

Mastering Cyber Defense:

Hands-On Training with Montimage Cyber Range

Session 2

Wissam Mallouli
Montimage, France



Key information of the company :

Type: SME

Creation date : 2004

Location: Paris, France

Employees : 15

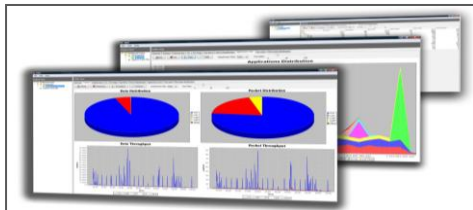
Expertise

- Cybersecurity – Risk management
- Network Monitoring and analysis
 - Classification of network traffic, Statistics, QoS/QoE
 - Incidents/Anomaly detection: behaviour, security and performance
- Research and innovation in different fields related to cybersecurity in future networks, 5G and beyond, IoT, CPS, cloud computing etc.
- Flagship tool: MMT for Montimage Monitoring Tool



Activity :

Analysis of network traffic - supervision, detection, decision making, reactions



Montimage



AI4CYBER



PRECINCT



DYNABIC



DETERMINISTIC6G



Objectives

- ▶ **Raise awareness** about the growing landscape of cyber threats and risks.
- ▶ **Understand common cyber attacks** through realistic simulations using the Montimage Cyberrange.
- ▶ **Learn to detect** intrusions and suspicious activities using advanced monitoring tools.
- ▶ **Explore effective response strategies** to mitigate cyber incidents in real-time.
- ▶ **Enhance readiness** by practicing incident handling in a controlled, simulated environment.
- ▶ **Promote** a proactive cybersecurity culture across teams and organizations.

Agenda

▶ **Part 1: Montimage ADR Cyber Range**

1. Introduction to ADR CR
2. Attack and Defense
3. Monitoring and Detection with Montimage Monitoring Tool (MMT)

▶ **Part 2: Hands-On the ADR CR - Practical exercises**

1. How to use the ADR CR
2. SSH Brute force attack
3. Nestea denial of service attacks

▶ **Part 4: Closing and Wrap-Up**

1. Summary of key takeaways
 2. Feedback collection from participants
-

Montimage ADR Cyber Range



Montimage Cyber-Range Target public

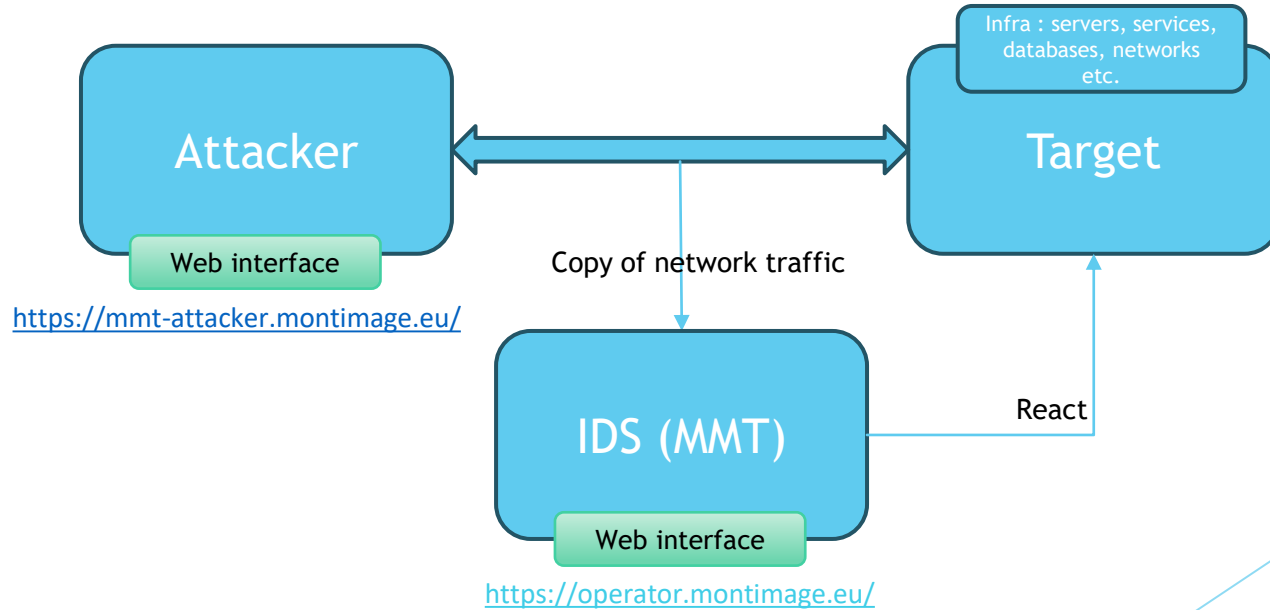
- ▶ Any employee of a company concerned by the development of good practices in terms of cyber security including
 - ▶ ~~Category 1: Non-ICT experts~~
 - ▶ Category 2: ICT experts
 - ▶ Category 3: Security experts

