



SupSec Seminar

Log Analysis Blueteam CTF

*CTF organized by
Malizen and AMOSSYS*



Blueteam CTF Context

MonkeyMoney is a NFT startup

Provides a market place to sell NFT (“monkeys”)

MonkeyMoney IT system security was not a priority...



Attack Day : January the 19th

Starting from 15h53, users cannot open a Windows session : AD server not reachable

Local connexion by admin to the AD server and... bim !

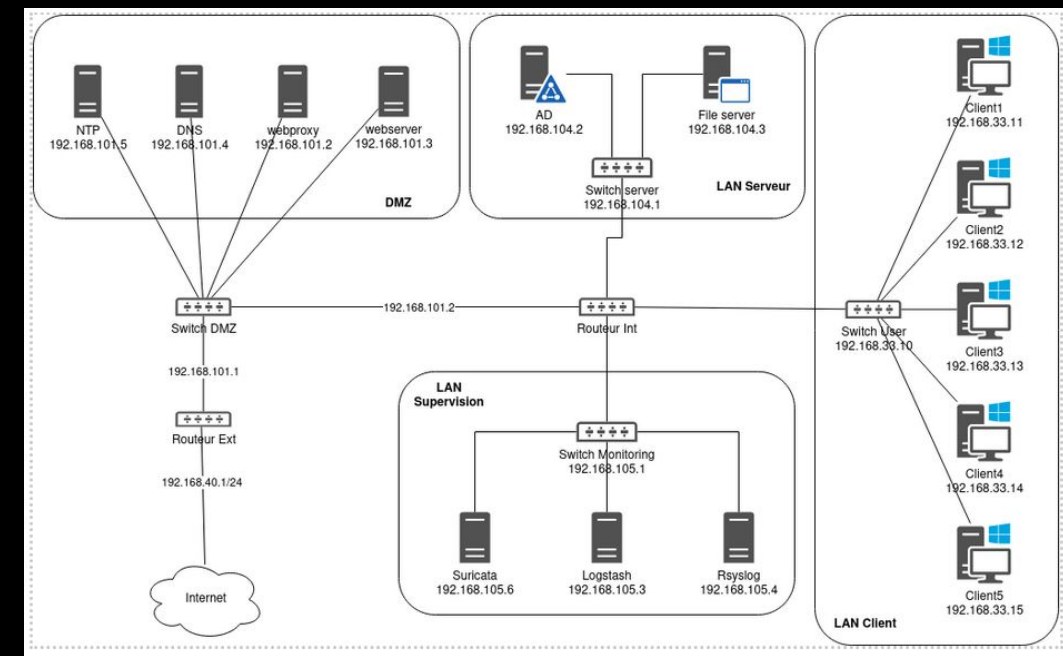


The day after

Your are an incident response analyst from CERTIFLEX

MonkeyMoney provides you with

- IT system topology
- Explanation of log collection chain
- And logs...



