MASTER CS – ESIG GLOBAL SUCCESS

2024-2025

NETWORK FORENSICS

M. Emmanuel ONUOHA-IGWO Emmanuel

TRAFFIC ANALYSIS EXERCISE 1: BIG FISH IN A LITTLE POND

ASSOCIATED FILES:

Zip archive of the pcap: 2024-09-04-traffic-analysis-exercise.pcap.zip 1.7 MB (1,697,386 bytes)

Zip archive of the alerts: 2024-09-04-traffic-analysis-exercise-alerts.zip 453.9 kB (452,950 bytes)

NOTES:

Zip files are password-protected. For the password, refer to M. Emmanuel

BACKGROUND

Reviewing the alerts in your network environment, you find indicators that a host within your environment has been infected with malware.

SCENARIO

LAN segment details:

- LAN segment range: 172.17.0[.]0/24 (172.17.0[.]0 through 172.17.0[.]255)
- Domain: bepositive[.]com
- Active Directory (AD) domain controller: 172.17.0[.]17 - WIN-CTL9XBQ9Y19
- AD environment name: BEPOSITIVE
- LAN segment gateway: 172.17.0[.]1
- LAN segment broadcast address: 172.17.0[.]255

TASK

Write an incident report based on malicious network activity from the pcap and from the alerts.

The incident report should contains 3 sections:

- **Executive Summary**: State in simple, direct terms what happened (when, who, what).
- **Victim Details**: Details of the victim (hostname, IP address, MAC address, Windows user account name).
- **Indicators of Compromise (IOCs):** IP addresses, domains and URLs associated with the activity. SHA256 hashes if any malware binaries can be extracted from the pcap.

TRAFFIC ANALYSIS EXERCISE 2: NEMOTODES

ASSOCIATED FILES:

Zip archive of the pcap: 2024-11-26-traffic-analysis-exercise.pcap.zip 19.7 MB (19,664,067 bytes)

Zip archive of the alerts: 2024-11-26-traffic-analysis-exercise-alerts.zip 297.5 kB (297,496 bytes)

NOTES:

Zip files are password-protected. For the password, refer to M. Emmanuel

BACKGROUND

You work as a analyst at a Security Operation Center (SOC) for a medical research facility specializing in nemotodes. Alerts on traffic in your network indicate someone has been infected. You don't know which is more disgusting, the nemotodes or the malware.

Shown above: A test subject at the nemotode research facility. Lolss…

LAN segment details:

LAN segment range: **10.11.26[.]0/24** (10.11.26[.]0 through 10.11.26[.]255)

Domain: **nemotodes[.]health**

Active Directory (AD) domain controller: **10.11.26[.]3 - NEMOTODES-DC**

AD environment name: **NEMOTODES**

LAN segment gateway: **10.11.26[.]1**

LAN segment broadcast address: **10.11.26[.]255**

TASK

Write an incident report based on malicious network activity from the pcap and from the alerts.

The incident report should contains 3 sections:

Executive Summary: State in simple, direct terms what happened (when, who, what).

Victim Details: Details of the victim (hostname, IP address, MAC address, Windows user account name).

Indicators of Compromise (IOCs): IP addresses, domains and URLs associated with the activity. SHA256 hashes if any malware binaries can be extracted from the pcap.