Montimage Cyber-Range - Fonctionnalités



- ▶ Traffic generation
- ▶ Attacks detection and reporting
- ▶ Reaction to attacks

Architecture



Architecture

Tcpreplay home

network

file

pcap

performance

support

tcpreplay

devices

flow

replay

send

test

traffic

Post

Tcpreplay - Pcap editing and replaying utilities

This is the official site for Tcpreplay version 4.0 and newer. The 3.x wiki and legacy Tcpreplay content is available [here](#).

Tcpreplay is a suite of free Open Source utilities for editing and replaying previously captured network traffic. Originally designed to replay malicious traffic patterns to Intrusion Detection/Prevention Systems, it has seen many evolutions including capabilities to replay to web servers.

Version 4.0.0 introduces features and performance enhancements to support switches, routers, and IP Flow/NetFlow appliances.

Example - 10GigE to IP Flow Appliance:

```
root@pw29:~# tcpreplay -i eth7 -tx --loop 5000 --unique-ip smallFlows.pcap
```

File Cache is enabled

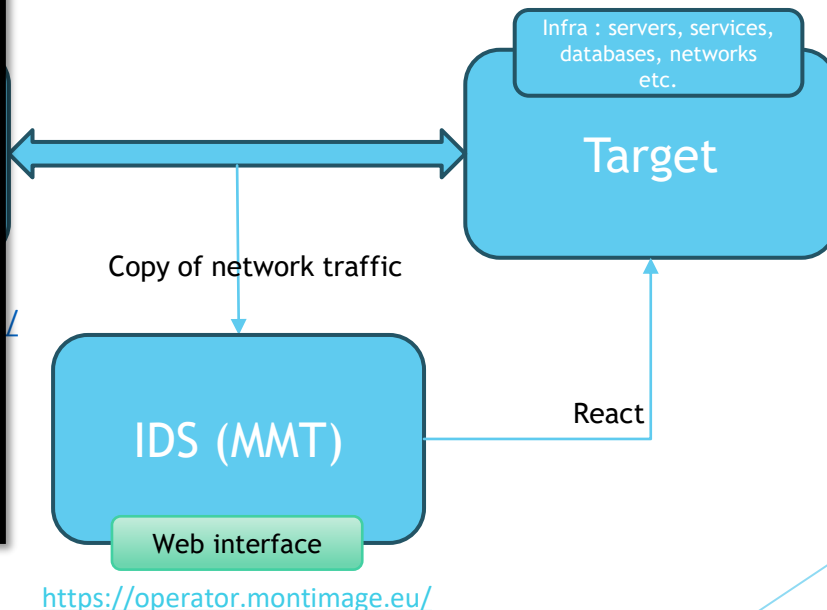
Actual: 71305000 packets (46082655000 bytes) sent in 38.05 seconds.

Rated: 1394330011.6 Bps, 9554.64 Mbps, 1848020.72 pps

Flows: 6045000 flows, 156669.03 fps, 71215000 flow packets, 90000 non-flow

Statistics for network device: eth7

Attempted packets:	71305000
Successful packets:	71305000
Failed packets:	0
Truncated packets:	0
Retried packets (ENOBUFS):	0
Retried packets (EAGAIN):	0



How to use the Montimage ADR

Montimage Cyber-Range - Fonctionnalités

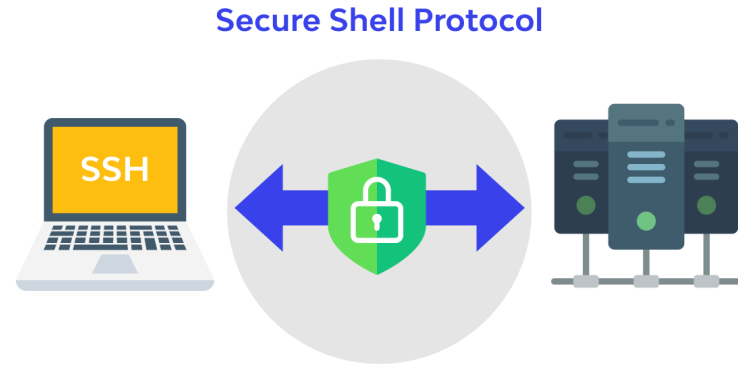
- Book a slot for testing the Montimage Cyber-Range:
<https://adr-reservation.montimage.eu/>
 - You'll receive a confirmation email
 - You'll receive credentials to connect
- MMT-Operator: <https://operator.montimage.eu/>
- MMT-Attacker: <https://mmt-attacker.montimage.eu/>

SSH Brute Force Attack

SSH brute force attack :

What is SSH and Why It Matters?