The challenge

For the challenge, logs are provided

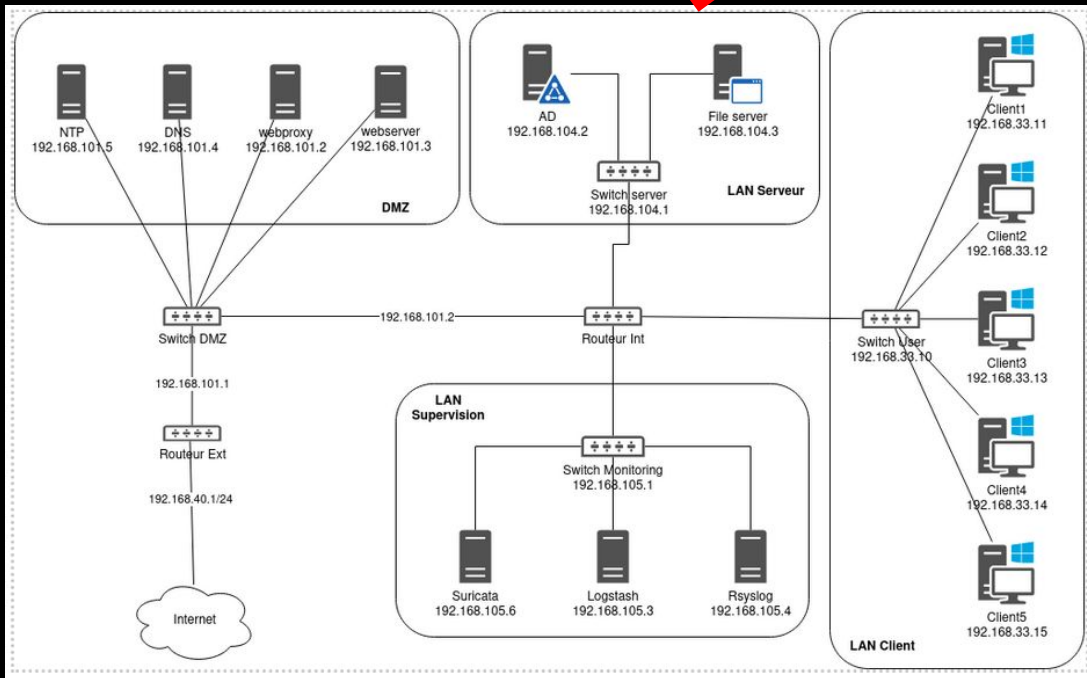
- as raw syslog files
- and either through Kibana (Elastic) : AMOSSYS competition
- or Malizen Investigation Platform : Malizen competition

```
$ wc */*
 517 ... CLIENT1/beats.log
 844 ... CLIENT2/beats.log
 544 ... CLIENT3/beats.log
 599 ... CLIENT4/beats.log
1059 ... CLIENT5/beats.log
1037 ... dcserver/beats.log
21077.. DNS/beats.log
  19 ... FileServer/beats.log
85602 ... Suricata/beats.log
 7719 ... webproxy/beats.log
  210 ... webserver/beats.log
119243 ... total
```

