Lab 9

NIDS_NIPS and Web Proxy Analysis

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

04/27/2025

Introduction

In today's cybersecurity landscape, analyzing logs generated by Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and web proxies is a fundamental component of detecting and responding to threats. These systems generate detailed logs that provide insights into network activity, potential intrusions, and user behavior. Developing proficiency in interpreting and investigating IDS/IPS alerts, particularly from tools such as Snort, is essential for identifying and understanding suspicious traffic patterns. Snort alerts offer structured information on packet payloads, attack signatures, and threat types that can be leveraged to investigate and respond to security incidents.

Similarly, proxy servers such as Squid maintain detailed logs of user web activity, which are invaluable for tracing web-based threats, such as malware downloads or access to malicious domains. Proxy logs record HTTP requests, IP addresses, timestamps, and content types, enabling security analysts to correlate user behavior with external threats. Mastery of both IDS/IPS and proxy log formats equips cybersecurity professionals with the skills to conduct thorough forensic investigations, assess the scope of incidents, and implement effective mitigation strategies. (Preethi & Reddy, 2024).

Pre-Analysis

Understanding NIP/DS vs. HIP/DS

In cybersecurity, understanding the differences between Network-based Intrusion Detection and Prevention Systems (NIP/DS) and Host-based Intrusion Detection and Prevention Systems (HIP/DS) is essential for designing a robust defense strategy. Both play critical roles in identifying and mitigating cyber threats, but their operational scopes and deployment architectures vary significantly.

NIP/DS: Network-Based Intrusion Prevention/Detection Systems

Network Intrusion Detection Systems (NIDS) and Network Intrusion Prevention Systems (NIPS) are deployed at strategic points within a network to monitor traffic to and from all devices. NIP/DS solutions analyze network packets for known threats and anomalies, raising alerts (NIDS) or actively blocking malicious traffic (NIPS) in real-time. These systems are typically composed of specialized appliances with dedicated network interface cards (NICs), processing units, and software tailored for traffic inspection (Scarfone & Mell, 2007).

An example of NIP/DS is Snort, a widely used open-source network IDS/IPS that supports real-time traffic analysis and packet logging on IP networks. Snort can detect attacks such as port scans, buffer overflows, and denial-of-service (DoS) attempts, making it ideal for monitoring large-scale enterprise networks (Roesch, 1999).

HIP/DS: Host-Based Intrusion Prevention/Detection Systems

In contrast, Host-based Intrusion Detection Systems (HIDS) and Host-based Intrusion Prevention Systems (HIPS) operate at the individual system level. Installed as software agents, HIP/DS tools monitor system logs, file integrity, process behavior, and system calls to identify malicious activity. These systems are crucial for detecting insider threats, unauthorized file modifications, and malware infections (Scarfone & Mell, 2007).

An example of HIP/DS is OSSEC, an open-source HIDS that performs log analysis, file integrity checking, policy enforcement, and active response. It is particularly effective in detecting rootkits and unauthorized configuration changes on critical servers (Singh, 2014).

Choosing the Right Solution for Business Networks

For most business environments, deploying a NIP/DS solution offers broader coverage and is generally more scalable. A single NIDS sensor can monitor network traffic for many hosts, making it cost-effective for detecting external threats like reconnaissance scans, unauthorized access attempts, and distributed denial-of-service (DDoS) attacks. However, for environments handling sensitive data or subject to strict compliance, integrating both NIP/DS and HIP/DS solutions ensures layered protection—commonly referred to as defense in depth.

Analysis

In this fictitious scenario, students are tasked with analyzing IDS/IPS alerts and proxy logs to investigate a potential security breach. The exercise emphasizes the importance of correlating network-based alerts with system behavior to detect and mitigate malicious activities.

The investigation begins with a peculiar initiative by an individual known as *Inter0ptic*, who has launched a controversial “credit card number recycling” program. Marketed as an eco-friendly solution, the program encourages companies to send in databases filled with previously used credit card numbers in exchange for financial compensation. This dubious activity raises immediate red flags, especially as the website is enhanced with additional features—potentially introducing new vulnerabilities.

