Name: Gaurav Kumar Singh

Registration Number 19BCE2119

Course: Information Security Analysis and Audit (CSE3501)

Digital Assignment-1

Group Members: - Gaurav Kumar Singh 19BCE2119

Chirag Agrawal 19BCI0202

Penke Lohith Sasi Anvesh 19BCE2069

1. **DATA BREACHES**
   TOOL: Metasploit
   Platform: Windows, macOS, Linux
   Language: ---
   Link: https://www.metasploit.com
   FEATURES:
   - Data Breach is the intentional or unintentional release of data to an unauthorized environment. It is also known as a data spill
   - Personal data such as banking information, records, personal account keys, etc. can be compromised by unauthorized people causing distress and monetary loss in some cases too.
   - Data breaches are a huge part of black hat hacking and scams such as ransomware, therefore it is really important to test the systems for data breach resistance.

   PROS:

   - Metasploit framework is one of the most popular open-source penetration testing frameworks implying anyone can contribute towards its development which generally means it tends to be up-to-date.
   - It enables the penetration testers to develop and exploit code against target machines to detect and fix system vulnerabilities.
   - It includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. It is pre-installed in the Kali Linux OS.

   CONS:

   - Learning Metasploit is a challenging task and requires good knowledge of penetration testing and cyber security to start with.
   - It is very CLI-driven instead of GUI which makes it non-intuitive at times.
   - It is a very powerful tool, so not only is it challenging to learn, if not handled properly it can compromise the system itself.

2. **Integrating AI with Cybersecurity**
   TOOL: CyberSecTK
   Platform: Windows, macOS, Linux
   Language: Python

Link: https://github.com/sumendrabsingh/CyberSecTK-Library

FEATURES:

- Artificial Intelligence has immense potential in cybersecurity as they can learn from themselves and get better at tackling cybersecurity issues as time goes on.
- Security enthusiasts can get a lot of help from intelligent machines and technologies such as AI to work and protect an organization successfully.
- Artificial Intelligence can have the ability to recognize unknown threats making new exploits less effective.

PROS:

- CyberSecTK is a python library which in itself is a great tool for data science, data analytics, machine learning, and AI-related programming.
- It enables experts to implement a machine learning pipeline from beginning to the end enabling us to utilize the machine learning algorithms and train and test the models to find out what suits best for our task.

CONS:

- There are not a lot of opensource AI tools available currently since it is not a well-established public sentiment right now to use AI for cybersecurity hence the opensource tools available right now are on a very basic level without proper research into them because they are generally made by enthusiasts of cybersecurity.
- Since these tools are made by enthusiasts and analyzed by enthusiasts as well, it lacks proper tutorial and documentation for someone new to it.
- It is challenging for new users to learn or even find proper tutorials on these open-source software because they are not very commonly used and the ones with proper tutorials and documentation are usually owned by a big organization for their personal use and if we want to use them as a consumer, more often than not they are subscription-based services and closed-source as well making it difficult for other people to learn and experiment on them.

3. **AUTOMOTIVE HACKING**:

TOOL: OPEN PILOT

LINK: https://comma-ai.medium.com/open-sourcing-openpilot-development-tools-a5bc427867b6

PLATFORM: Windows, Linux, macOS

FEATURES:

Automated lane-centering

It's an advanced driver-assistance system that keeps a road vehicle centered in the lane, relieving the driver of the task of steering.

Adaptive cruise control

Adaptive cruise control is a system designed to help road vehicles maintain a safe following distance and stay within the speed limit.

Driver monitoring

is an advanced safety feature that uses a camera mounted on the dashboard to track driver drowsiness or distraction, and to issue a warning or alert to get the driver's attention back to the task of driving.

Assisted lane change

It's a feature that, in addition to the *lane departure* warning system, automatically takes steps to ensure the vehicle stays in its *lane*.

Software updates

Openpilot receives over-the-air software updates via WiFi or a cellular phone network

PROS:

- OpenPilot will provide the steering, acceleration, and braking instructions to the vehicle
- OpenPilot also makes driver monitoring mandatory, meaning that it will know whether or not you're paying attention to the road.
- The Openpilot allows you to be driving hands-free and feet-free for long periods without driver involvement
- Openpilot maintains a safe following distance from the vehicle ahead. It is capable of driving in stop-and-go traffic with no user intervention.
- It uses OpenStreetMap's road curvature and speed limit data to allow slowing on sharp turns and setting the vehicle's desired speed to the current speed limit.

