RESEARCH ARTICLE OPEN ACCESS

Osint Automation on A Full-Fledged Hacking Mobile Device Running Net-Hunter Os

Abu Wenisch P [1], Sathya Srinivas [2]

[1] M.Sc. Department of Computer Science and Engineering, Dr. MGR Educational and Research Institute, Chennai - India
[2] Faculty of Centre of Excellence in Digital Forensics, Dr. MGR Educational and Research Institute, Chennai - India

ABSTRACT
Open-source intelligence, or OSINT, is important for cybersecurity and threat intelligence. An operating system, called Net Hunter OS, has been designed for hacking and penetration testing. It is built on the Android platform and is considered quite impressive. It is a useful tool for automating Open-Source Intelligence (OSINT). With automation, we can make OSINT collection and analysis a lot easier. "We integrate scripts and tools to gather info from online sources, social media, databases, and websites." This way, security professionals do not have to waste their time on manual data retrieval. Focus on critical analysis and decision-making instead of mundane tasks to enhance productivity and efficiency. However, we need to be careful when automating OSINT tasks on Net Hunter OS. Data privacy and ethical guidelines are critical in business and academia. Following the best practices in data protection is crucial to maintaining trust and reputation among users. When done right, OSINT automation can be super helpful for threat hunting, vulnerability assessment, and digital forensics in cybersecurity. Compact hacking, easier hacking.

Keywords: - Net Hunter, OSINT, Social Engineering, Penetration Testing, Gathering Information.

I. INTRODUCTION

Smartphones have become important in today's society, revolutionizing how we communicate, work, and access information. These handheld devices have developed significantly since invented, combining many functions into a single, portable, and compact device [1]. A smartphone is essentially a pocket-sized computer that serves as a communication device and integrates various features like computing, communication, and accessing the internet making it part of our daily lives. The significant characteristic of smartphones is their ability to connect to the internet, enabling users to access a vast array of information, social media, and online services from anywhere and wherever they are.

A. Comparison of Performance: [Intel i5 10th gen VS Snapdragon 855+]

It is challenging to do a comparison between an Intel Core i5 10th Gen processor and a Snapdragon Gen 1 as these components are designed for different types of devices and have different architectures, use cases, and purposes. However, the benchmarking from different platforms proves that Snapdragon 855+ has better processing and performance than the Intel i5 10th gen.

B. Net Hunter OS:

Net Hunter OS, short for Net Hunter Offensive Security, is a specialized mobile penetration-testing platform based on the Android operating system. Developed by Offensive Security, the same organization behind the famous Kali Linux distribution for desktop computers, Net Hunter OS was designed to bring powerful hacking tools and capabilities to mobile devices that are compact and made for less computational tasks [2]. It provides security professionals, ethical hackers, and penetration testers with a portable and versatile platform for assessing and securing networks, ethical hacking, and cyber security purposes. With a range of pre-installed tools and a customizable environment, Net Hunter OS enable users to conduct security assessments, test vulnerabilities, and enhance the overall cybersecurity posture directly from their Android devices. This mobile penetration-testing platform has gained popularity for its flexibility, ease of use, and ability to transform everyday smartphones into a powerful tool for ethical hacking and security works.

C. OSINT (Open-Source Intelligence):

Open-source intelligence, commonly known as OSINT, is a powerful and evolving field that uses publicly available information to gather information about a person or an organization and analyze trends, and take decisions quickly. OSINT involves collecting, analyzing, and interpreting data from a wide range of open sources. These sources include but are not limited to websites, social media platforms, public records, news articles, academic publications, and any other publicly available information [3]. The primary goal of OSINT is to transform raw data into actionable intelligence. This intelligence can be used to understand and mitigate security threats, investigate criminal activities, and monitor geopolitical developments. OSINT provides a comprehensive view of a subject by aggregating information from different sources, enabling analysts to create a more accurate and holistic picture.

D. Maltego and its role in open-source intelligence (OSINT) and link analysis.

Maltego is a robust and widely used tool in the realm of open-source intelligence (OSINT) and digital forensics. Developed by Paterva, this software application stands out due to its capability of aiding professionals, from the law enforcement and intelligence sectors to private security firms and investigative journalists. With Maltego, users can visually

map out complex networks of interconnected entities, which might include individuals, organizations, websites, domains, social media profiles, IP addresses, and more.