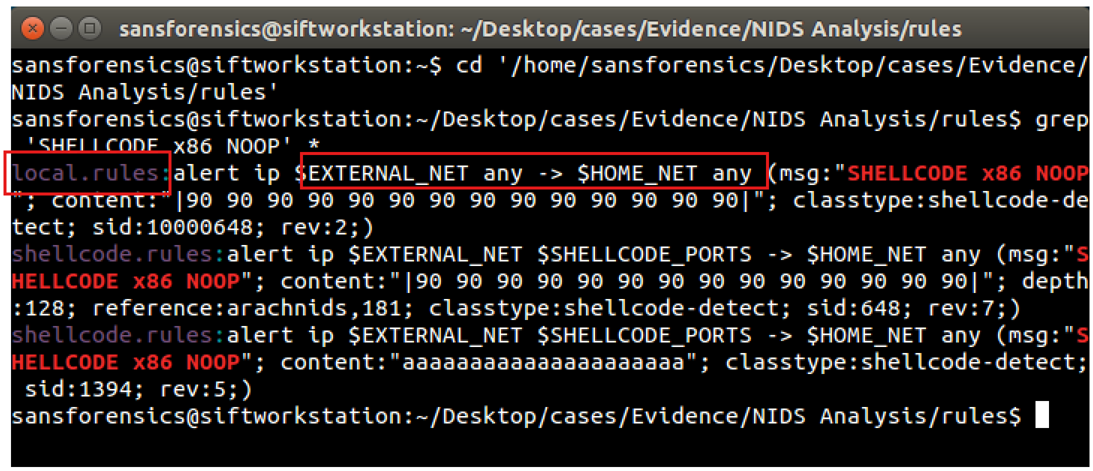
Simultaneously, *MacDaddy Payment Processor*—an organization entrusted with handling sensitive financial data—has deployed Snort Network Intrusion Detection System (NIDS) sensors to monitor both inbound and outbound traffic. On the morning of May 18, 2011, at 08:01:45, Snort flagged a high-priority alert indicating the transmission of x86 shellcode over port 80 TCP. The payload, originating from an external host (172.16.16.218), was directed at an internal system (192.168.1.169). This event suggests a deliberate attempt to exploit the internal network via executable code delivery, prompting immediate forensic analysis.

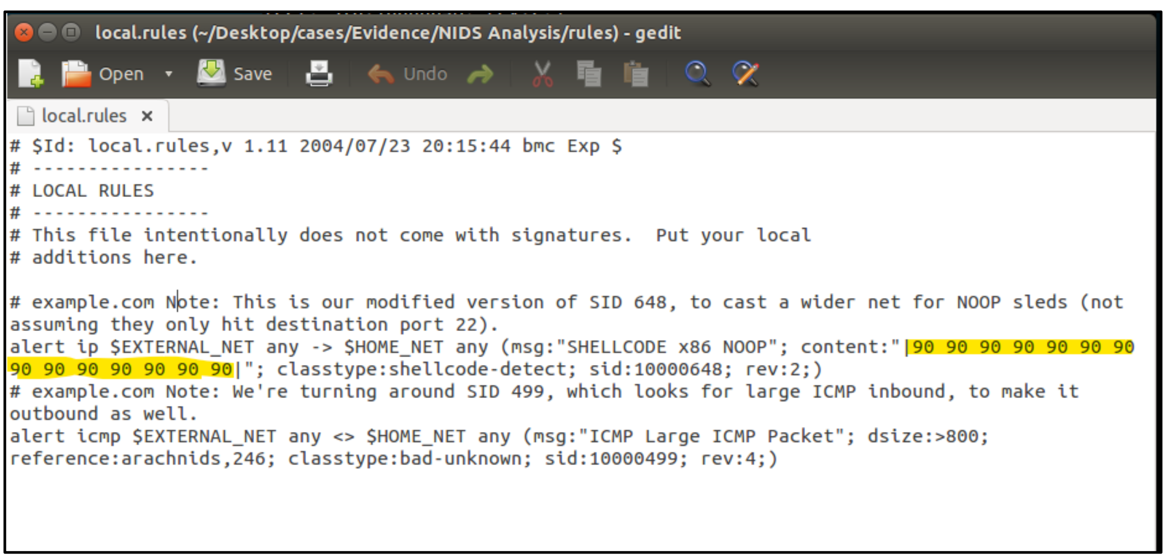
The security team responds by securing relevant Snort alerts, logs, and configuration files. The internal and external network structures—including the internal network (192.168.1.0/24), the DMZ (10.1.1.0/24), and the "Internet" segment (172.16.16.0/24)—as well as suspicious domains like “.evl,” are critical components in tracing the source and intent of the attack.