CONS:

- Poor visibility (heavy rain, snow, fog, etc.) or weather conditions that may interfere with sensor operation.
- The road-facing camera is obstructed, covered, or damaged by mud, ice, snow, etc.
- Obstruction is caused by applying excessive paint or adhesive products (such as wraps, stickers, rubber coating, etc.) onto the vehicle.
- Bright light (due to oncoming headlights, direct sunlight, etc.).
- Bugs in software

4. SOCIAL ENGINEERING:

TOOL: MALTEGO

LINK: https://www.maltego.com/

PLATFORM: Windows, Linux, macOS

FEATURES:

- Mine:
  Easily gather information from dispersed data sources
- Merge:
  Automatically link and combine all information in one graph.
- Map:
  Annotate your graph and export it for further use

PROS:

- It is used for gathering information for security-related work. It will save your time and make you work smarter and accurately.
- It will help you in the thinking process by demonstrating connected links between all the searched items.
- If you want to get hidden information, it (Maltego) can help you to discover it.
- It will demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure.

CONS:

- It scans only these limited sites for gathering information. It doesn't include inbuilt transforms to scan other popular social media websites.
- It runs transforms on a single entity (e.g. Name, IP address, etc.). It cannot take a combination of entities such as name and location.
- Maltego does not allow the use of transforms to extract any particular information from a company's profile.
- Maltego doesn't allow to search within the company the name of a particular employee. It does not have in-built transforms to extract emails, phone numbers, or names of persons from a document text.

5. **DEVICE SYNCHRONIZATION**
   TOOL: FreeFileSync
   PLATFORM: Windows, macOS, Linux
   LANGUAGE: ---
   LINK: https://freefilesync.org
   FEATURES:
   - File Synchronization between devices is the process of ensuring that the data in two or more systems are in a consistent state.
   - It is also called mirroring because it ensures that if a file is changed in one system, that commit is automatically mirrored in other connected systems.

- It is commonly used for taking up backup or integrated development projects. It can be as simple as just updating and maintaining a single directory to mirroring and backing up the entire system.
- Common features of file synchronization may include encryption, security, compression, etc.

PROS:

- FreeFileSync is a folder comparison and synchronization software that creates and manages backup copies of important files.
- It saves bandwidth on remote devices involving mirroring because instead of copying every file, every time, it determines the differences between target directories and only updates the changes.
- Minimum data transfer is required.

CONS:

- It can face issues on a large-scale device synchronization process because it needs to keep track of what has been updated.
- Since it only updates on detecting changes, it is sometimes possible for the software to fail detection if the last updated times of files are maliciously updated to trick the software causing the software to not detect the changes to be mirrored.

6. **IOT & 5G NETWORKS**

TOOL: MOSAIC 5G

LINK: https://mosaic5g.io/

PLATFORM: Windows, Linux, macOS

FEATURES:

- RAN Control & Data Plane separation.
- Abstraction & Virtualized Control Functions.
- RESTful API.
- RAN Optimization.
- Network slicing.
- IoT Gateway.
- Content caching.
- CN Control & Data Plane separation.

PROS

- Mosaic provides a clean and interface that is easy to understand, a great tool for team communication and collaboration.
- It's easy to adapt to the mosaic ecosystem
- It helps us to develop some innovatory applications
- It will provide tutorials that help with our projects.

CONS

- It has some software bugs
- The updates are very slow
- Mosaic takes a few hours to bring all current projects into the platform
- Receiving email notifications for all updates on projects.

7. **Biometric Security**

TOOL: OpenBR

LINK: http://openbiometrics.org/

PLATFORM: Windows, Linux, macOS

LANGUAGE: Python and R

FEATURES:

- OpenBR exposes a C++ API that can be embedded into one's applications.
- It is a complete NIST-compliant software that evaluates facial recognition, detection, and land-marking.
- It implements the 4SF2 algorithm to perform face recognition.
- The software algorithms also work for age estimation and gender estimation.

PROS:

- It helps in securing the transactions without a need of customers OTP, Secret, personal message, key, etc.
- Innovative facial security measures are useful for handling sensitive data of a family or organization and keep tight control over whoever is entering their facilities.
- Helps in identifying the suspects from people's driver's licenses, merchant licenses, delivery service licenses, and so on.
- It provides security to patient data by using a unique photo of the patient & checking out the illness from features of the patient.
- Doesn't even need customers to use their credit/debit cards for online shopping.

