

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



sanchayofficial



sanchayofficial@gmail.com



Sanchay Singh

CYBERSECURITY EXPERT | CORPORATE
TRAINER | PUBLIC SPEAKER

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:

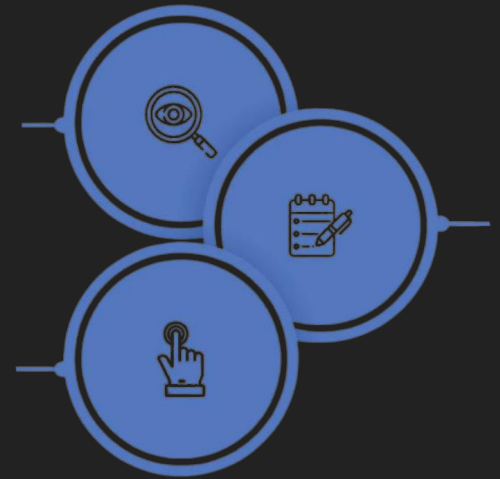
- Complexity of modern attacks.
- Blurring lines between state-sponsored and criminal activities.

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.



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

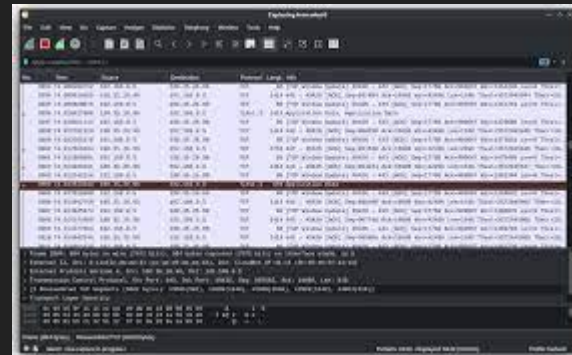
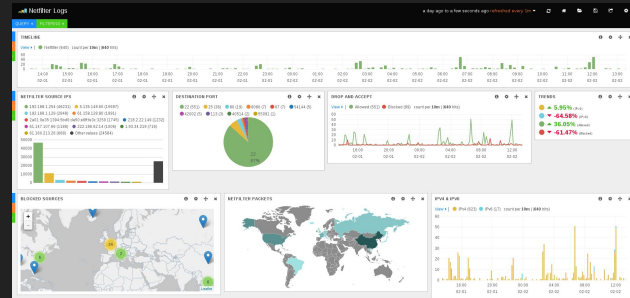
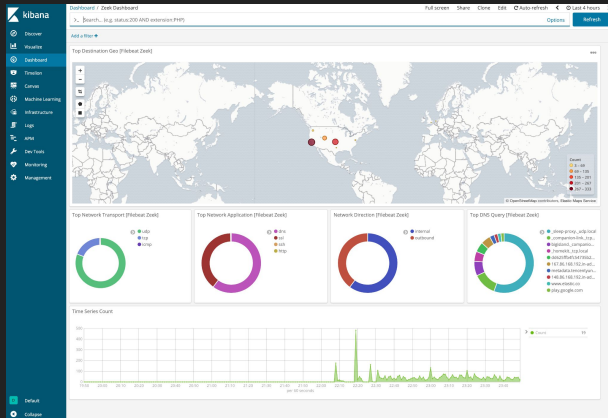
Network traffic analysis is a cornerstone of cybersecurity.

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

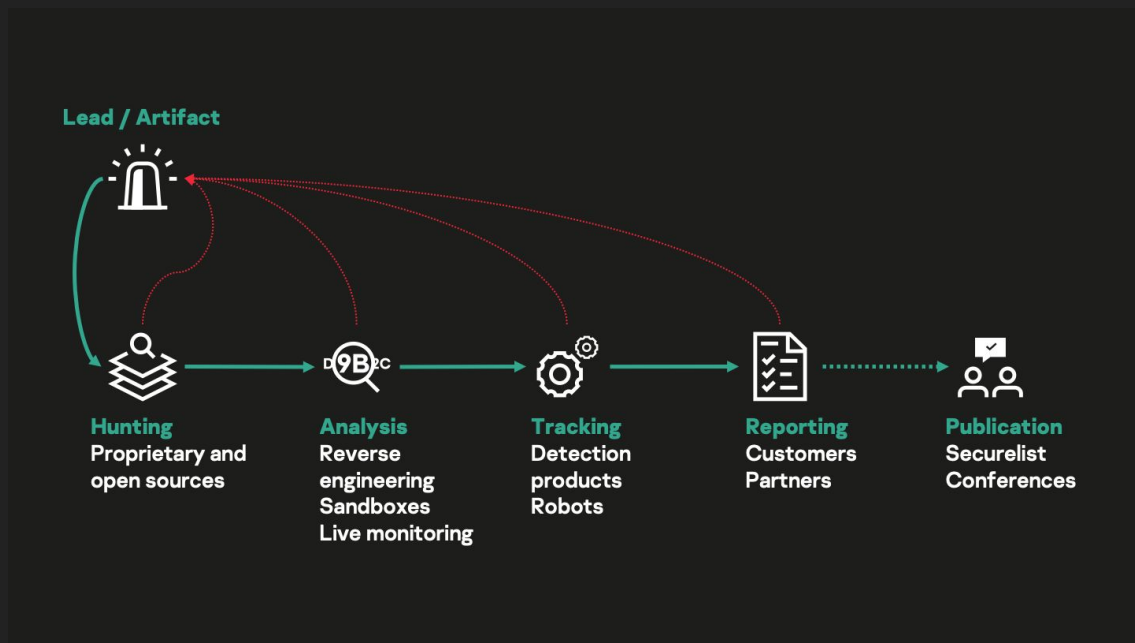
Dynamic: Observing the behavior of the malware in a controlled environment.