This investigation will involve dissecting packet captures, reviewing IDS alert data, and evaluating proxy logs to uncover the scope of the intrusion attempt and identify any possible compromise or data exfiltration. Through structured analysis, the exercise aims to reinforce skills in threat detection, network forensics, and incident response planning.

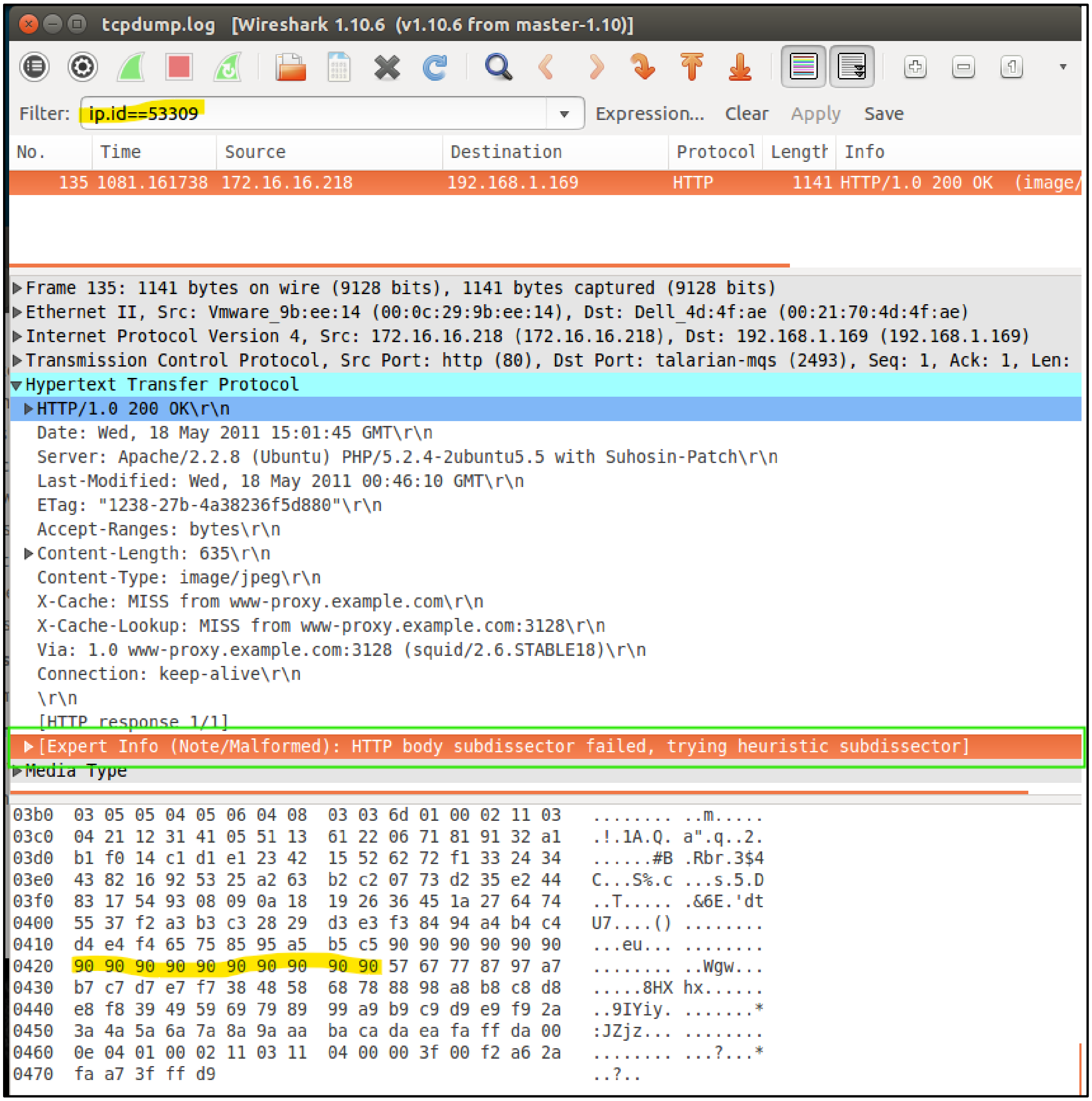
IDS/IPS Log Analysis

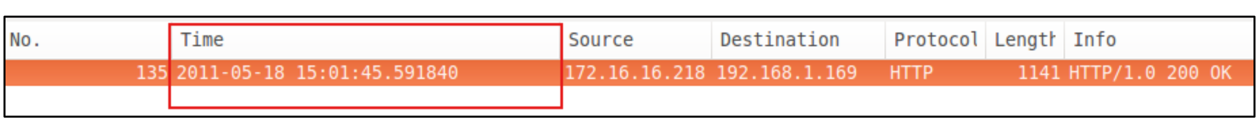
Initial determination is that this is a true positive alert. The alert was triggered by an inbound transmission of shellcode targeting a host within the internal network. The source port (80) and classification as shellcode suggest an exploit attempt masquerading as normal HTTP traffic. The detection of a NOOP sled—commonly used in buffer overflow attacks—further supports the conclusion of malicious intent.





A suspicious JPEG file, which may have contained executable code, was found from the packet capture for deeper examination.





Logistical Context

- Source (Attacker): 172.16.16.218 (external)
- Target (Victim): 192.168.1.169 (internal)
- Port Usage: Source port 80 (HTTP), suggesting the attack may be web-based.
- Detection Signature: "SHELLCODE x86 NOOP" — flags patterns associated with NOP sleds used to facilitate arbitrary code execution.

Timeline

