Analysis & Threat Hunting

Techniques using Open Source Tools

Presenter – Sanchay Singh

@ defcon delhi 0x06

December, 2023

>_whoami

-> Co-founder of HackersVilla CyberSecurity

-> Security Consultant/Trainer at MakeIntern

-> Worked as SME at UpgradCampus

-> Trained Employees of KPMG, Cognizant, etc

-> Security Mentor/Speaker at OWASP Delhi

-> Security Mentor at BSides Noida

-> Active part of NULL and THM Delhi Chapter

Sanchay Singh

CYBERSECURITY EXPERT | CORPORATE TRAINER | PUBLIC SPEAKER

sanchayofficial

sanchayofficial@gmail.com

Introduction

Welcome to the Advanced Analysis and Threat Hunting Workshop!

Objectives:

- Equipping you all with advanced analysis skills in cybersecurity.
- Diving into the evolving threat landscape.
- Familiarizing with open source tools for threat hunting.
- Hands-on experience through practical exercises.

Agenda Overview

1. Threat Landscape and Methodologies
2. Open Source Tools
3. Network and Log Analysis Techniques
4. Malware Analysis Techniques
5. Advanced Memory Forensics
6. Best Practices and Challenges

The need for Advanced Analysis

Traditional security measures are no longer sufficient against sophisticated cyber threats.

Advanced analysis is essential to proactively detect and respond to evolving threats.

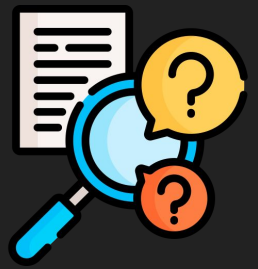
Role of Threat Hunting in Cybersecurity

Threat hunting involves actively searching for signs of malicious activity within an environment.

It complements traditional security measures by identifying threats that may go undetected.

Prerequisites for Participants

- Basic Cybersecurity Knowledge
- A working laptop/system
- Curiosity and Enthusiasm



Threat Landscape and Methodologies

Evolving Threat Landscape

Cyber threats are dynamic and continuously evolving.

Rapid technological advancements present new attack vectors.

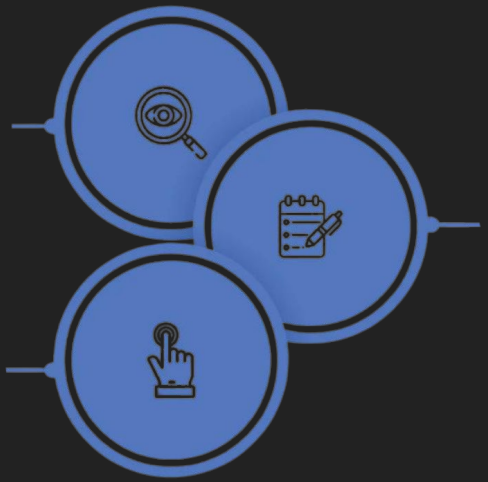
Challenges:

- Complexity of modern attacks.
- Blurring lines between state-sponsored and criminal activities.

Threat Hunting Methodologies

Proactive approach to identifying and mitigating threats.

Involves continuous monitoring and analysis.



Frameworks:

- MITRE ATT&CK framework.
- Cyber Kill Chain methodology.

Lets understand this with a case study.


CASE
STUDY

Open Source Tools

Introduction to Open Source Tools

Open source tools play a crucial role in cybersecurity.

Community-driven development fosters innovation and adaptability.

Advantages:

- Cost-effective solutions.
- Transparency and community support.

Featured Tools:

Wireshark, Suricata, Bro/Zeek, Cuckoo Sandbox, YARA, etc

Overview and Features of Each Tool

Bro/Zeek:

- Network security monitor.
- Features: Real-time analysis, protocol detection.

Cuckoo Sandbox:

- Automated malware analysis.
- Features: Dynamic analysis, behavior tracking.

YARA:

- Pattern-matching swiss knife.
- Features: Malware detection, code analysis.

Wireshark:

- Network protocol analyzer.
- Features: Packet inspection, traffic analysis.

Suricata:

- Open-source IDS/IPS.
- Features: Intrusion detection, network security monitoring.

Let’s do some practical...

Purpose and Usage of the Tools

- Capture and analyze packets to detect anomalies.
- Real-time analysis to identify and respond to threats.
- Helps in the detection of malicious activities.
- Provides insights into malware behavior.
- Allows for the creation of custom rules for malware detection.
- Choosing the right tool based on the specific security situation.

