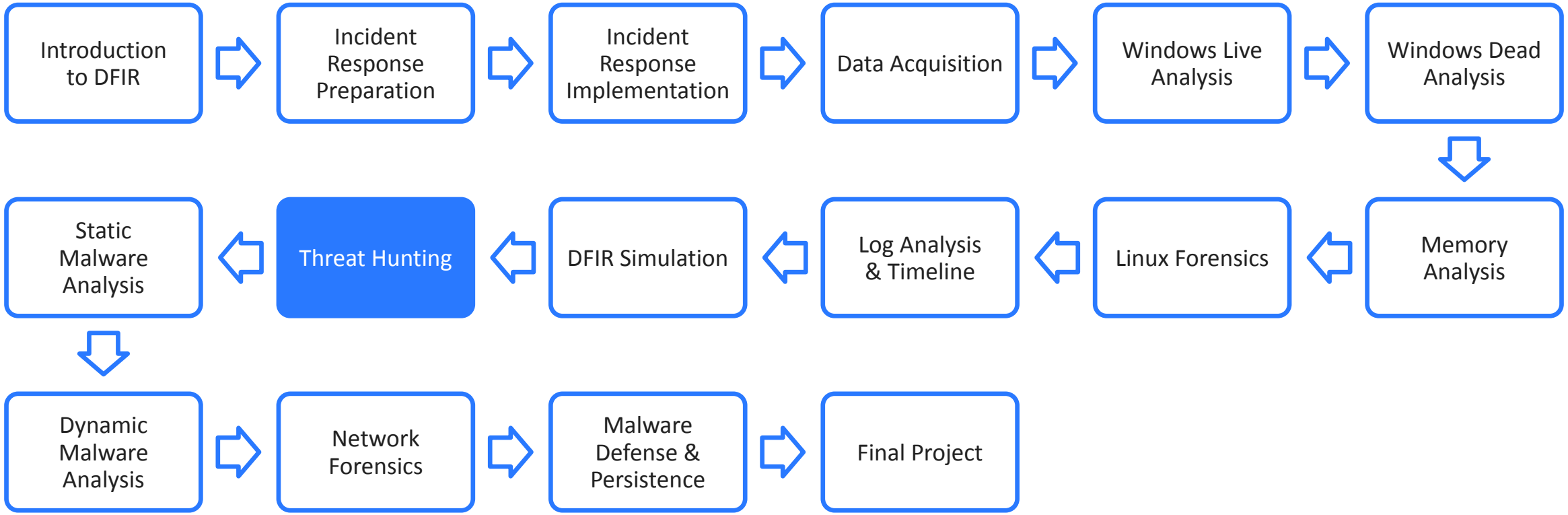
Cybersecurity Professional Program

Threat Hunting

Digital Forensics & Incident Response

Digital Forensics & Incident Response

Course Path



Objectives

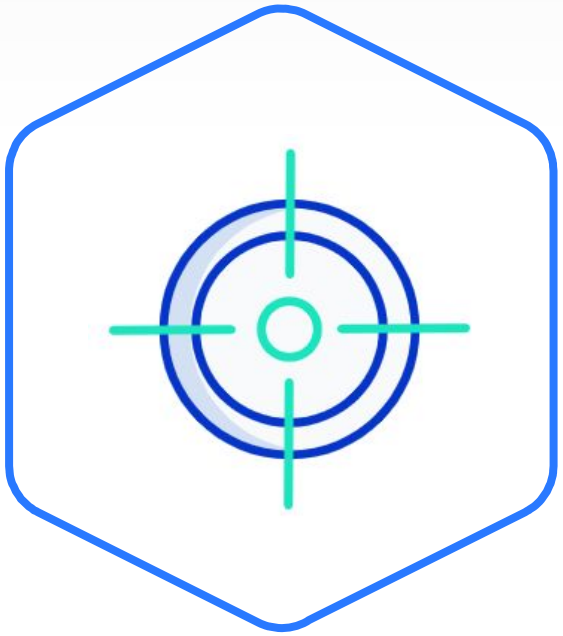
This lesson explains what threat hunting is and demonstrates the cyberthreat investigation process. It also explains the differences between threat hunting and threat intelligence.

- Threat Hunting & Intelligence
- Threat Exchange
- Malware Forensics

Threat Hunting

Threat Hunting & Intelligence

Threat Hunting



- Threat hunting is a proactive approach to handling cyberattacks.
- Its aim is to protect an organization from covert cyberthreats.
- It typically is performed by Tier 3 SOC personnel.

> The average breach can go undetected for more than six months.

Threat Intelligence

- Threat intelligence is based on learning from other's mistakes.
- Forensic researchers can learn about new exploitation techniques from public sources.

> Threat intelligence involves much more than simply reading an article about a breach.

