Cybersecurity Tools

Author: Harry E Lopez Ubinas
Advisor: Dr. Jeff Duffany
Computer Science

Abstract

This projects presents a comprehensive examination of various cybersecurity tools such as Nmap for vulnerability scanning, John the Ripper for password cracking, and Aircrack-ng for Wi-Fi hacking. Purpose was to evaluate effectiveness of such tools in detecting and mitigating threats within network environment.

Introduction

Cybersecurity is constantly evolving, with new threats looming frequently. This project provides an analysis of several cybersecurity tools designed to identify and mitigate vulnerabilities. Trough efficient evaluation , we have explored how these tools can be utilized effectively to strengthen cybersecurity defenses and respond to the vigorous daily challenges posed by hackers and spiteful entities.

Background

This research dives into the mechanism and application of various cybersecurity tools such as Nmap, John the Ripper, and Aircrack-ng. Each tool Nmap for network scanning, John the Ripper for password cracking, and Aircrack-ng for Wi-Fi security. The project contextualizes the importance of these tools within cybersecurity domain and discusses their operational.

Problem

Despite widespread adoption, the real-world effectiveness of cybersecurity tools remain under-examined. This project addresses this gap by testing this tools against typical security that individuals face. By doing so, it aims to focus both strength and weaknesses of this tools, fostering a comprehensive understanding of their functionality.

Methodology

Methodology of this research was structured test the efficacy of the tools under control conditions within my own network and multiple devices and security setting.

1. Setup and Environment Preparation: For each tool, a test environment was created that included devices, documents, and network configuration, to include Kali Linux.

2. Execution of tools:

- Nmap was used on control environment to test my own network and devices to perform host discovery, port scanning, service and version detection, and OS detection on all devise connected to the network, Nmap utilized was on windows platform.

Methodology

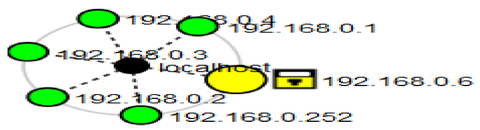


Figure 10: star topology from a network scan using Nmap tool, that shows multiples nodes connected within a private network, and tallow node that indicates a different device such as printer.

```
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:B8:34:92:A2:A9 (Hewlett Packard)

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

Figure 2: shows a TCP SYN scan on target IP address 192.168.0.3. showing multiple ports open that includes http/https which are good one for gaining access to the device.

- John the Ripper was used from within windows OS to crack password of protected file that was needed to be cracked for an arson case.

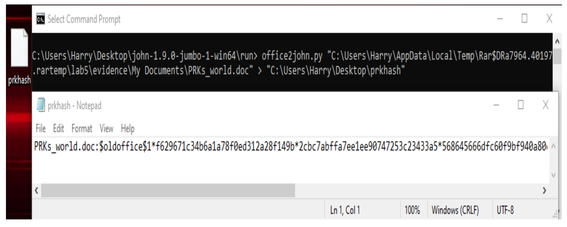


Figure28: generating the hash file for a specific document currently password protected, hash file is utilized with john the ripper to attempt and crack password.

```
C:\Users\Harry\Desktop\john-1.9.0-jumbo-1-win64\run> john "C:\Users\Harry\Desktop\prkhash"
Warning: detected hash type "oldoffice", but the string is also recognized as "oldoffice-opencl"
Use the "--format=oldoffice-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (oldoffice, MS Office <= 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type) is 1 for all loaded hashes
Will run 16 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
Proceeding with incremental:ASCII
MITM key: 12dbc34616
art              (PRKs_world.doc)
```

Figure29: shows john the ripper successfully cracking the password for the specific hash “art” using 16OpenMP threads for the cracking process.

- Aircrack-ng was employed on Linux within a virtual machine to assess the security of the Wi-Fi networks around the area, assessing the encryption method and targeting multiple devices to capture and cracking WPA handshakes.

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC CIPHER  AUTH ESSID
60:B7:6E:D4:6C:69  -83        4        0    0   6  130  WPA2 CCMP   PSK  family
3C:5C:F1:E6:3A:A4  -85        4        1    0   6  360  WPA2 CCMP   PSK  eero Perez Merced
3C:5C:F1:E6:3A:A6  -82        4        0    0   6  360  OPN              <length:  0>
3C:5C:F1:29:65:06  -83        3        2    0   6  360  WPA2 CCMP   PSK  eero Perez Merced
3C:5C:F1:39:65:04  -83        3        0    0   6  360  WPA3 CCMP   SAE  <length:  0>
3C:5C:F1:E6:3A:42  -85        3        1    0   6  360  WPA3 CCMP   SAE  <length:  0>
9C:4F:5F:A0:AA:69  -86        3        2    0   6  130  WPA2 CCMP   PSK  El Guapo
40:0D:10:2E:B1:A1  -89        0        2    0   6   -1  WPA              <length:  0>
60:B7:6E:E2:1F:4E  -87        4        1    0   6  130  WPA2 CCMP   PSK  Raven0431
8C:3B:AD:99:2C:6D  -90        2        0    0  11  130  WPA2 CCMP   PSK  ngHub_339485N302CE7
AE:AE:19:DA:F1:74  -79        2        0    0   5   65  WPA2 CCMP   PSK  <length:  0>
78:8C:B5:3D:A6:62  -75        6        0    0  10  360  WPA2 CCMP   PSK  Arturo y Lizy
7E:9F:80:E7:DB:68  -83        2        0    0   9  360  WPA2 CCMP   PSK  <length:  0>
E8:9F:80:E7:DB:68  -82        2        0    0   9  360  WPA2 CCMP   PSK  DMMF-Z
40:B8:34:92:A2:AA  -30        1        0    0  11   65  WPA2 CCMP   PSK  DIRECT-A9-HP OfficeJet 4650
28:B7:8A:72:FA:32  -73        5        1    0   3  270  WPA2 CCMP   PSK  Cuadrado
8A:98:B5:48:29:42  -66       10        0    0   5  130  WPA2 CCMP   PSK  Family Network-Gues
```