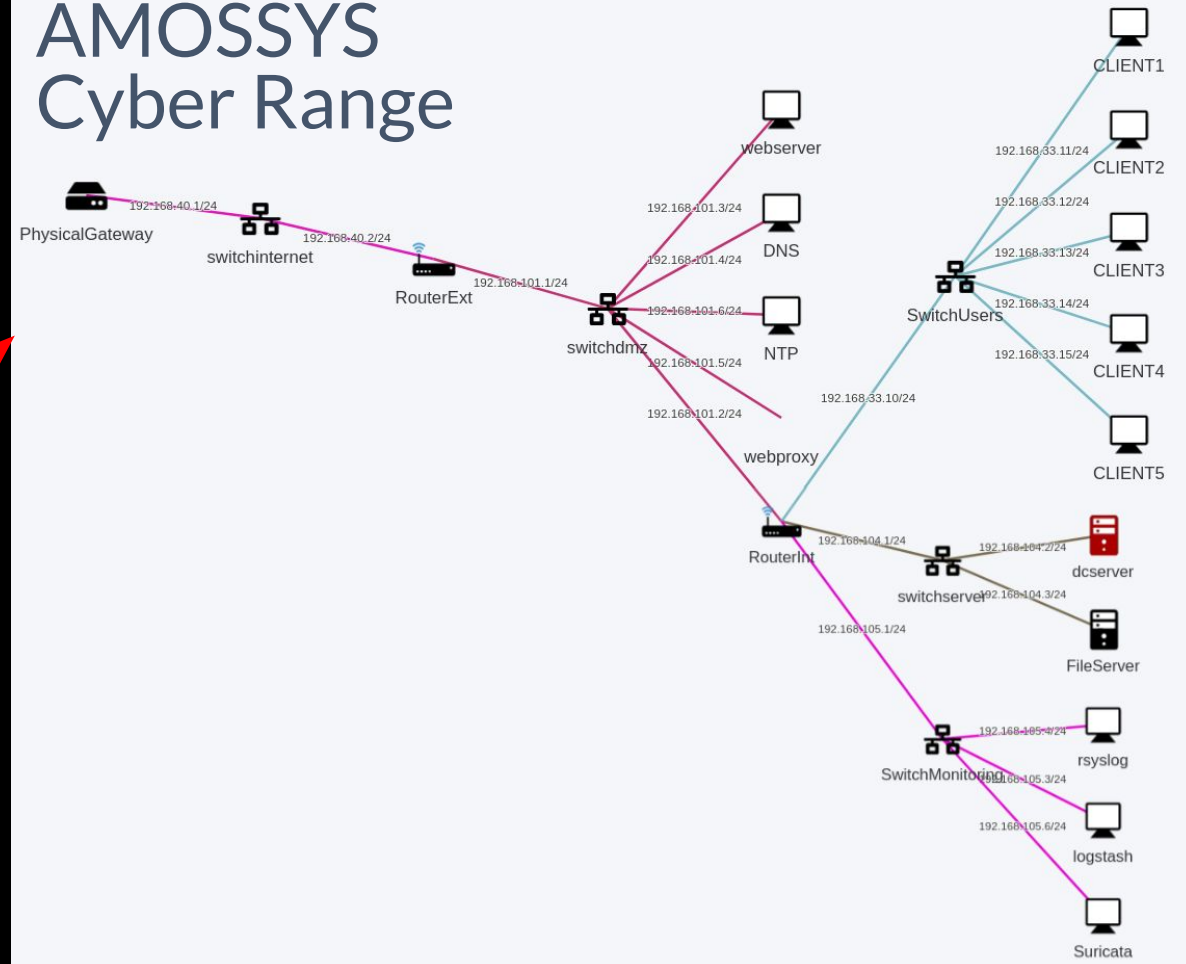
| Dataset generation : Behind the scene

Emulating IT system topology

Infrastructure as Code



AMOSSYS Cyber Range



Emulating life

On top of the emulated IT system

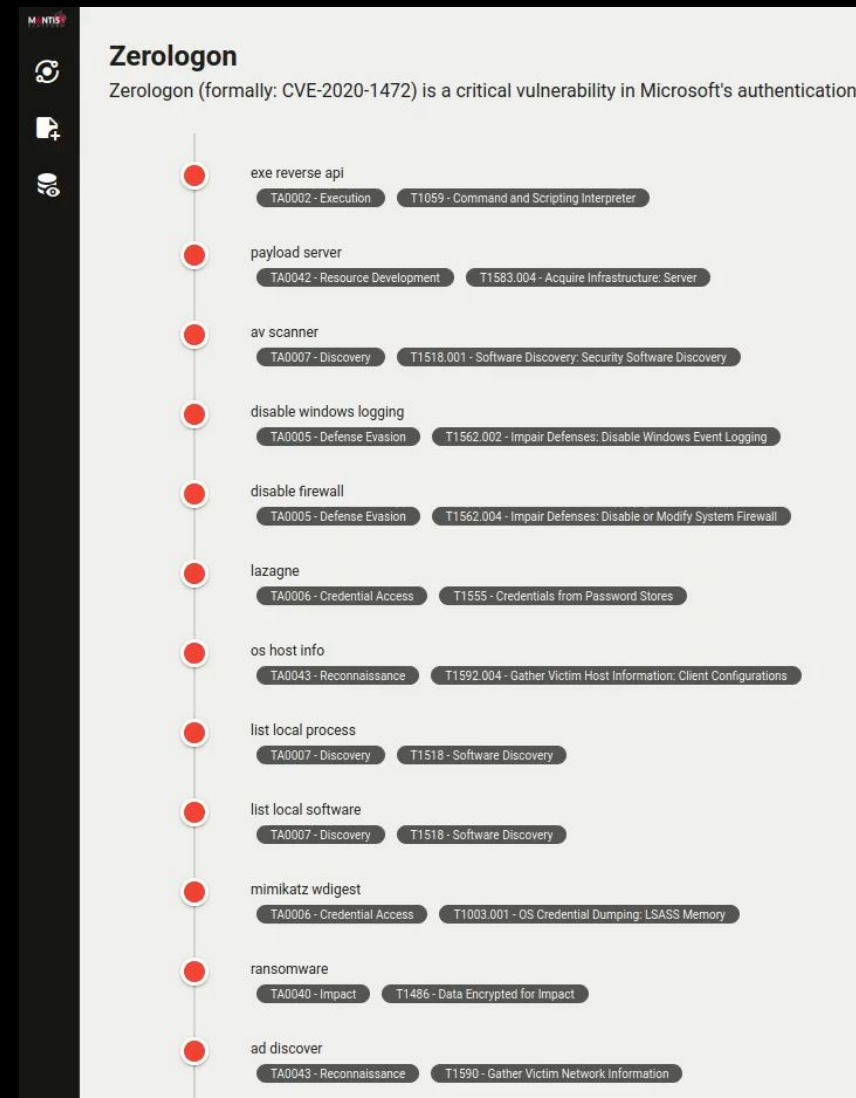
- provisioning of artefacts and data on all endpoints
- provisioning of weaknesses
- realistic legitimate user activity on desktop endpoints
 - agent-less
 - mostly automated :)