Threat Hunting vs. Threat Intelligence

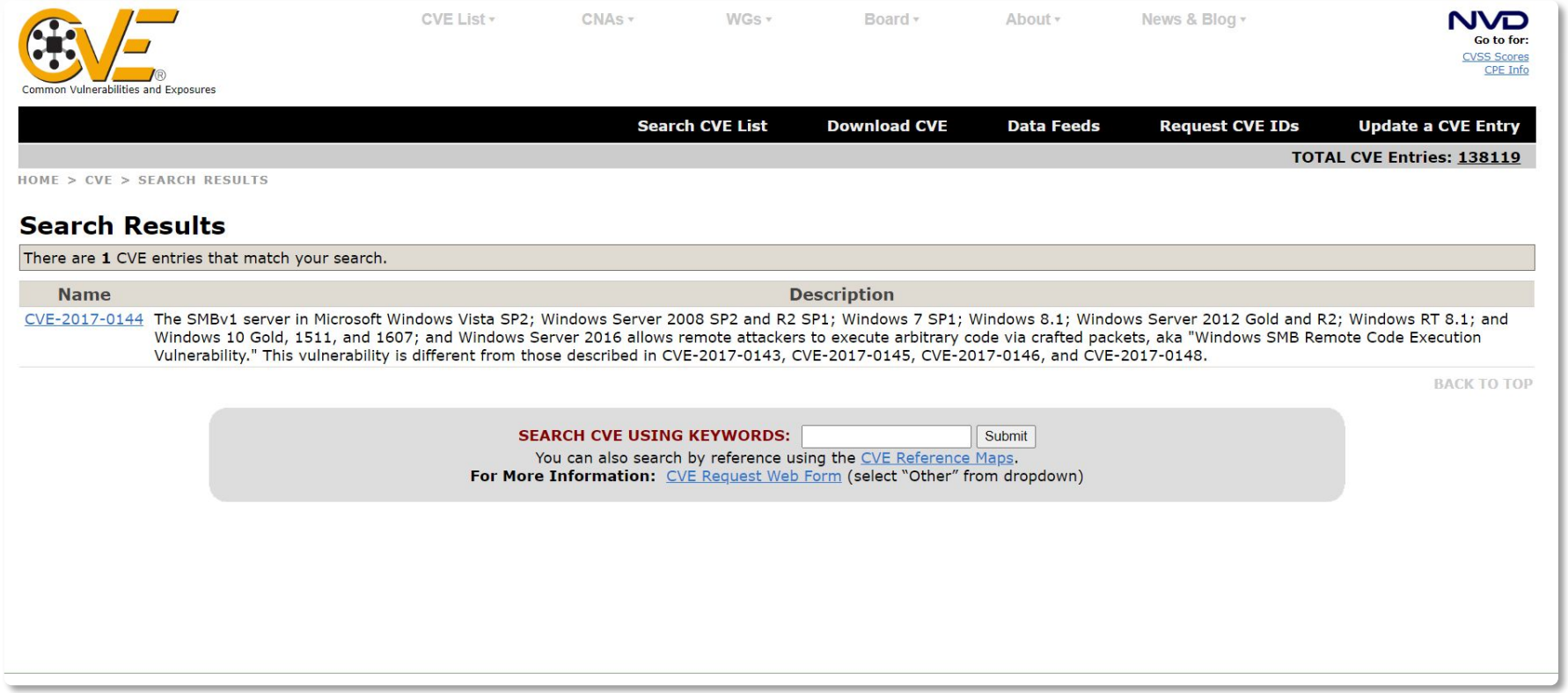
- **Threat intelligence** involves obtaining threat-related information from various sources.
- The technique is used to improve the level of security in an organization.

- **Threat hunting** involves the discovery of seemingly undetectable breaches.
- The process investigates anomalies and suspicious activity.

> Threat hunting includes forensics, log parsing, and research.

Hunting for Threats via CVEs

- As part of threat hunting, a researcher may look for well-known CVEs.
- A potential attack vector for a computer may be a documented CVE.
- Search engines for CVEs include ***https://cve.mitre.org/***



From: ThriveDX

Short Practice

CVE Details

20–30 Min.

Mission

> Search for CVE details about BlueKeep and SMB ghost exploits.

Steps

Search for an exact CVE ID number:

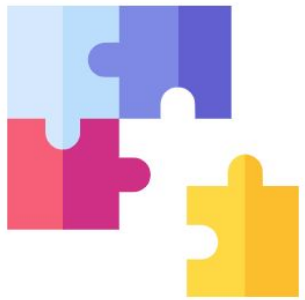
- Go to ***https://cve.mitre.org/***
- Click **Search**.
- Enter an exact CVE ID number.
- Note the information about the exploit.
- Answer the following questions:
  - What is the year of each CVE?
  - Which operating systems were exposed to it?
  - Which service was exploited?

Tracking Breaches

- Tracking CVEs is often not enough.
- More information must be gathered online.

- By sharing information about breach IOCs, a researcher can easily find potential attack vectors.
- The vectors can be used to compromise a network.