Figure 34: scanning the surrounding area with Wi-Fi-Adapter in monitor mode revealed multiple networks with important information such as mac address of access points, channel, encryption type, cypher which are critical information when trying to gain access to Wi-Fi.

Methodology

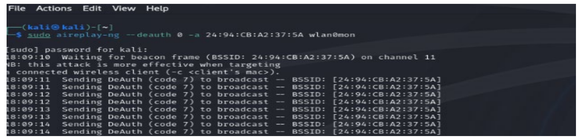


Figure 44: Deauthentication process to an access point that is used to be able to capture a handshake between devices and the access point in order to gain access.

Results and Discussion

- Nmap: Proved highly effective in discovering active devices and services on the networks. However, scans were at time slow, depending on the scan type and target device. The tool was particularly effective in detecting open ports and service that could potentially be exploited which is useful when assessing your network and doing penetration testing.

```
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: port scan on device 192.168.0.6 that almost 30 minutes to perform.

Figure 12: printer interface that was accessible due to port 80/443 being open. Giving access to add password since it was unsecured.

- John the Ripper: Demonstrated robust performance in cracking simple passwords protection quickly, the tool struggled with more complex passwords, highlighting the need for strong, multifaceted password in sensitive documents. Also, the tool interface could seem to be a little to complex to understand make it seem like an undesirable tool.

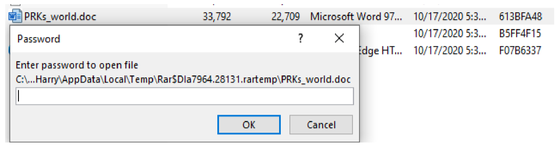
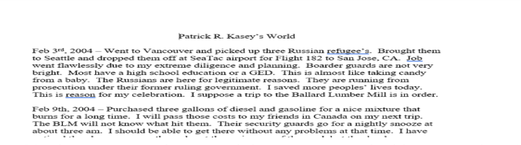


Figure 27: shows password protected document.



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: shows password protected document opened with password “art”. That indicates involvement in arson

Aircrack-ng: Successfully cracked WPA2 handshakes in environments with weak password protection, the tool’s effectiveness prove the necessity and importance of using strong complex password along with WPA3 security. Also, the tool worked outstanding at discovering multiple Wi-Fi networks

Results and Discussion

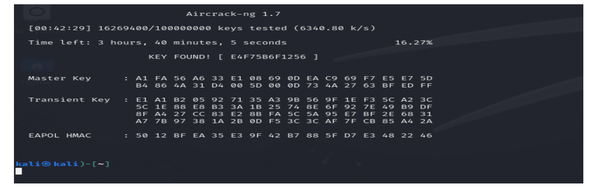


Figure 46: shows the successful crack of an access point, the scan took 42 minutes.

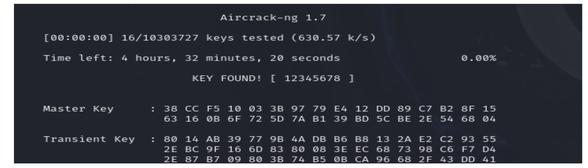


Figure 42: shows scan of a different AP with simpler password and length. Scan was instantly.

- Discussion: the project confirmed that while these tools are without a doubt powerful in penetrating security measures, their effectiveness heavily depends on the configuration of the targets systems and the complexity of the security they have in place. It is important to note that the nature of these tools could be used for securing system and for exploiting vulnerabilities, which bring ethical considerations.

Conclusion

This project demonstrates the crucial role that tools like nmap, John the Ripper, and Aircrack-ng play in identifying vulnerabilities and securing digital assets. Conclusion as follows:

- Nmap is effective for comprehensive network scanning, but can be time consuming
- John the Ripper excels at breaking simple passwords which underscore the need of strong passwords but could be challenging to use for inexperience users.
- Aircrack-ng ability to scan is outstanding, the ability to crack Wi-Fi passwords varies depends on how strong the password is, but is easy to learn.

Future work

- Utilizing more sophisticated simulation environment to test tools against more challenging systems
- Expanding the scope of tools examined
- Attacking more protected Wi-Fi networks with WPA3 and stronger password with special characters.

Acknowledgements

- Dr. Jeff Duffany

References

[1]. Lyon, “Port Scanning Techniques Nmap Network Scanning” Nmap.org,2019. [Online]. Available: https://nmap.org/book/man-port-scanning-techniques.html. [Accessed March. 27, 2024]

[2] M. Buckbee, “How to Use John the Ripper: Tips and Tutorials,” www.varonis.com, Dec 21, 2022. [Online]. Available: https://www.varonis.com/blog/john-the-ripper. [Accessed Apr. 5, 2024]

[3] Aircrack-ng, “Cracking WPA,” Aircrack-ng.org. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=cracking_wpa. [Accessed Apr. 18, 2024]