- ▶ SSH (Secure Shell) is a widely used protocol for secure remote login and system administration.
- ▶ Used by sysadmins and developers to manage servers and devices.
- ▶ Default port: 22 (unless configured otherwise).
- ▶ Highly targeted by attackers due to its powerful access capabilities.



SSH brute force attack : What is a brute force attacks ?

- ▶ A brute force attack is a method where an attacker tries many usernames and passwords repeatedly until access is gained.
- ▶ Often automated using tools (e.g., Hydra, Medusa, Ncrack).
- ▶ Exploits weak or default credentials.
- ▶ Goal: Gain unauthorized SSH access to a server.

#bash

hydra -l root -P passwords.txt ssh://192.168.1.100



SSH brute force attack : Anatomy of an SSH Brute Force Attack

- ▶ Step 1: Attacker scans for machines with open port 22.
- ▶ Step 2: Initiates repeated login attempts with different credentials.
- ▶ Step 3: May use dictionary or credential lists.
- ▶ Step 4: If successful, attacker gains shell access and control of the system.
- ▶ Often leads to further exploitation (e.g., installing malware, creating backdoors).

<https://attack.mitre.org/tactics/TA0006/>
<https://attack.mitre.org/techniques/T1110/>

Simulating the attack using the ADR Cyberrange

Pcap Traffic

Select a pcap file to be replayed

SSH brute force attack

Description

Several attempts to connect via ssh (brute force attack). Source address is either infected machine or attacker (no spoofing is possible).

This attack traffic can be detected by rule 1 ...

Parameters

Traffic output NIC	ens3	?	Max sleep (ms)		?
Preloads packets	yes	?	Loop	1	?
Delay between loops (ms)	0	?	Packet length		?
Number of packets to send		?	Timeout (second)		?

Security Alerts

Total: detected 9

Search:

Last updated	Probe ID	Property	Type	Verdict	Description
2025-04-13 19:22:05	3	56	attack	detected 7	Probable SYN flooding attack (Half TCP handshake without TCP RST)
2025-04-13 19:22:10	3	1	attack	detected 2	Several attempts to connect via ssh (brute force attack). Source address is either infected machine or attacker (no spoofing is possible).