Indicators of Compromise



- An important part of dealing with a threat is obtaining IOCs.
- IOCs help determine if an organization was harmed by a threat that was implemented.
- IOCs can also be used to distinguish false positives.

Threat Hunting & Intelligence

Lab DFIR-11-L1

IOC Research

30–45 Min.

Mission

Download a dangerous malware and identify IOCs and the incident using Wireshark.

Steps

- Take a snapshot of your machine.
- Download a malware.
- Run the malware.
- Run Wireshark and analyze the traffic.

Environment & Tools

- VirtualBox
- 2x Windows 10 VM
- Wireshark

Related Files

- Lab document
- ***ExeFile.exe***

Threat Hunting

Threat Exchange

Known Threat Exchanges

IBM logo

IBM X-Force

AlienVault OTX logo

AlienVault OTX

CrowdStrike logo

CrowdStrike

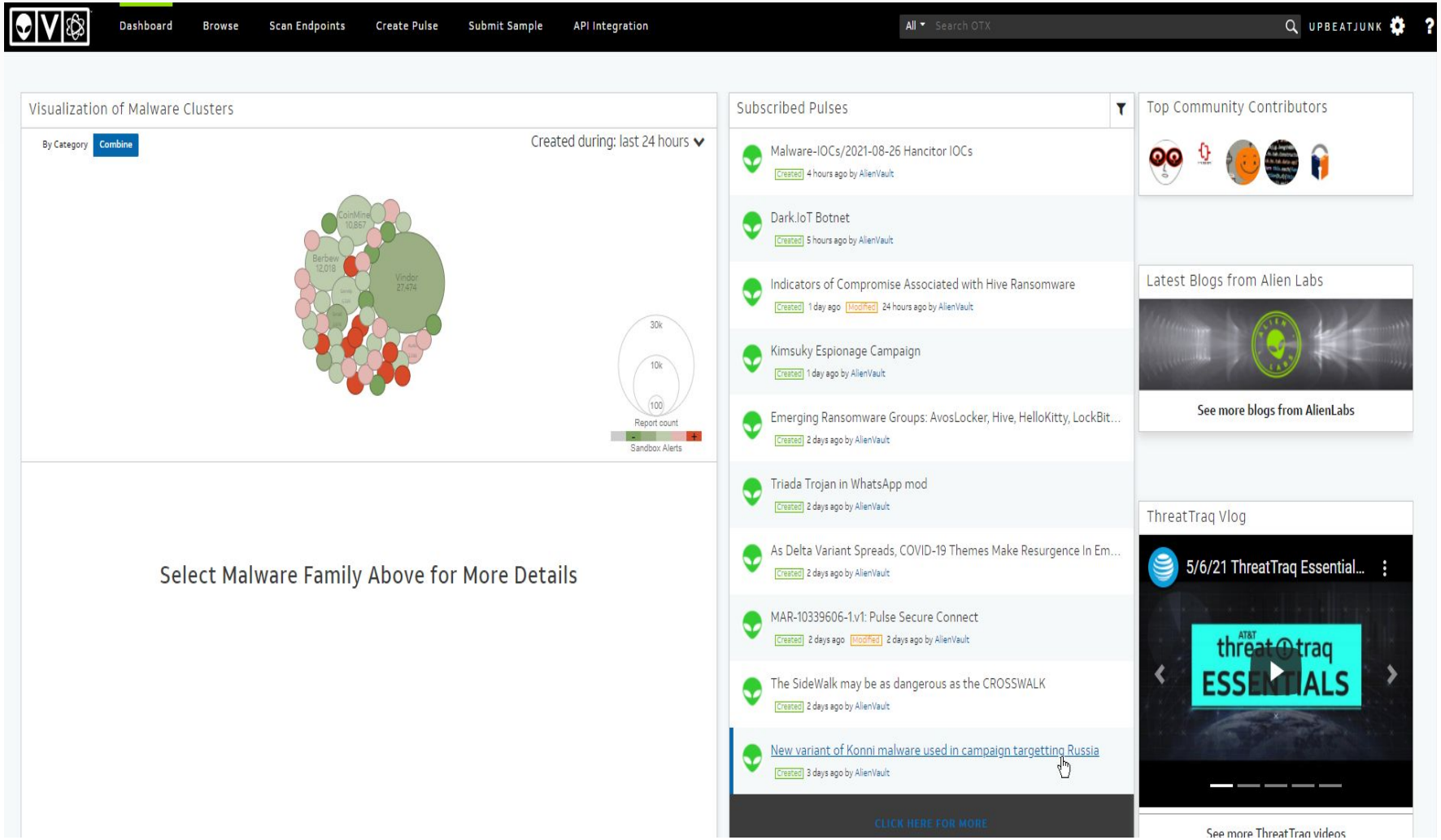
Facebook logo

Facebook

Threat Exchange

AlienVault Open Threat Exchange

- Different threat exchange platforms exists in the market.
- Their aim is to share information about newly discovered threats.
- AlienVault OTX is an example of a platform that shares information regarding threats: ***https://otx.alienvault.com***



From: ThriveDX

Threat Exchange

AlienVault OTX IOCs

- AlienVault OTX provides a list of discovered IOCs.
- It also offers a way to search for IOCs.