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.

```
root@kali:~/Desktop# volatility
Volatility 3 Framework 2.0.0 PD8 scanning finished

PID PPID ImageName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime
4 0 System 0xbdb0574ac000 153 - N/A False 2021-05-20 07:28:25.000000 N/A
** 312 4 smss.exe 0xbdb058d18000 2 - N/A False 2021-05-20 07:28:25.000000 N/A
** 492 312 smss.exe 0xbdb0596cd000 0 - 1 False 2021-05-20 07:28:39.000000 2021-05-20 07:28:40.000000
*** 584 492 winlogon.exe 0xbdb0599e0000 6 - 1 False 2021-05-20 07:28:40.000000 N/A
**** 664 584 userinit.exe 0xbdb05a5d6000 0 - 1 False 2021-05-20 07:31:33.000000 2021-05-20 07:31:49.000000
***** 1900 664 explorer.exe 0xbdb05a5e0000 112 - 1 False 2021-05-20 07:31:33.000000 N/A
***** 3384 1900 PCAScan.exe 0xbdb05a63a000 5 - 1 False 2021-05-20 07:32:06.000000 N/A
***** 5408 1900 chrome.exe 0xbdb05c67c000 26 - 1 False 2021-05-26 12:27:16.000000 N/A
***** 6312 5408 chrome.exe 0xbdb04d0a2000 10 - 1 False 2021-05-26 12:27:17.000000 N/A
***** 10308 5408 chrome.exe 0xbdb05b5f4000 6 - 1 False 2021-05-26 12:27:17.000000 N/A
***** 1832 5408 chrome.exe 0xbdb05c3a3000 12 - 1 False 2021-07-06 17:14:35.000000 N/A
***** 4112 5408 chrome.exe 0xbdb049d50000 13 - 1 False 2021-05-26 12:27:23.000000 N/A
***** 8116 5408 chrome.exe 0xbdb057eb4000 8 - 1 False 2021-05-26 12:27:16.000000 N/A
***** 4856 5408 chrome.exe 0xbdb05c4f63000 6 - 1 False 2021-05-26 12:27:19.000000 N/A
***** 6780 5408 chrome.exe 0xbdb04fb03000 22 - 1 False 2021-05-26 12:27:23.000000 N/A
***** 5428 1900 vmtoolsd.exe 0xbdb05a0e7000 9 - 1 False 2021-05-20 07:32:06.000000 N/A
***** 6648 1900 Process Hacker, 0xbdb05a0f4000 18 - 1 False 2022-01-13 09:52:53.000000 N/A
**** 926 584 dm.exe 0xbdb0598d00 11 - 1 False 2021-05-20 07:28:44.000000 N/A
*** 516 492 csrss.exe 0xbdb059900280 15 - 1 False 2021-05-20 07:28:39.000000 N/A
** 2228 4 MemCompression 0xbdb059440040 24 - N/A False 2021-05-20 07:28:46.000000 N/A
** 428 428 csrss.exe 0xbdb059250000 11 - 0 False 2021-05-20 07:28:39.000000 N/A
500 412 wininit.exe 0xbdb0598c2000 1 - 0 False 2021-05-20 07:28:39.000000 N/A
1 652 500 lsass.exe 0xbdb0599c0000 8 - 0 False 2021-05-20 07:28:41.000000 N/A
1 636 500 services.exe 0xbdb059920000 9 - 0 False 2021-05-20 07:28:41.000000 N/A
** 4356 636 svchost.exe 0xbdb060833000 6 - 0 False 2021-05-26 12:20:35.000000 N/A
** 2056 636 vmtoolsdService, 0xbdb059180000 2 - 0 False 2021-05-20 07:28:46.000000 N/A
** 648 636 sedsvc.exe 0xbdb059100000 7 - 0 False 2021-05-20 07:30:50.000000 N/A
** 1804 636 MpPmpg.exe 0xbdb059c54000 13 - 0 False 2021-05-20 07:28:46.000000 N/A
** 6540 636 svchost.exe 0xbdb061890000 7 - 0 False 2022-01-13 09:53:19.000000 N/A
** 2004 636 vmtoolsdService, 0xbdb059ca8000 2 - 0 False 2021-05-20 07:28:46.000000 N/A
*** 2384 2004 vmtoolsdService, 0xbdb059d92000 2 - 1 False 2021-05-20 07:28:47.000000 N/A
** 1608 636 spoolsv.exe 0xbdb05d135200 4 - 0 False 2022-01-13 09:53:29.000000 N/A
** 1684 636 spoolsv.exe 0xbdb0596bf000 14 - 0 False 2021-05-20 07:28:45.000000 N/A
** 1948 636 svchost.exe 0xbdb059ca3000 15 - 0 False 2021-05-20 07:28:46.000000 N/A
** 180 636 svchost.exe 0xbdb059a00000 28 - 0 False 2021-05-20 07:28:44.000000 N/A
** 2724 636 dlhhost.exe 0xbdb059f98000 12 - 0 False 2021-05-20 07:28:48.000000 N/A
** 452 636 svchost.exe 0xbdb0586e7000 8 - 0 False 2021-05-20 07:28:44.000000 N/A
*** 6180 1652 audiodg.exe 0xbdb05ee59000 7 - 0 False 2021-07-06 17:16:18.000000 N/A
```

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 smsfwd.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 smsfwd.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 smsfwd.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