Simulating the attack using the ADR Cyberrange

github.com/Montimage/mmt-security/blob/main/rules/1.ssh.xml

Montimage / mmt-security

Code Issues Pull requests 1 Actions Projects Wiki Security Insights Settings

Files

main + Q

Go to file t

.github

check

doc

rules

properties_all

.93.corrupted_ngap.xml.swp

1.ssh.xml

11.ip_size.xml

13.datainSYN.xml

15.nikto.xml

18.GRE.xml

20.icmp_flood.xml

21.ip_frag_off.xml

22.ip_frag_size.xml

23.ip_frag_ooo.xml

24.ip_frag.xml

25.ip_frag.xml

mmt-security / rules / 1.ssh.xml

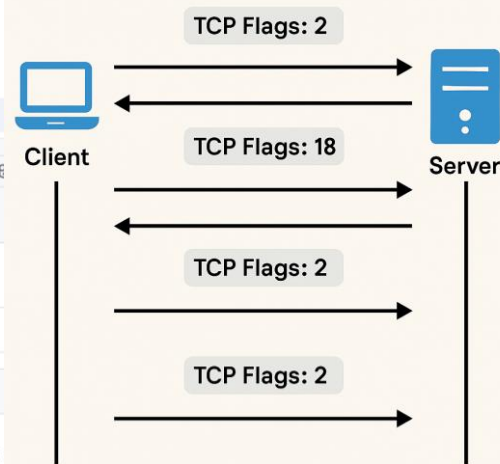
vinh_hoa ++new rule

Code Blame 22 lines (22 loc) · 1.5 KB

```
1 <beginning>
2 <!-- Property 1: Several attempts to connect via ssh (brute force attack). Source address is either infected machine or
3 <property value="THEN" delay_units="s" delay_min="0+" delay_max="5" property_id="1" type_property="ATTACK"
4 description="Several attempts to connect via ssh (brute force attack). Source address is either infected machine or attacker (no spoofing is possible).">
5 <operator value="THEN" delay_units="s" delay_min="0+" delay_max="3">
6 <event value="COMPUTE" event_id="1"
7 description="SYN request"
8 boolean_expression="((tcp.flags == 2)&&&((tcp.dest_port == 22)&&&(ip.src != ip.dst)))"/>
9 <event value="COMPUTE" event_id="2"
10 description="SYN ACK reply"
11 boolean_expression="((tcp.flags == 18)&&&((tcp.src_port == 22)&&&(ip.dst == ip.src.1)&&&(ip.src == ip.dst.1)))"/>
12 </operator>
13 <operator value="THEN" delay_units="s" delay_min="0+" delay_max="3">
14 <event value="COMPUTE" event_id="3"
15 description="2nd attempt"
16 boolean_expression="((tcp.flags == 2)&&&((tcp.dest_port == 22)&&&(ip.src == ip.src.1)&&&(ip.dst == ip.dst.1)))"/>
17 <event value="COMPUTE" event_id="4"
18 description="3rd attempt"
19 boolean_expression="((tcp.flags == 2)&&&((tcp.dest_port == 22)&&&(ip.src == ip.src.1)&&&(ip.dst == ip.dst.1)))"/>
20 </operator>
21 </property>
22 </beginning>
```

<https://github.com/Montimage/mmt-operator/tree/main/www/data/attack/pcap>

Abnormal Behavior



SSH brute force attack : How to Defend Against SSH Brute Force

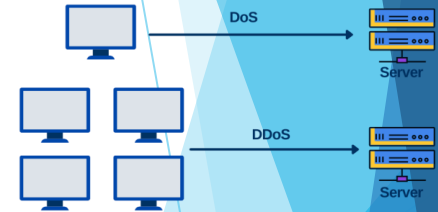
- ▶ Change default SSH port (not foolproof, but reduces noise).
- ▶ Disable root login via SSH.
- ▶ Use strong, unique passwords or better: SSH key-based authentication.
- ▶ Apply multi-factor authentication
- ▶ Limit SSH access via firewall rules or allowlists.
- ▶ Install tools like Fail2Ban: blocks IPs after too many failed attempts.

<https://attack.mitre.org/techniques/T1110/>

Nestea Denial of Service attack

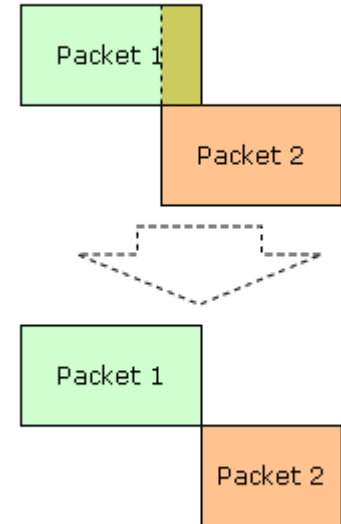
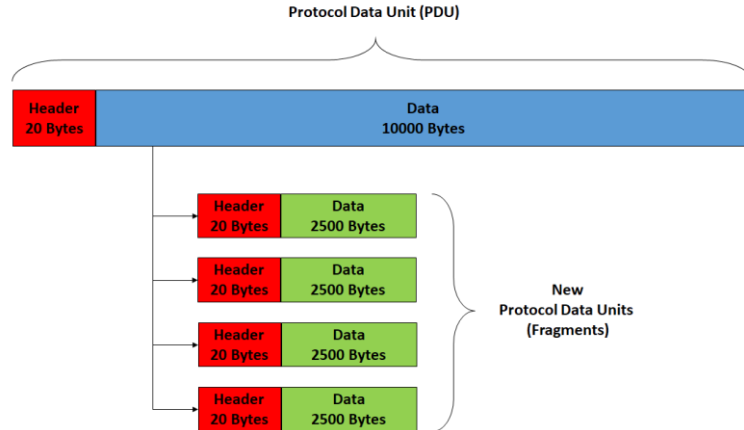
Nestea DoS: What is a Denial of Service (DoS) Attack ?