Dashboard | Browse | Scan Endpoints | Create Pulse | Submit Sample | API Integration

Profile

0 pulses

0 contributions

STATISTICS

0 FOLLOWERS | 0 SUBSCRIBERS | 0 CONTRIBUTED INDICATORS

GROUPS

No Groups

FOLLOWERS FOLLOWING

No Followers

SUBSCRIBERS SUBSCRIBING

No Subscribers

TOP COMMUNITY CONTRIBUTORS

Pulses | Activity | Suggested Edits

AlienVault | New | Updated | Subscribed

Malware-IOCs/2021-08-26 Hancitor IOCs — Unsubscribe (155,671)

CREATED 4 HOURS AGO by AlienVault | Public | TLP: White

FileHash-MD5: 18 | FileHash-SHA1: 3 | FileHash-SHA256: 3 | IPv4: 1 | URL: 32 | Domain: 6 | Email: 100

Hancitor IOCs collected by @executemalware

cobalt strike, hancitor

Dark.IoT Botnet — Unsubscribe (155,673)

CREATED 5 HOURS AGO by AlienVault | Public | TLP: White

CVE: 6 | FileHash-SHA256: 12 | IPv4: 7 | Domain: 2

Over the past several months, Radware researchers have been monitoring the evolution of a Mirai variant Radware have named "Dark.IoT." Palo Alto Networks first reported on this botnet on March 15, 2021. On August 6, 202...

Dark.IoT, Botnet, IoT

Indicators of Compromise Associated with Hive Ransomware — Unsubscribe (155,677)

CREATED 1 DAY AGO | MODIFIED 24 HOURS AGO by AlienVault | Public | TLP: White

FileHash-MD5: 2 | FileHash-SHA256: 1 | URL: 2 | Domain: 1

The FBI has released a FLASH of information related to the Hive ransomware, a type of ransomware that encrypts files and demands a ransom for their release, to help cyber security professionals guard against the persiste...

hive, Ransomware, HiveLeaks, FBI

Kimsuky Espionage Campaign — Unsubscribe (155,673)

CREATED 1 DAY AGO by AlienVault | Public | TLP: White

FileHash-MD5: 5 | FileHash-SHA1: 5 | FileHash-SHA256: 6 | Hostname: 1

A few days ago, InQuest found an exciting Javascript file masquerading as a PDF that, upon activation, will drop and display a PDF (to maintain the ruse) as well as drop an executable. The document is a lure for the Korean F...

kimsuky, javascript file, korean foreign, Keylogger, Espionage

Emerging Ransomware Groups: AvosLocker, Hive, HelloKitty, LockBit 2.0 — Unsubscribe (155,678)

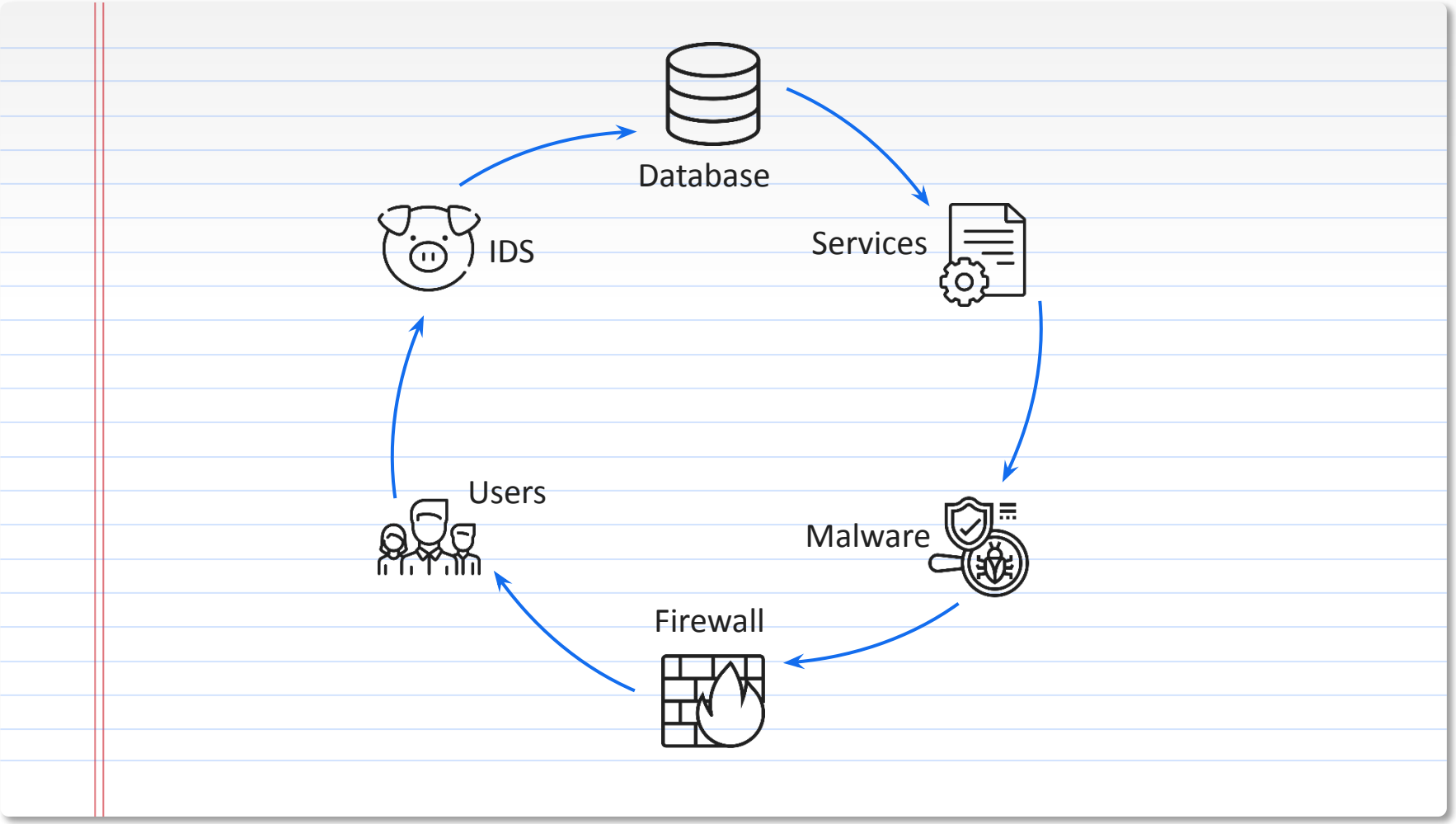
Emerging Ransomware Groups: AvosLocker, Hive, HelloKitty, LockBit 2.0