II. REVIEW OF LITERATURE

Jason Swope ORCID Icon, Faiz Mirza, et al., [4] proposed space mission applications on the Snapdragon processor. In that model, they had benchmarked the variety of instrument processing and mission planning on a Qualcomm Snapdragon. Future space missions will process and analyze imagery on board as well as plan and act more autonomously, placing greater demands on flight computing. Traditional flight hardware provides modest computing power, even when compared to common laptop and desktop computers. A new generation of commercial-off-the-shelf (COTS) processors designed for commercial electronics such as cell phones and tablets, such as the Qualcomm Snapdragon, deliver significant computing in a small size, weight, and power; and they offer hardware acceleration in the form of graphics processing units and digital signal processors. We benchmark a variety of instrument processing and mission planning software on a Qualcomm Snapdragon system on a chip currently hosted by Hewlett Packard Enterprise's Spaceborne Computer-2 on board the International Space Station to highlight the potential of using embedded COTS processors on future space missions.

Faiz Mirza, Jason Swope et al., [5] proposed the benchmark of several space planning/scheduling applications on the Qualcomm Snapdragon 855 Handheld Development Kit (HDK), a high-performance embedded processor used in many mobile phones. They are flying 2 Snapdragon HDKs onboard the International Space Station (ISS) where they are hosted by the Spaceborne Computer-2 by Hewlett Packard Enterprise and linked by USB and 12V power delivery. They run computational benchmarks using three planners/schedulers that are used for several space missions: Multi-Mission Executive (MEXEC), Compressed Large-scale Activity Scheduling and Planning (CLASP), and M2020 Ground Scheduler (Co-pilot). They are comparing the Snapdragon performance to a performance baseline on Linux workstations. In addition, we are currently working on benchmarking the same applications on other space flight processors, such as the LEON4 Processor on the Sabretooth card, the LEON3 Processor on the Sphinx card, and the RAD750 processor.

Rajamäki, Jyri; Lahti et al., [6] proposed OSINT (Open source Intelligence) on the dark web. The Dark Web allows users to hide their identity while browsing or sending information, providing an ideal environment for transferring information, goods, and services with potentially illegal intentions. Therefore, Law Enforcement Agencies (LEAs) are interested in Open Source Intelligence (OSINT) on the Dark Web. LEAs need appropriate techniques to find darknet sites used by criminals. In this model, they had examined online child sexual exploitation and the various OSINT automation tools that can be exploited on the Dark Web. They consider OSINT on the Dark Web, paying attention to the challenges LEAs face when investigating crimes related to child abuse material (CAM). The biggest challenges are related to data storage and the criminal investigation itself. CAM may not be recorded or examined except by an LEA officer specifically designated and trained for this purpose. This proposed model examines how OSINT could be implemented without exposing researchers to the contents of CAM. The method could be to focus the inquiry on already known links and sites. This has challenges, but a bigger number of LEAs could carry out such an inquiry, and the storage of such data would not be illegal.

Anton O. Bryushinin, Alexandr V. Dushkin et al., [7] proposed the model, the automation of the information collection process by OSINT methods during the information security audit. In this model, they had done the penetration testing during the security auditing process for that they are using OSINT methods. With the help of Python programming language, they automated the process of information collection during the pen testing of the organization's security while auditing.

Andrea Tundis a, Samuel Ruppert b and et al., [8] had proposed the feature-driven method for Automating the Assessment of OSINT in the cyber threat sources. A method to automate the assessment of cyber threat intelligence sources and predict a relevance score for each source is proposed. Specifically, a model based on meta-data and word embedding is defined and experimented with by training regression models to predict the relevance score of sources on Twitter. The results evaluation show that the assigned score allows to reduce the waiting time for intelligence verification, based on its relevance, thus improving the time advantage of early threat detection.

Renas R. Asaad [9] proposed the penetration testing i.e., wireless network attacks method on the Kali Linux OS. In this model, the author mentioned the various wireless attacks. In this proposed model, the author has done all the types of wireless attacks on the Linux OS. In this model, the author used the brute-force attack for the online attacks and used straight attacks for the offline attacks. An example of a brute-force attack is the dictionary attack. Also in this proposed model, the author had dealt with the MD5 hash algorithm and SHA-512 algorithm in Linux. The entire wireless attacks and the process were done in the Linux OS.

