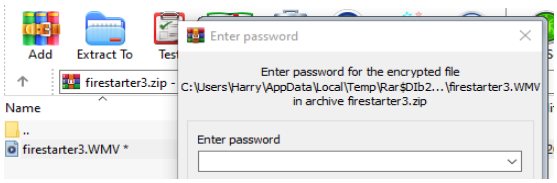


Figure 31
Password-protected document

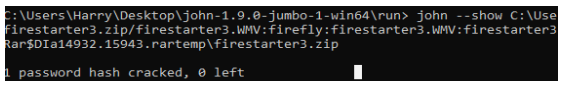


Figure 32
Decoding the hashes

The password-protected video is 3 minutes and 22 seconds long and is the music video of the song "Firestarter" by Gene Simmons, which is about being a fire enthusiast and arson.

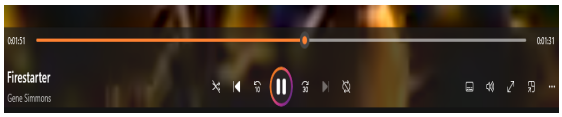


Figure 33
Media player controls for the password-protected video

Wi-Fi Hacking

For wi-fi hacking, some from our own networks will be selected to attempt to crack their passwords using Aircrack-ng on Kali Linux and a long-range USB adapter to capture surroundings networks. A printer network and Liberty modem will be targeted. Some topics include:

- Scanning
- Choosing network
- Attacking the network
- Wireshark

Monitor mode is the mode whereby a user's card can listen to every packet in the air (figure 33) [3]. Normally a card will only "hear" packets addressed to the user.

Figure 33
Monitor mode

At the scanning stage, there were multiple networks found using the airodump-ng command in combination with an adapter on monitor mode. This yielded the MAC address, signal strength, beacons, number of data packets, the channel where AP is broadcasting, network speed, encryption, cipher, authentication protocol, and the name of the wi-fi signal. From this scan, we know most of them are running WPA2 (figure 34).

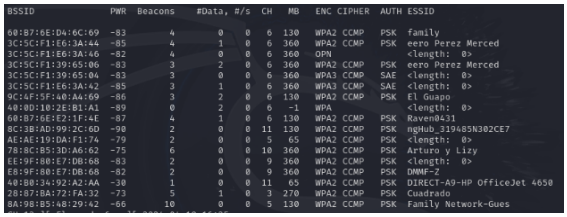


Figure 34
Available networks

Upon choosing a network, the OfficeJet device was chosen, showing the actual network and the devices connected to that network (figure 35).

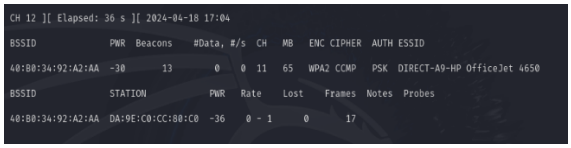


Figure 35
OfficeJet and devices

To attack the network, Aircrakc-ng is started to capture files (figure 36) and save them to a folder called "OfficeJet" that will be used later. The

purpose of Airodump-ng is to capture 4-way authentication handshakes [3].

Figure 36
Capturing the files

This step is optional [3]. This will send a message to the wireless AP saying that it is no longer associated with the AP. The client's reauthentication (figure 37) generates the 4-way handshake.

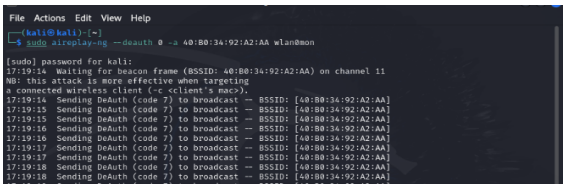


Figure 37
Deauthentication

The WPA handshake was successful (figure 38), so we moved in further.

Figure 38
Handshake

I used Wireshark to open the file shown on figure 36. That file will contain the information on the handshake between the devices.

The handshake between the devices (figure 39) and the WPA key data (figure 40) will be used to attempt to hack the wi-fi signal.

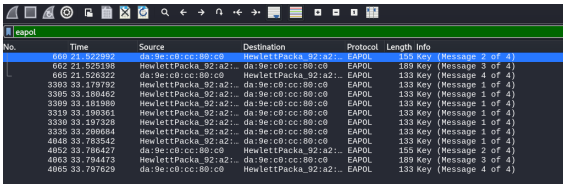


Figure 39
Handshakes and WPA key data

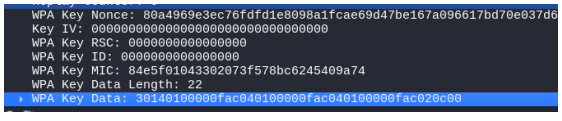


Figure 40
Handshakes and WPA key data

Aircrack-ng was used on the file that had been stored in the handshake to successfully obtain the network password against a wordlist "rockyou.txt" (figure 41) and found the key "12345678" (figure 42). With this information, access was gained.