CREATED 2 DAYS AGO by AlienVault | Public | TLP: White

From: ThriveDX

Threat Hunting Cycles

- Threat hunting is often divided into separate categories.
- The hunt in each category will include different targets.
- A hunt cycle can be created to change the focus of the threat hunting process periodically.



From: ThriveDX

Threat Exchange

Lab DFIR-11-L2

Exploit Hunting

30–45 Min.

Mission

Enter AlienVault OTX and search for information about the **Mimikatz** tool.

Steps

- Enter the AlienVault website.
- Sign up.
- Look for data about the tool.
- Answer the questions in the lab document.

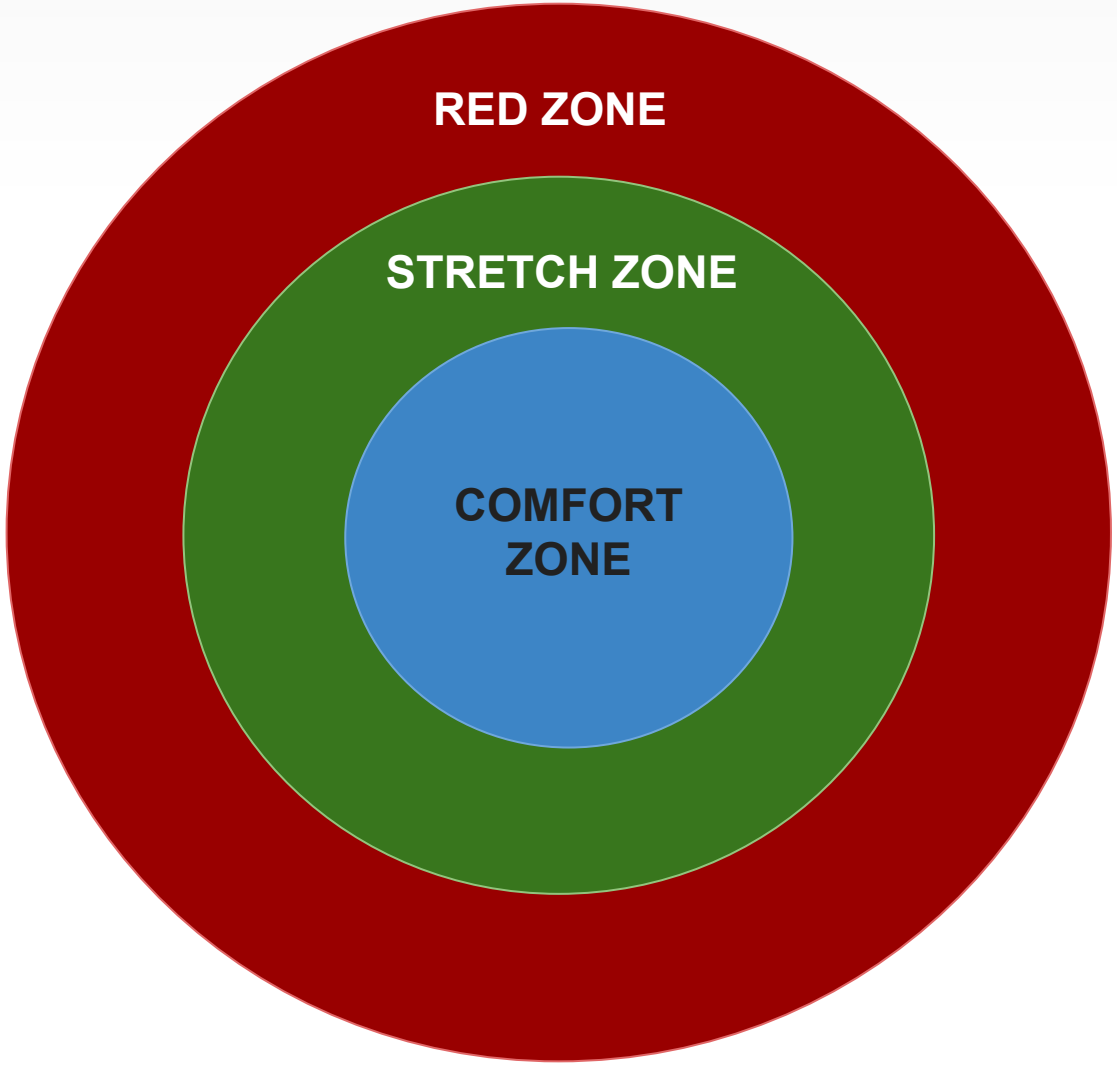
Environment & Tools

- Live internet connection

Related Files

- Lab document

Pulse Check



Threat Hunting

Malware Forensics

Malware

- Many types of malware have been developed.
- Each type behaves differently.
- Malware activity can be discovered by analyzing the behavior of a computer.