- ▶ A DoS attack aims to disrupt the normal functioning of a service by overloading or crashing it.
- ▶ It can target bandwidth, system resources, or protocol vulnerabilities.
 - ▶ Volumetric Attacks : Flood the target with massive traffic to saturate bandwidth.
 - ▶ Protocol Attacks : Exploit weaknesses in network protocols (TCP/IP, ICMP).
 - ▶ Application Layer Attacks: Target specific applications or services with resource-heavy requests.
 - ▶ Fragmentation Attacks : Send fragmented packets to exhaust reassembly logic.
 - ▶ Logic/Exploit-based Attacks: Exploit software bugs to crash or freeze the system.
- ▶ Nestea is a type of protocol-level and fragmentation related DoS.



Nestea DoS: What is a Denial of Service (DoS) Attack ?

- ▶ Nestea is a crafted IP fragmentation attack.
- ▶ Targets systems with poor handling of overlapping IP fragments.
- ▶ The result: kernel panic or system crash.



Nestea DoS: How Does Nestea Work?

- ▶ Attacker sends 3 IP fragments:
 - ▶ First fragment is normal.
 - ▶ Second fragment completes the datagram.
 - ▶ Third fragment overlaps previous data (confuses reassembly).
- ▶ Vulnerable systems fail during reassembly, causing a crash.

Nestea DoS: How Does Nestea Work?

The screenshot shows a GitHub repository for 'Montimage / mmt-security'. The file '52.nestea.xml' is selected in the 'Files' sidebar. The main content area displays the XML rule code, which is designed to detect Nestea DoS attacks by identifying malformed IP fragments and the last IP fragment. The rule includes comments and XML tags for property, operator, and event definitions.

Montimage / mmt-security

Search: Type / to search

<> Code Issues Pull requests 1 Actions Projects Wiki Security Insights Settings

Files

main + 🔍

Go to file t

- 45.TCP_Maimon_scan.xml
- 46.SCTP_COOKIE_ECHO_scan.xml
- 47.TCP_idle_scan.xml
- 48.FTP_bounce_scan.xml
- 5.arp.xml
- 51.ping_of_death.xml
- 52.nestea.xml**
- 53.ip_fragment_overrun.xml
- 54.EICARvirusTCP.xml
- 56.syn_flooding.xml
- 59.bogus_ip_version.xml
- 6.SYNFUL.xml
- 60.ip_option_non_standard.xml
- 62.ip_proto_id_non_standard.xml

mmt-security / rules / 52.nestea.xml

vinh_hoa.la New rules 51, 52 a5078e0 · 8 years ago History

Code Blame 18 lines (18 loc) · 1.13 KB

Raw Download Edit View

```
<beginning>
<!-- Property 52: This rule aims to detect Nestea DoS (also known as Off by one IP header) attack.
-->
<property value="THEN" delay_units="ms" delay_min="0+" delay_max="150" property_id="52" type_property="ATTACK"
  description="Malformed IP fragments. Possibly Nestea DoS attack.">
  <operator value="THEN" delay_units="ms" delay_min="0+" delay_max="100">
    <event value="COMPUTE" event_id="1"
      description="An IP fragment with MF flag"
      boolean_expression="((ip.src != ip.dst) &&& (ip.mf_flag == 1))"/>
    <event value="COMPUTE" event_id="2"
      description="Last IP fragment"
      boolean_expression="((ip.src == ip.src.1)&&&((ip.dst == ip.dst.1) &&& ((ip.identification == ip.identification.1) &&& ((ip.df_flag + ip.mf_
    </operator>
    <event value="COMPUTE" event_id="3"
      description="IP fragment comes after the last one"
      boolean_expression="((ip.src == ip.src.1)&&&((ip.dst == ip.dst.1) &&& ((ip.identification == ip.identification.1) &&& (ip.mf_flag == 1)))"/>
  </property>
</beginning>
```


Nestea DoS: Mitigation and Prevention

- ▶ Update the OS/kernel to patch known vulnerabilities.
- ▶ Use stateful firewalls that detect invalid fragments.
- ▶ Enable intrusion detection/prevention systems (IDS/IPS).
- ▶ Harden IP stack configurations to reject overlapping fragments.

Closing and Wrap-Up

Takeaways

- **Exploration of ADR Cyber Range:**
 - Understanding an attack allows to detect it and to react to it
 - The more « classical way » to react to an attacker is to block its IP source
 - Next session : AI-based anomaly detection

Post-training evaluation questionnaire

Profile

<https://forms.gle/VN22UYAZFnkiuB6h6>

Pseudo starts by ADR2.....

Post-training evaluation questionnaire

<https://forms.gle/JsA2nksf1LkuaH3Q6>

- ▶ Use the same pseudo
- ▶ Select training : [DAY 2] Mastering Cyber Defense: Hands-On Training with Montimage Cyber Range (Session 2) by Wissam Mallouli (MI)