SUCIU, George; ANWAR et al. [10], proposed the mobile application and wi-fi network security for e-learning platforms. In this proposed model they are trying to do identify and mitigate the risks when the users connect to a wi-fi public network and also analyze how the vulnerable devices are exposed by the cyber criminals. They also identify how the hackers can intercept the communications between mobile devices such as smartphones or tablets using public wi-fi

hotspots, namely a man-on-the-middle attack (MITM). In this proposed model, they concentrated on the security of the e-learning applications when connecting to a public wi-fi network at a hotel or a library. In the conclusion, they evaluated several open-source penetration testing tools that aid in the identification of vulnerabilities and proper security solutions for e-learning platforms in the context of using public wi-fi networks.

III. RESEARCH METHODOLOGY

The methodology used in this paper needs an Android smartphone running Net Hunter stably. First, enable the developer option on the smartphone device and enable USB debugging. Now connect the device to a computer. To flash the Net Hunter kernel to the Android device, download the latest kernel from the Kali website. Set up SDK platform tools on a computer to get Android Bootloader Interface. Within the Platform-tools directory, open Command Prompt. Now unlock the device from the OEM lock. Now download the OTA of the current OS running on the Android device. Extract the OTA file look for the bin file and move it to the Platform-Tools folder. Download the Payload-Dumper tool, extract it, and copy the exe file to the Platform-Tools Directory. Now run Payload-Dumper to extract the BOOT.img from the OTA File. Copy the BOOT.img to the Platform-tools directory. Now push the BOOT.img into the phone with ABD commands. Download Magisk from the browser, install it, and open Magisk. Inside the Magisk application insert the BOOT.img file as a patch file and flash it using Magisk. Now pull out the patched file onto the computer. Now with the ABD command reboot the bootloader of the smartphone and flashboot the Magisk-patched file onto the Android device. On the computer, download the Disable_Dm-verity and TWRP custom recovery. Move these two to the Platform-tools directory and push it to the Android device. Now on using ABD commands boot the TWRP in the Android phone. Once the phone is booted into TWRP. Install the disable software and flash the TWRP recovery. Once the Phone is rebooted into the Android, push the downloaded Net Hunter OS into the phone and flash it using the magisk just like the BOOT.img is flashed. By opening the Net Hunter APP check for patch updates and driver updates. Once the update is done, launch the Kex control menu to set up the Kex Server. After the Kex manager is done setting, launch the Kex server. The Kex manager must keep running the background to run Maltego. Maltego uses GUI-based operations to work and operate. Start the Kex server and Launch Kali Linux. In Kali Linux, Start the Maltego setup and configure it with APIs. Configuring the API from different domains and many different sources takes a lot of time and is very much necessary for Automating OSINT. After the Configuration of APIs Create a new project and import the category of initial data to the work plane or work graph sheet for automation. The initial data will be given a tag according to the type of information or data it is. With the configured API and publicly available data, Maltego will gather information about the given data and output it as a flow chart. Further details can be extracted from the options menu near the branched connected data with multiple APIs configured.

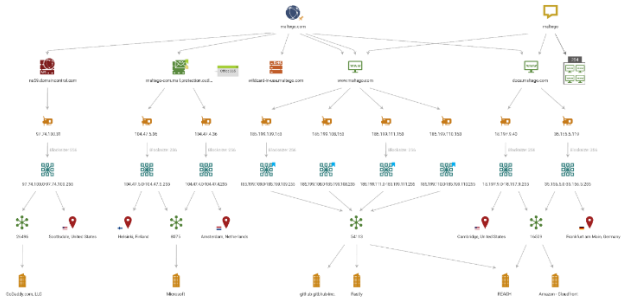

Fig. 1: The automated open-source information gathered and presented in a graph

IV. RESULTS

By conducting this project we can create a pocket/portable hacking machine that is powerful enough to run OSINT Automation or any other cyber security and cyber forensics software/program. This pocket hacking machine is a person's mobile phone running Net Hunter kernel, which enables a lot of advantages in comparison to a laptop or a PC. A mobile phone can be easily carried anywhere and a security analyst, a network engineer, an ethical hacker, and any other professional user who uses a laptop or PC for their work can use their mobile phone. In comparison, which can be easily carried, anywhere gives mobility. OSINT Automation can save time when an ethical hacker does social engineering to collect details about a person or a target when he/she is near them. Automation makes the user put less amount of effort, work, and time spent on the social engineering process saving time with better and faster results. It can swiftly sift through vast datasets, social media platforms, and public databases, gathering intelligence on targets, potential weaknesses, and entry points. The result is a formidable arsenal of actionable insights, empowering the user to launch targeted attacks, penetration testing, or reconnaissance missions. When Net Hunter is unleashed on a powerful phone, the result is akin to wielding a cyber-Swiss Army knife with the force of a cutting-edge computing powerhouse. This grants users an unprecedented level of mobility, agility, and versatility in their hacking endeavors. With that much of processing power and memory at their disposal, users can seamlessly run complex penetration testing tools, execute resource-intensive tasks, and manipulate vast amounts of data with lightning speed. Whether conducting reconnaissance missions, launching targeted attacks, or probing network defenses, the combination of Net Hunter and a high-performance phone elevates the capabilities of cybersecurity professionals and ethical hackers to new heights.