Suspicious Behavior

Increased Traffic

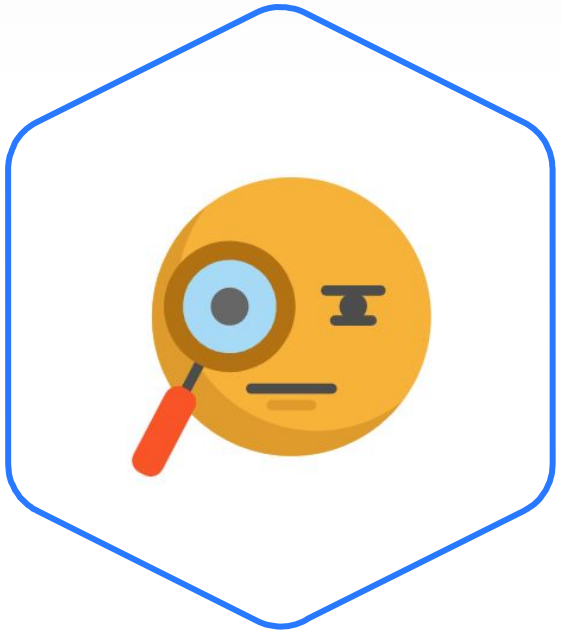
Accessed File Types

Service Inspection

Domain Identification

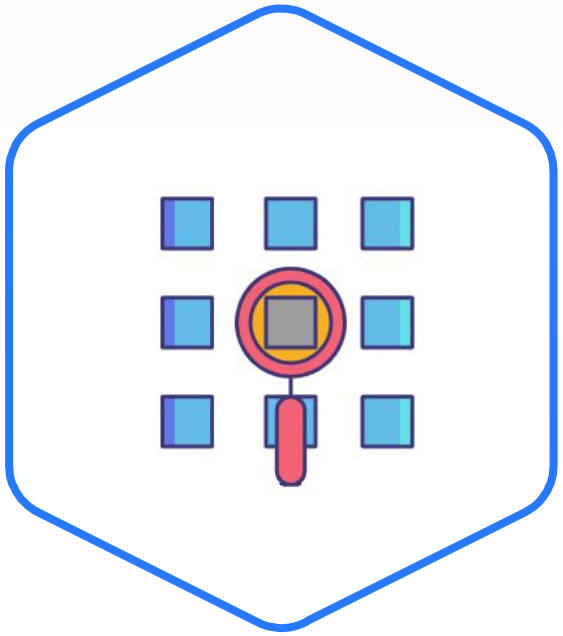
Persistence

Identifying Suspicious Behavior



- To identify malware activity, you must monitor suspicious system behavior continuously.
- You can use several tools to monitor such behavior, including Wireshark and PowerShell.

Zeek



- Zeek is a framework used to parse, normalize, and correlate logs.
- It focuses on extracting security-related information from logs to detect anomalies.
- Zeek was previously known as Bro.

> Zeek can read PCAP files and extract useful security-related fields from them.

Zeek Logs

- Zeek can monitor traffic on its own or investigate PCAP files.
- Zeek outputs log files in a structured format with predefined names.
- Zeek can also be used online to parse small PCAP files.