Emulating a threat actor

Attack scenario

- Log4Shell Tomcat exploitation from internet
 - 1105_000_001
- Connexion to C&C to retrieve orders
- Local discovery
 - 1518_000_001
- Lateral move to User LAN with scheduled task fetching Powershell script from Tomcat web server
- Multiple local discovery steps
 - 1007_000_001 / 1518_000_001
- Multiple network discovery steps
 - 1590_000_001 / 1046_000_002 / 1046_000_003
- Compromise of AD server with Zerologon exploit
 - 1046_000_003
- Ransomware deployed on AD server

Attack execution : expert system with pre- and post- conditions, and graph traversal



Validating the defense : Explainability of attack steps

Attack report containing metadata of attack steps

Attack scenario visualization

The diagram illustrates an attack scenario with the following steps and their associated TTPs:

- exe_reverse_api** (TA0002 - T1059) branches into:
 - payload_server (TA0042 - T1583)
 - disable_windows_logging (TA0005 - T1562)
 - disable_firewall (TA0005 - T1562)
 - lazagne (TA0006 - T1555)
 - list_local_process (TA0007 - T1518)
 - list_local_software (TA0007 - T1518)
 - mimikatz_wdigest (TA0006 - T1003)
 - ransomware (TA0040 - T1486)
 - ad_discover (TA0043 - T1590)
- ad_discover** leads to **intern_port_scan** (TA0007 - T1046)
- intern_port_scan** leads to **intern_netbios_scan** (TA0007 - T1046)
- intern_netbios_scan** leads to **intern_zerologon** (TA0008 - T1210)
- intern_zerologon** leads to **intern_secretdumps_smb** (TA0006 - T1003)
- intern_secretdumps_smb** leads to **lateral_winnm_control** (TA0008 - T1021)

On the right, a detailed view of the **intern_zerologon** step shows:

- Exploitation de la vulnérabilité Zerologon depuis une session d'attaque.**
- Status :** success
- Started date :** 2022-06-27 12:1...
- Last update date :** 2022-06-27 12:1...
- TA0008 - Lateral Movement**
- T1210 - Exploitation of Remote Services**
- Actions** (Download r...)
- Attempted Administrat...**
- ET EXPLOIT Possible Zerologon Phase 1/3 - NetrServerReqChallenge with 0x00 Client Challenge (CVE-2020-1472)**
- Event type :** alert
- Started date :** 2022-06-27T12:...
- Source :** 192.168.33.12:4...
- Destination :** 192.168.104.2:4...
- Protocole :** TCP

At the bottom, a timeline shows the sequence of steps: exe_reverse, payload_server, disable_wind, disable_firewall, agne, list_local, list_local_software, wdig, ransomware, ad_dis, intern_por, intern_net, intern_zerol, intern_secretdul, lateral_winnm_control.

M&NTIS Platform



Platform for testing efficiency of security products and SOC/CERT capabilities

Adversary Emulation on Cyber Range

Execution of real attack scenarios

- Attacker infrastructure
- Execution of TTPs on targeted system (MITRE ATT&CK)
- CTI/IoC injection from attack reports

Use cases: live testing and dataset generation

Financial support by
DGA MI and AID