CONS:

- Costs – Significant investment needed in biometrics for security
- Data breaches – Biometric databases can still be hacked
- Tracking and data – Biometric devices like facial recognition systems can limit privacy for users
- Bias – Machine learning and algorithms must be very advanced to minimize biometric demographic bias
- False positives and inaccuracy – False rejects and false accepts can still occur preventing select users from accessing systems

8. **Mobile Security**

TOOL: MobSF

LINK: https://github.com/MobSF

PLATFORM: Linux, MacOS

FEATURES:

- Responsive UI
- Live device/VM screencast on dynamic analyzer view
- Dynamic SSL testing
- Exported activity tester and PoC generation
- All new REST API fuzzer for security testing backend servers of hybrid mobile apps
- Custom VM and Android device support for MobSF dynamic analysis
- An updated static analyzer rule set
- Recent scan view
- Improved web proxy, error handling, and dynamic analyzer logic
- Anti-emulator check bypass.

PROS:

- it's a free-of-charge open-source tool and hosted in a local environment, so sensitive data never interacts with the cloud.
- Can be used to test multiple vulnerabilities.
- Can be used to perform Dynamic as well as static test for a mobile application.
- Easy to install
- Malware detection
- Detection of sensitive information in the code or resources
- Can generate and download reports in PDF.

CONS:

- Missing access management features
- The framework is still in beta
- It is hard to run an Android emulator.
- Lots of false positives - as they do regular expression search which is not accurate enough, whereas Appknox uses a Data flow algorithm to figure out more specific and correct security issues.

9. **CyberWarFare Security**

TOOL: CIMPLICITY Script PowerShell

LINK: https://www.securityweek.com/open-source-tool-helps-organizations-secure-ge-cimplicity-hmiscada-systems

LANGUAGE: C sharp

PLATFORM: Windows

FEATURES:

- Analyzes the collected data according to OTORIO's profound research on CIMPLICITY security and hardening.
- Provides Security of Passwords, sensitive Files & ports

PROS

- The new tool designed by OTORIO is simple to use and requires no cyber expertise.
- The tool is by default installed with OT servers.
- The CYMPLICITY hardening tool checks the system to ensure that passwords need to be long and complex and are not stored in clear text
- Users who don't need them don't have elevated privileges

CONS

- Creates a very uncertain and unstable situation globally, where anybody's sensitive data could be accessed at any time, without their consent.
- Undetected zero-days can lead to huge impacts all over the cyber world.

10. **Cloud Vulnerability**

TOOL: Osquery

LINK: https://github.com/osquery/osquery

PLATFORM: Windows, Linux, macOS
LANGUAGE: C++

FEATURES:

- **Interactive Query Console:** Osquery equips a SQL interface that helps to explore the operating system with various queries. It also helps in understanding various processes, kernel modules, active user accounts, and active network connections.
- **Powerful Performance Diagnosis:** With the help of SQL power and highly useful built-in tables, Osquery is an invaluable and very aggressive tool for diagnosing systems operations problems, troubleshooting a performance issue, etc.
- **Large-scale host monitoring:** Osquery, which is regarded as the high-performance host monitoring daemon, allows you to schedule queries for execution across your infrastructure.
- **Real-Time Monitoring:** All the query results are monitored in a real-time scenario which further helps in understanding the security, performance, configuration, and state of the entire infrastructure. Osquery has a logging mechanism that is powerful enough to integrate the existing internal log aggregation pipeline via a robust plug-in architecture.
- **Cross-Platform and Open source:** Osquery is a cross-platform framework and a complete open-source tool, which has major user credibility across the globe, especially in security streams.
- **Native packages and extensive documentation:** To make deployment simple and possible, Osquery comes with native packages for all supported operating systems. The tooling and documentation help to understand Osquery functionalities easily.
- **Osquery for Security:** Osquery-Powered Security Analytics is the most happening thing now. Osquery is extremely capable and can be used as a universal agent for many use cases including:
    - ❖ Intrusion/Malicious activity detection (EDR)
    - ❖ File Integrity Monitoring
    - ❖ Incident Investigation
    - ❖ Vulnerability Detection
    - ❖ Audit and Compliance
    - ❖ SIEM (SOC) by capturing precise input for SIEM solutions like Splunk/ELK

- ❖ Malware Analysis
- ❖ Digital Forensics
- ❖ System Administration

PROS:

- Very simple and flexible to install and implement
- Modular CodeBase is a highly added advantage
- Simple Query processing
- More customizable and real-time recording of events
- Provides a new endpoint data to which we never had access.

CONS:

- The cost of data storage is high
- Complexity in translating the incremental data
- Optimizing queries and query packs is critical
- Third-party assistance and data are still required for threat detection.