- Between 07:45:09 and 08:15:08 on 5/18/11, the internal host 192.168.1.169 was actively browsing the web
- At 08:01:45, a remote server delivered a JPEG image that embedded a suspicious binary sequence, indicating a potential exploitation attempt.
- By 08:04:28, the internal host began transmitting specially crafted packets, indicative of possible scanning and system fingerprinting.

Conclusion

The detection of the SHELLCODE x86 NOOP alert, followed by the transmission of reconnaissance packets, strongly indicates a drive-by exploitation attempt that may have compromised the internal host. This pattern of activity suggests that the host could have been leveraged for further malicious actions, such as network scanning, fingerprinting, or lateral movement within the environment.

```
[**] [1:2925:3] INFO web bug 0x0 gif attempt [**]
[Classification: Misc activity] [Priority: 3]
05/18-07:45:00.179227 207.171.185.201:80 -> 192.168.1.170:59891
TCP TTL:63 TOS:0x0 ID:9883 IpLen:20 DgmLen:693 DF
***AP*** Seq: 0x6AFC454F  Ack: 0x711BD654  Win: 0x6B4  TcpLen: 32
TCP Options (3) => NOP NOP TS: 5596130 166439099
```

```
[**] [1:10000648:2] SHELLCODE x86 NOOP [**]
[Classification: Executable code was detected] [Priority: 1]
05/18-08:01:45.591840 172.16.16.218:80 -> 192.168.1.169:2493
TCP TTL:63 TOS:0x0 ID:53309 IpLen:20 DgmLen:1127 DF
***AP*** Seq: 0x1B2C3517  Ack: 0x9F9E0666  Win: 0x1920  TcpLen: 20
```