Output Logs

capture_loss | conn | files | http | known_hosts | known_services | software | stats

ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	resp_bytes	conn_state	local_orig
1320279554.496300	CP4xul1yHT2foPOrFc	192.168.2.76	52025	208.85.42.28	80	tcp	-	2.125850	0	1092421	SF	T
1320279567.181431	Cjs17X25qCHKv2aYXk	192.168.2.76	52034	174.129.249.33	80	tcp	http	0.082899	389	1495	SF	T
1320279567.452735	CAvEQu4y9Y7W1tCTVg	192.168.2.76	52035	184.72.234.3	80	tcp	http	2.561940	905	731	SF	T
1320279567.181050	C3iRM32TOAxIjiWG18	192.168.2.76	52033	184.72.234.3	80	tcp	http	3.345539	1856	1445	SF	T
1320279572.537165	CV68A621HcLNBRGDqk	192.168.2.76	52014	132.235.215.117	80	tcp	-	0.005881	0	0	SF	T
1320279578.886650	CHqmmW1P0DwTEWn6Rg	192.168.2.76	52052	63.241.108.124	80	tcp	http	0.498720	1566	2543	SF	T
1320279577.453637	CrNFnI0L5BIhWgrwc	192.168.2.76	52044	216.34.181.48	80	tcp	http	5.077548	596	576	SF	T
1320279581.284239	CkBXHPqxTSH298Zj	192.168.2.76	52059	207.171.163.23	80	tcp	-	5.056486	0	0	SF	T
1320279577.507914	CgMoDp338B42Pgya34	192.168.2.76	52045	216.34.181.45	80	tcp	http	11.654832	2603	181933	SF	T
1320279590.558878	CsbI5x2cPULQ9w2yYj	192.168.2.76	52077	74.125.225.78	80	tcp	-	5.048744	0	0	SF	T
1320279601.552309	C9FuZp4O97NgG5pfwc	192.168.2.76	52085	199.59.148.201	80	tcp	http	0.237418	883	1071	SF	T
1320279600.826685	C3TtpS2vmCJWrpdJ41	192.168.2.76	52083	192.150.187.43	80	tcp	http	5.233472	442	31353	SF	T
1320279600.826441	CEpN0Z5YJHPJNyCEk	192.168.2.76	52081	192.150.187.43	80	tcp	http	5.233763	446	24258	SF	T
1320279600.826004	CS8tjf10FX29qjdWPI	192.168.2.76	52080	192.150.187.43	80	tcp	http	5.404390	886	16577	SF	T
1320279600.825492	C1b1py4jQwSR5m6v04	192.168.2.76	52079	192.150.187.43	80	tcp	http	5.496459	1309	17849	SF	T
1320279600.826607	CwL1VE27p44Lmi5f37	192.168.2.76	52082	192.150.187.43	80	tcp	http	5.515177	1746	14412	SF	T
1320279600.581672	CIZv5A2jWBUmAMSymh	192.168.2.76	52078	192.150.187.43	80	tcp	http	5.825503	1599	80801	SF	T
1320279607.998777	CZvBU416RiwTdoesXk	192.168.2.76	52022	74.125.225.68	80	tcp	-	0.021505	0	0	SF	T
1320279607.998577	CmxTG1L0fWte3Jv14	192.168.2.76	52023	209.85.145.101	80	tcp	-	0.031533	0	0	SF	T

From: ThriveDX

Malware Forensics

Short Practice

Zeek Parsing

15–30 Min.

Mission

Use Zeek online to parse a PCAP file.

Steps

- Go to ***https://try.bro.org/***
- From the **Use PCAP** dropdown menu at the bottom, select ***exercise_traffic.pcap***.
- Click **Run**.
- Answer the following questions:
  - Which file types were downloaded?
  - How can a DFIR researcher find malware via the **Files** tab?
  - Which services are active in the organization?

Persistence

- Malware may use persistence techniques to preserve a foothold in a compromised computer.
- Persistence techniques may also constitute IOCs.
- Although many persistence techniques exist, malware developers typically stick to just a few.

> Since persistence is performed using high-level privileges, many types of malware launch privilege escalation attacks.

Common Hiding Mechanisms

Many hiding techniques are detailed at:
https://attack.mitre.org/tactics/TA0003/

Hiding Mechanism	Explanation
Registry Keys	Regedit can be used to hide and launch programs automatically.
Scheduled Tasks	A task can be scheduled to run a malicious payload.
Services	A malware service can be added to the system.
Startup Folder	Malware can be hidden in a startup folder.
AppCert DLLs	DLLs that run in every process can be infected.
Bootkit	MBR can be manipulated to load malware upon restart.

Analysis Process

Find
Find persistent malware.

Analyze
Analyze the file's hash and extract IOCs.

Others ?
Check if other machines are infected.

Anomaly
Find anomalies, such as suspicious IPs.