Network and Log Analysis Techniques

Introduction to Network Traffic Analysis

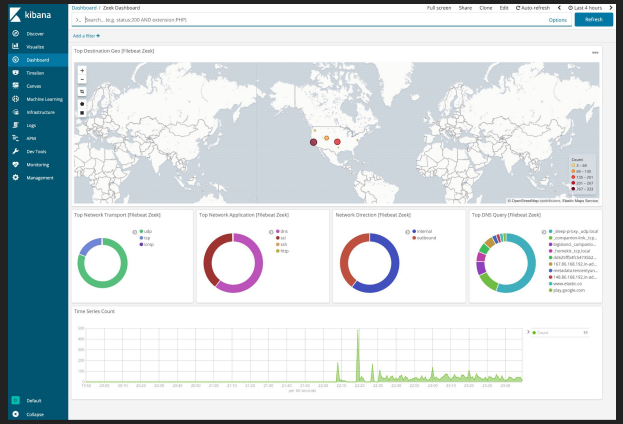
Network traffic analysis is a cornerstone of cybersecurity.

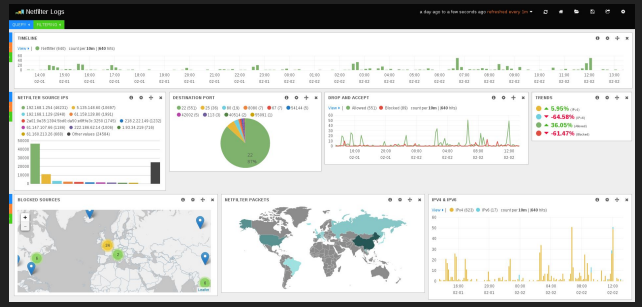
Involves monitoring and analyzing data flowing over a network.

Importance:

- Early detection of anomalies and potential threats.
- Identification of malicious activities.

Tools - Wireshark, Suricata, Bro/Zeek





Malware Analysis Techniques

Malware Analysis Techniques

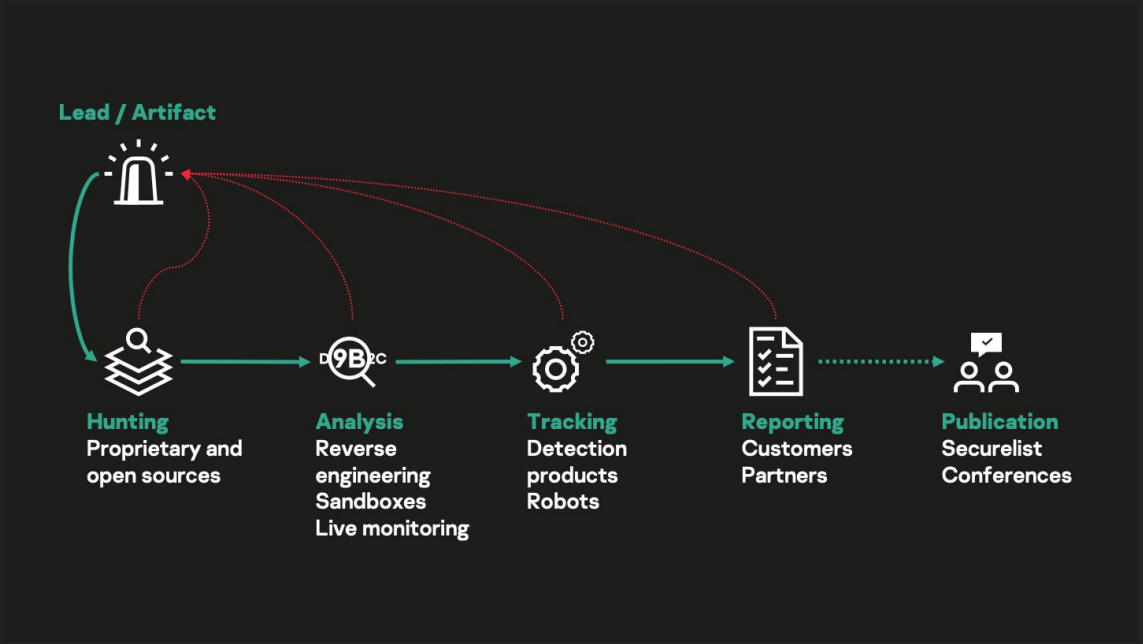
Dynamic: Observing the behavior of the malware in a controlled environment.

Static: Analyzing the code without executing it.

Tools - Cuckoo Sandbox, YARA:

- Cuckoo Sandbox for automated dynamic analysis.
- YARA for pattern-matching and code analysis.

Identifying Malicious Behaviors and Extracting IOCs



Advanced Memory Forensics

Memory Acquisition Techniques

Memory forensics involves analyzing the volatile memory of a computer system.

Vital for detecting sophisticated threats and uncovering malicious activities.

Memory Acquisition Techniques:

- Live system acquisition.
- Memory image acquisition.