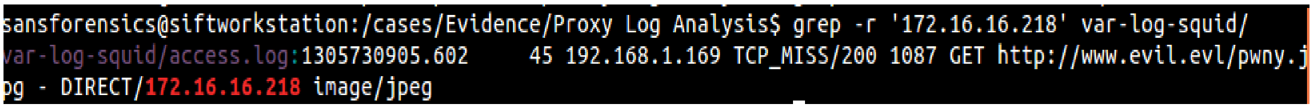
```
[**] [1:2925:3] INFO web bug 0x0 gif attempt [**]
[Classification: Misc activity] [Priority: 3]
05/18-08:15:06.474654 64.30.224.42:80 -> 192.168.1.169:2634
TCP TTL:63 TOS:0x0 ID:24543 IpLen:20 DgmLen:639 DF
***AP*** Seq: 0x5EA4839  Ack: 0x2CDFA0DE  Win: 0x2180  TcpLen: 20

[**] [1:2925:3] INFO web bug 0x0 gif attempt [**]
[Classification: Misc activity] [Priority: 3]
05/18-08:15:08.286168 216.239.113.95:80 -> 192.168.1.169:2650
TCP TTL:63 TOS:0x0 ID:57018 IpLen:20 DgmLen:728 DF
***AP*** Seq: 0x95FC010  Ack: 0x9C6308FA  Win: 0x1A28  TcpLen: 20
```

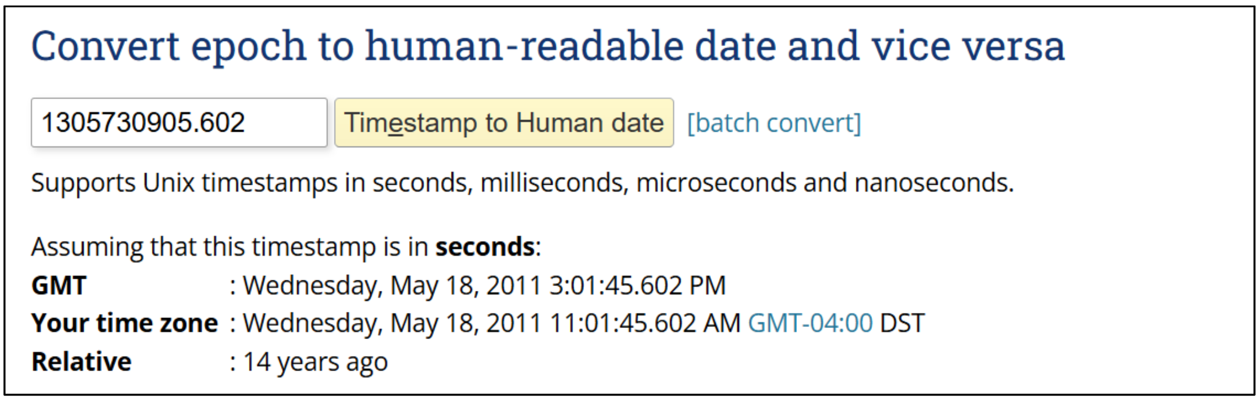
Proxy Log Analysis

Looked at IP 172.16.16.218 in quid logs and found out the time in epoch format:

1605730905.602. Then convert the time : May 18, 2011 at 03:01:45 which (UTC) in local

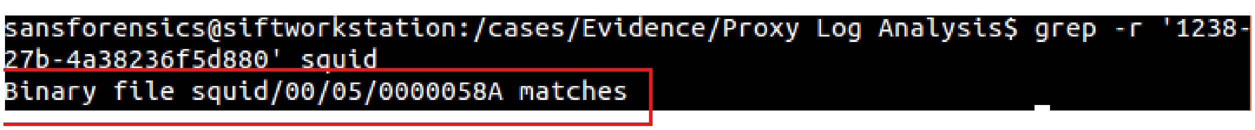
time it would be 06:





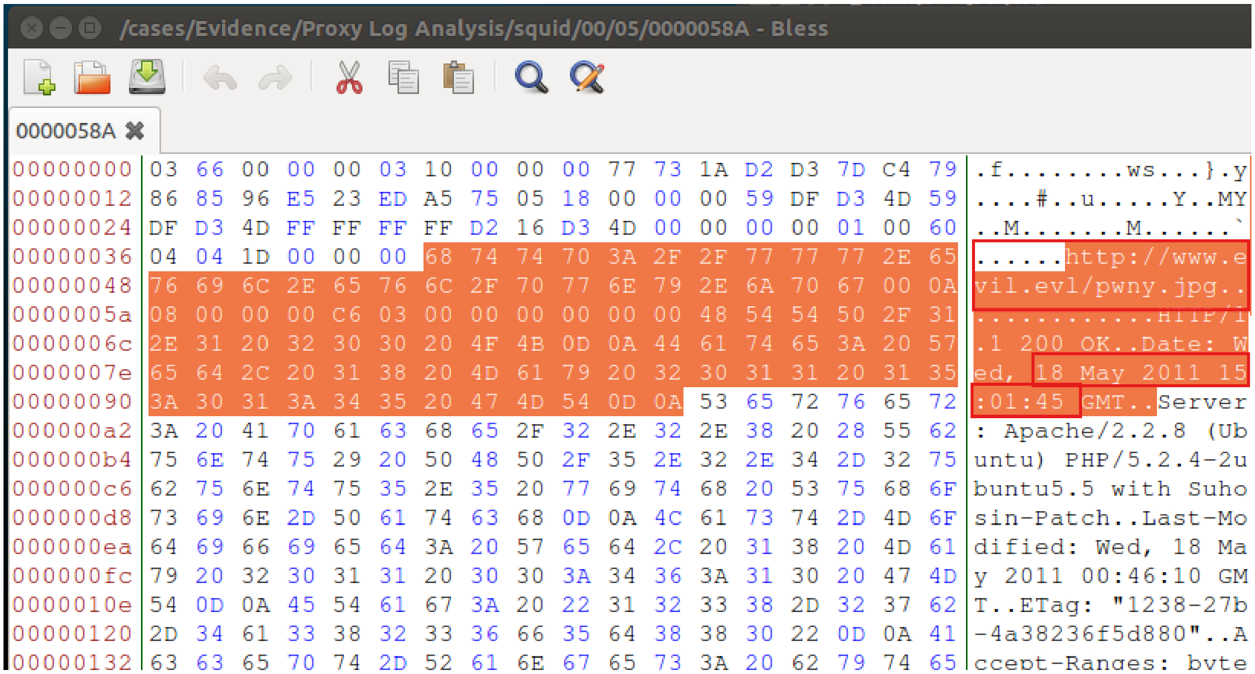
I started by analyzing the Squid proxy cache to search for any evidence related to the suspicious image identified in the Snort alert. During the review, I found that the Squid cache contained a unique ETag value: 1238-27b-4a38236f5d880. Using standard Linux command-line tools, it is possible to search through the Squid cache directories and locate the specific cache file associated with this ETag value, as demonstrated below:

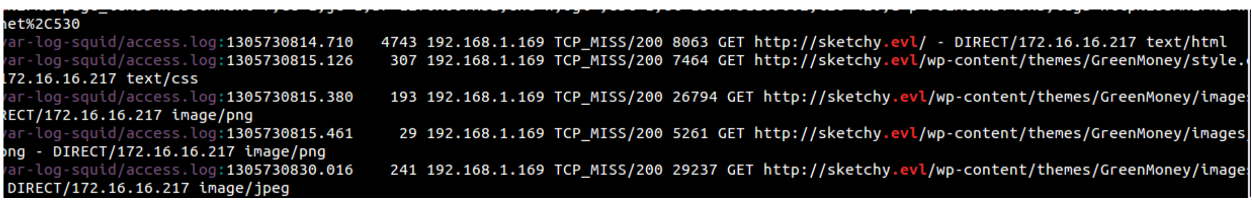
$ grep -r '1238 -27 b -4 a38236f5d880 ' squid