Conclusion
Should you continue to investigate the incident or not?

Malware Forensics

Lab DFIR-11-L3

Persistence Hunting

20–50 Min.

Mission

Create a persistent malware using Metasploit Framework (MSF) and hunt for its process.

Steps

- Create a malware using MSF.
- Run the persistence module.
- Investigate the persistence method.
- Run the analysis process.

Environment & Tools

- VirtualBox
- Windows 10
- Kali Linux

Related Files

- Lab document

Hiding from Analysis

- Many malware developers use well-known techniques for persistence.
- Some persistence methods are very difficult to monitor.

> For example, advanced malware can use process hollowing as a hiding technique.

Process Hollowing

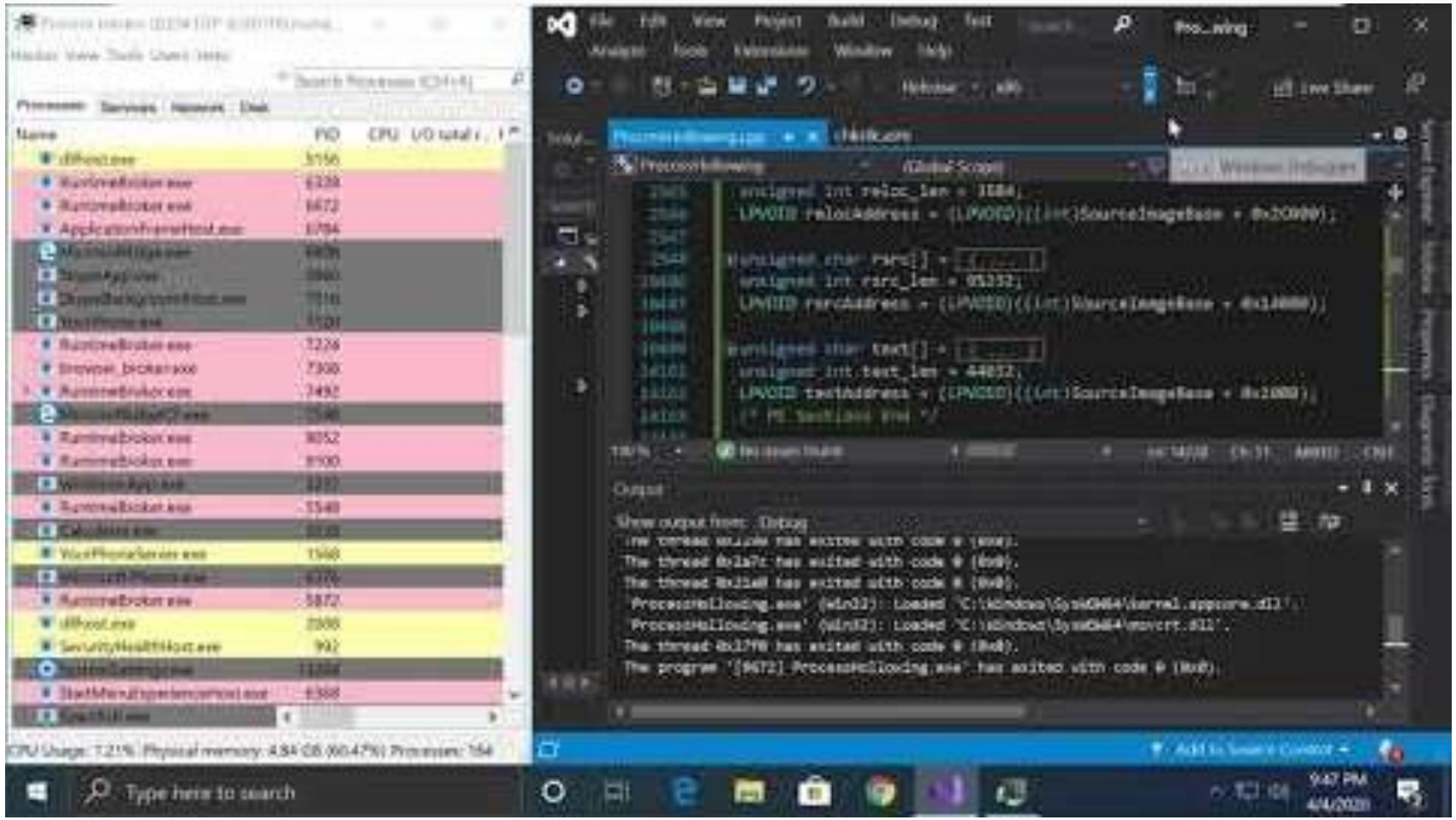
Main
Open the main process in suspend mode.

Copy
Open a malware and copy its contents.

Paste
Paste the copied contents to the process's memory.

Run
Run the hollowed process with the new content.

Process Hollowing Video



https://www.youtube.com/watch?v=5IyGiEajltM

From: YouTube (accessed 9/17/21)

Thank You

Questions?