Hands-On Exercise on Memory Acquisition

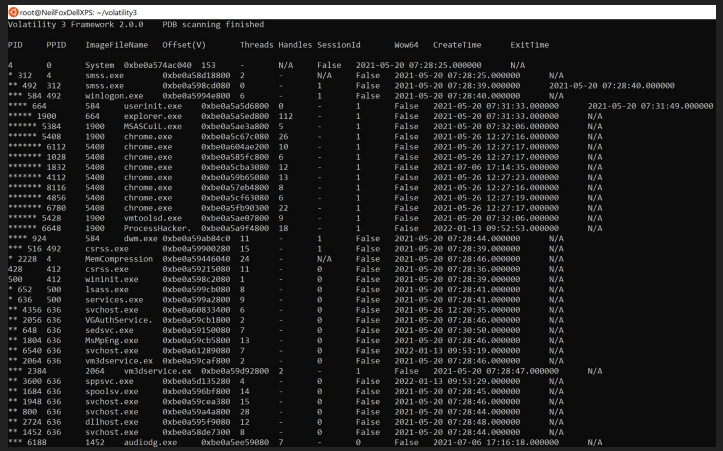
Tools - Volatility and Rekall:

- Overview of these open-source tools for memory analysis.
- **Volatility:** A powerful framework for memory forensics.
- **Rekall:** Providing a flexible interface for memory analysis.

Deep Dive into Volatility Framework

Features of Volatility:

- Memory analysis of Windows, Linux, macOS systems.
- Identification of running processes, open network connections, etc.



Advanced Analysis Using Volatility

```
0xdb898221dae0  UDPv4   0.0.0.0 4500    *       0               984     svchost.exe     2021-05-10 10:18:24.000000
0xdb8982313390  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       1552    spoolsv.exe     2021-05-10 10:18:24.000000
0xdb8982313390  TCPv6   ::      49667   ::      0       LISTENING       1552    spoolsv.exe     2021-05-10 10:18:24.000000
0xdb89825e68f0  TCPv4   192.168.233.128 49728   203.99.187.137  443     CLOSED  6336    smsfwdr.exe     2022-01-17 09:04:55.000000
0xdb89827e33b0  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2021-05-10 12:01:40.000000
0xdb8982aa2730  TCPv4   0.0.0.0 49676   0.0.0.0 0       LISTENING       576     lsass.exe       2021-05-10 10:18:33.000000
0xdb8982aa2730  TCPv6   ::      49676   ::      0       LISTENING       576     lsass.exe       2021-05-10 10:18:33.000000
0xdb8982abc650  UDPv4   0.0.0.0 5355    *       0               1272    svchost.exe     2021-05-10 12:01:40.000000
0xdb8982abc650  UDPv6   ::      5355    *       0               1272    svchost.exe     2021-05-10 12:01:40.000000
0xdb8982b23860  TCPv4   0.0.0.0 49676   0.0.0.0 0       LISTENING       576     lsass.exe       2021-05-10 10:18:33.000000
0xdb898367c6d0  TCPv4   192.168.233.128 49732   144.76.62.10    8080    SYN_SENT        6336    smsfwdr.exe     2022-01-17 09:06:37.000000
0xdb898369fec0  TCPv4   192.168.80.129  139     0.0.0.0 0       LISTENING       4       System  2021-05-10 12:01:12.000000
0xdb8983700960  UDPv4   0.0.0.0 5353    *       0               1272    svchost.exe     2021-05-10 12:01:40.000000
0xdb8983700960  UDPv6   ::      5353    *       0               1272    svchost.exe     2021-05-10 12:01:40.000000
0xdb898371e1a0  UDPv4   0.0.0.0 0       *       0               1272    svchost.exe     2022-01-17 09:06:25.000000
0xdb898371e1a0  UDPv6   ::      0       *       0               1272    svchost.exe     2022-01-17 09:06:25.000000
0xdb89837cfd00  TCPv4   192.168.233.128 49727   190.117.206.153 443     CLOSED  6336    smsfwdr.exe     2022-01-17 09:04:30.000000
```

Let us do perform some advanced analysis on a machine

Best Practices and Challenges

Best Practices for Implementing Open Source Tools

Documentation and Knowledge Sharing:

- Thoroughly document configurations and procedures.
- Encourage knowledge sharing within the cybersecurity team.

Forensic Integrity:

- Ensure forensic soundness in all activities.
- Maintain the integrity of evidence for legal and investigative purposes.

Best Practices and Challenges in Memory Forensics

Documenting the analysis process.

- Maintaining forensic integrity.
- Collaborative analysis for comprehensive results.

Challenges:

- Complexity of memory analysis.
- Rapidly changing memory structures.

Scalability, Performance, and Maintenance

Scalability Challenges

- Evaluate tools for scalability to handle increasing data volumes.
- Consider the impact on performance as the toolset expands.

Performance Optimization & Maintenance Considerations:

- Regularly optimize tool configurations.
- Implement efficient data storage and retrieval mechanisms.
- Stay updated with tool versions and security patches.
- Regularly review and refine the toolset to align with evolving threats.

So....
Lets Interact?

Thank you for your active engagement in the workshop.

Now, I invite **any questions** or discussions you may have.

Thank You