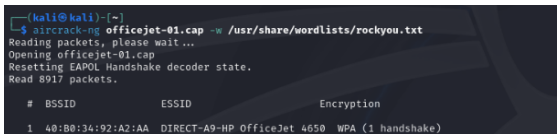


Figure 41
Aircrack-ng

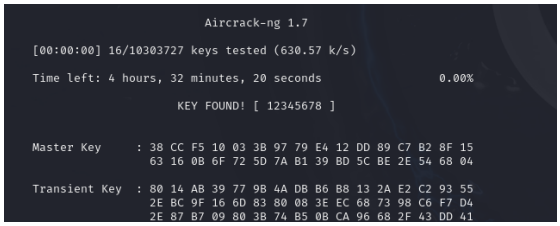


Figure 42
Password obtained

Modem Hacking

A different network was chosen to attack: a Liberty modem that uses WPA2 encoding. Usually these take a little longer to crack, since the pre-shared keys are longer.

Figure 43 shows the new target with the information needed. The same steps as with the OfficeJet were followed.

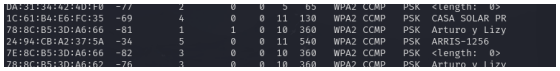


Figure 43
Arris-1256

The deauthentication process was started (figure 44). This process is done to capture a handshake between the devices connected to the network. The handshake was captured successfully (figure 45).

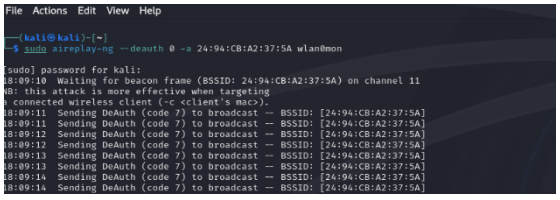


Figure 44
Deauthentication

Figure 45
Handshake

A pre-shared key of the Liberty modem "Arris-1256" was obtained (figure 46). For the most part, these modems have a 12-character password consisting of number and letters.

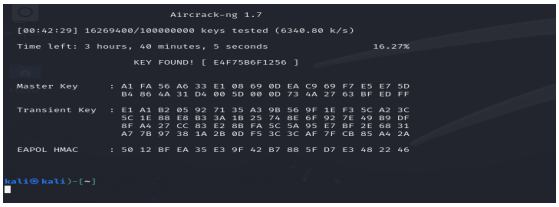


Figure 11
Obtaining the password

CONCLUSION

This project focused on the effectiveness of cybersecurity tools. We dove into their capabilities in various areas, such as password cracking, vulnerability scanning, and wi-fi hacking. We were able to explore practical applications of standard tools such as Aircrack-ng, Nmap, and John the Ripper.

Vulnerability Scanning

Nmap was used to demonstrate how the tools could be leveraged to perform various security and network auditing functions. This includes port scanning, host discovery, and OS version with service detection. In addition, we showed different components of the tool that could help identify potential threats.

Wi-Fi Hacking

We were able to showcase the ability of Aircrack-ng to analyze the security of wi-fi networks. We also demonstrate how easily networks could be compromised due to low security standards. We also emphasized on the importance of the need for more robust measures to mitigate unwanted access.

Password Cracking

John the Ripper was used for showing how to crack password-protected files. It was easy to break into the documents because their passwords were short and contained no special characters. This scenario also highlights the importance of this tool for cybersecurity and forensics.

The project conclusively shows that cybersecurity tools such as Nmap, John the Ripper, and Aircrack-ng are effective for identifying and exploiting vulnerabilities in digital networks. However, effectiveness of these tools is limited by the user's knowledge and are double-edged: while they are beneficial tools for network defense, they could also be used for harm. This highlights the critical importance of for cybersecurity experts to keep up to date in their knowledge on security methodologies.

REFERENCES

[1] Nmap.org, "Port scanning techniques." Accessed March 27, 2024. Available: https://nmap.org/book/man-port-scanning-techniques.html

[2] M. Buckbee, "How to use John the Ripper: tips and tutorials," Varonis, December 21, 2022. Available: https://www.varonis.com/blog/john-the-ripper

[3] darkAudax (author), "Tutorial: How to Crack WPA/WPA2," Aircrack-ng, March 7, 2010. Available: https://www.aircrack-ng.org/doku.php?id=cracking_wpa