The file containing Etag value is cached in the squid/00/05/0000058A folder. I opened the cached page in Bless and found the URL:

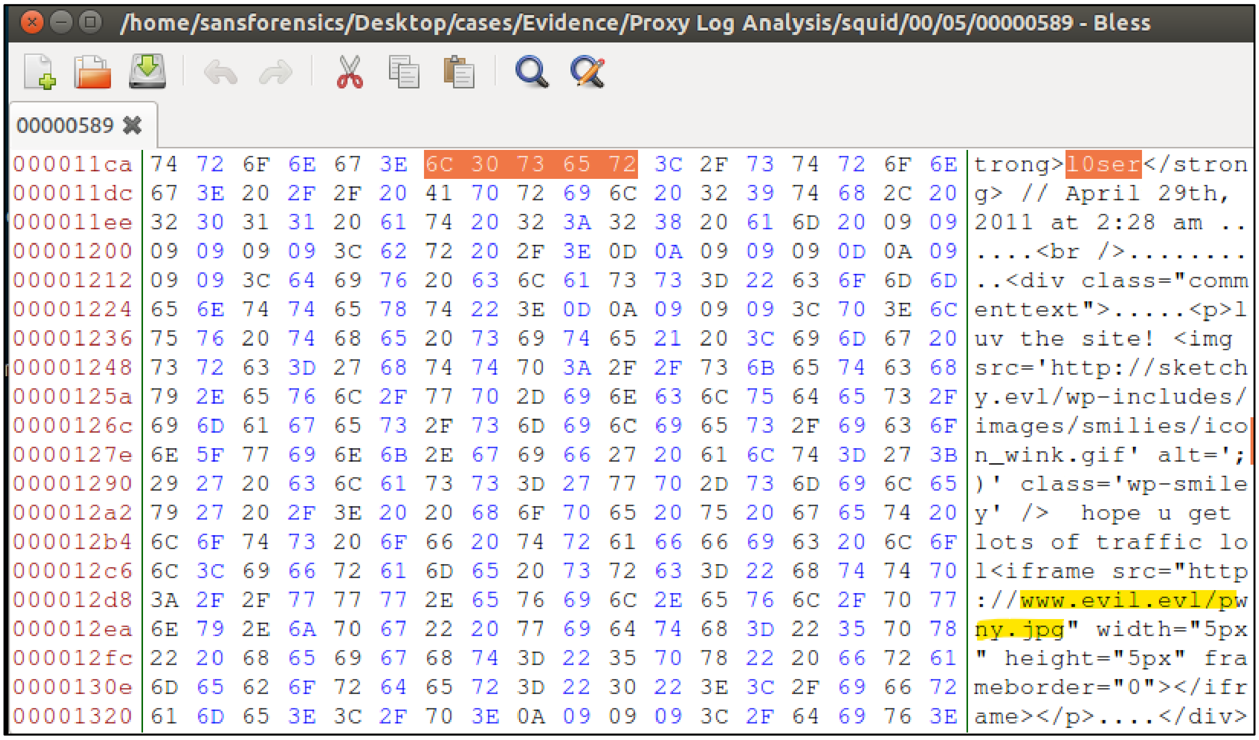
http://www.sketchy.evl/pwny.jpg

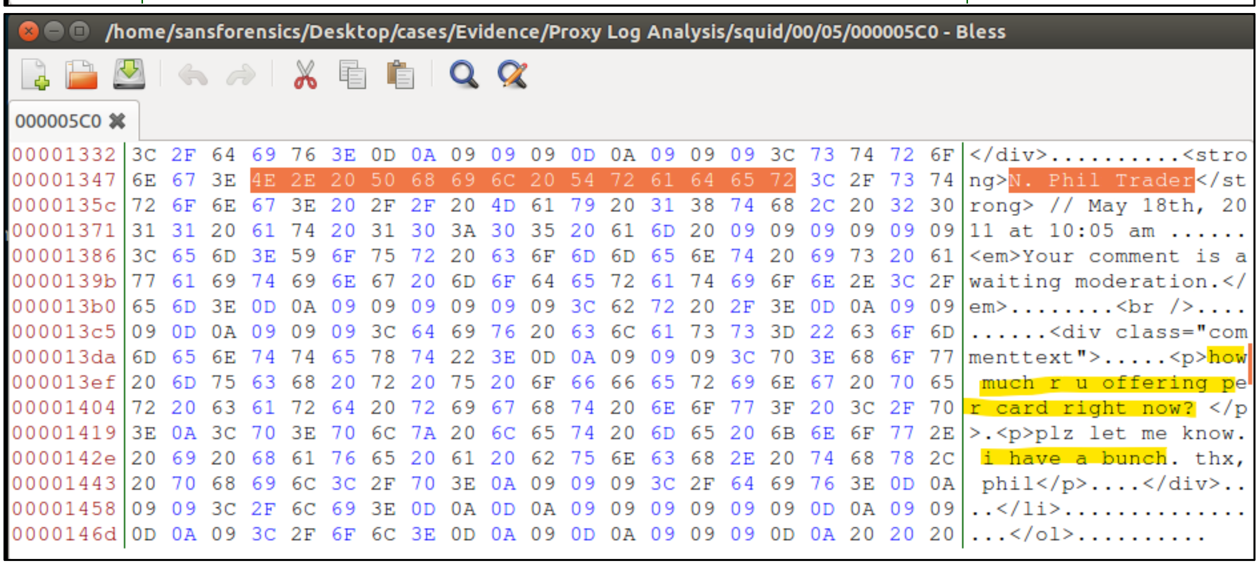




The website skethcy.evl had a user account with the name of Phil Trader with a post indicating he has a bunch of credit card information and wanted to know how much it was worth.

Additionally, the domain sketchy.evl contained a comment posted by a user named "l0ser", which included a link to pwny.jpg. When the internal host 192.168.1.169 accessed the page, the browser automatically loaded and downloaded the suspicious image without requiring any user interaction. This behavior suggests that the image may have been used as a delivery mechanism for malicious payloads.





Glossary

Denial of Service (DoS): An attack that aims to make a system or service unavailable by overwhelming it with traffic.

IDS/IPS (Intrusion Detection/Prevention Systems): Systems that monitor and optionally block malicious or suspicious network activity.

NIP/DS (Network Intrusion Prevention/Detection System): Tools that detect or prevent malicious activity by monitoring network traffic.

OSSEC: An open-source host-based IDS that supports log analysis, file integrity checking, and rootkit detection.

Proxy Logs: Logs generated by web proxies that detail user requests to external websites, often including timestamps, URLs, and HTTP status codes.

Reconnaissance Attack: A type of attack aimed at gathering information about a network to identify potential vulnerabilities.

Snort: An open-source network IDS/IPS that inspects packet-level traffic and generates alerts based on predefined rules.

Squid: A widely used web caching proxy server that logs web traffic and assists in both performance optimization and security monitoring.

References

Preethi, T. & Reddy, P. (2024). *A Novel Approach for Anomaly Detection using Snort Integrated with Machine Learning*. *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*.

Roesch, M. (1999). *Snort: Lightweight intrusion detection for networks*. Proceedings of the 13th USENIX Conference on System Administration (LISA '99), 229–238. USENIX Association. https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Singh, A. & Singh, M. (2014). A*nalysis of Host-Based and Network-Based Intrusion Detection System*. Modern Education and Computer Science. IJCNIS-V6-N8-6.pdf