REFERENCES

[1] Szymoniak, Sabina, and Kacper Foks. "Open Source Intelligence Opportunities and Challenges–A Review." *Advances in Science and Technology. Research Journal* 18.3 (2024): 123-139.

[2] Aditya, Eka Wahyu, et al. "Smartphone penetration test: Securing Industry 5.0 mobile applications." *The Future of Human-Computer Integration*. CRC Press, 2024. 76-84.

[3] Akhtar, Zarif Bin. "Securing Operating Systems (OS): A Comprehensive Approach to Security with Best Practices and Techniques." (2024).

[4] Jason, Faiz. *Benchmarking Space Mission Applications on the Snapdragon Processor Onboard the ISS*. ARC.arc.aiaa, 2023.

[5] Mirza, Faiz, Jason Swope, and Steve Chien. "Benchmarking Planning Applications on the Qualcomm Snapdragon." (2021).

[6] Rajamäki, Jyri, and Parviainen,. Information & Security; Sofia Vol. 53, Iss. 1, (2022): 21-32. DOI:10.11610/isij.5302

[7] Muralidharan, M., Keshav Balaji Babu, and G. Sujatha. *"Pyciuti: A Python Based Customizable and Flexible Cybersecurity Utility Tool for Penetration Testing."* 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA). IEEE, 2023.

[8] Tundis, Andrea, et al. "*A Feature-driven Method for Automating the Assessment of OSINT Cyber Threat Sources.*" Computers & Security, vol. 113, 2022

[9] Asaad, Renas. (2021). *Penetration Testing: Wireless Network Attacks Method on Kali Linux OS*. Academic Journal of Nawroz University. 10. 7. 10.25007/ajnu.v10n1a998.

[10] Suciu, George et al. "*mobile application and wi-fi network security for e-learning platforms*." eLearning and Software for Education (2019)

[11] Tundis, Andrea, Samuel Ruppert, and Max Mühlhäuser. "*A feature-driven method for automating the assessment of osint cyber threat sources*." *Computers & Security* 113 (2022): 102576.

[12] Asaad, Renas R. "*Penetration testing: Wireless network attacks method on Kali Linux OS*." Academic Journal of Nawroz University 10.1 (2021): 7-12.

[13] Ungureanu, Gabriel Traian. "*Open-source intelligence (OSINT). The way ahead*." Journal of Defense Resources Management (JoDRM) 12.1 (2021): 177-200.

[14] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). *The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends*. IEEE Access, 8, 10282-10304.

[15] Singh, Glen D., and Sean-Philip Oriyano. *Hands-On Penetration Testing with Kali NetHunter: Spy on and protect vulnerable ecosystems using the power of Kali Linux for pentesting on the go*. Packt Publishing Ltd, 2019.

[16] Hernández, Martin, et al. "Open source intelligence (OSINT) as Support of Cybersecurity Operations: Use of OSINT in a Colombian Context and Sentiment Analysis*." Revista Vínculos Ciencia, tecnologíay sociedad* 15.2 (2018).

[17] Hernández, Martin, et al. "Open source intelligence (OSINT) as Support of Cybersecurity Operations: Use of OSINT in a Colombian Context and Sentiment Analysis." *Revista Vínculos Ciencia, tecnología y sociedad* 15.2 (2018).

[18] Weir, George RS. "*The limitations of automating OSINT: understanding the question, not the answer*." Automating Open Source Intelligence. Syngress, 2016. 159-169.

[19] Layton, Robert, and Paul A. Watters. "*Automating open source intelligence*." *Automating open source intelligence algorithms FOR OSINT* (2016): 1-17.

[20] Layton, Robert, and Paul A. Watters. Automating open source intelligence: algorithms for OSINT. Syngress, 2015.