OTLab 13
Jump Host

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

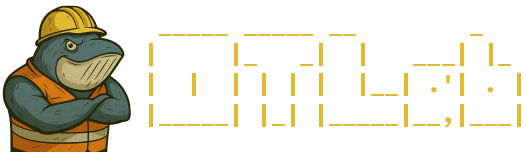
luiz.gutierres@ufsm.br

Problem Overview

Conduct an internal network security assessment for an industrial manufacturing organization. Your initial access point is a workstation (`corp-pc1`) within the corporate IT network. Your primary objective is to **identify security vulnerabilities or misconfigurations** that could allow a malicious actor **to pivot from the IT network into the organization's OT-ICS systems**. No network diagrams, asset inventories, or administrative credentials have been provided.

Tasks

1. Verify the IP address assigned to the `corp-pc1` workstation. `OTLab13{XXX.XX.X.XX}`
2. Determine the network subnet to which `corp-pc1` belongs. `OTLab13{XXX.XX.X.X/XX}`
3. From `corp-pc1`, identify the IP addresses and vendor (MAC OUI) information of other active hosts within the corporate network. `OTLab13{XXX.XX.X.XX:<Vendor>, XXX.XX.X.XX:<Vendor>, XXX.XX.X.XXX:<Vendor>}`
4. Identify at least one additional reachable network from `corp-pc1` by inspecting the system routing table. `OTLab13{XXX.XX.XX.X/XX via XXX.XX.X.XXX dev ethX}`
5. For the network discovered in the previous task, perform a TCP port scan and identify open ports and exposed services. *Hint: Use `--top-ports 50`. Hint: Firewall rules may restrict scanning on some hosts.* `OTLab13{XXX.XX.XX.XX:<Port>:<Service>}`
6. Using the results from the previous task, gain access to the jump host and locate the hidden flag within its directories. `OTLab13{Xxxx_Xx_Xxx_Xxxxx}`
7. Perform an `nmap` ping sweep to identify available OT-ICS hosts in the industrial network. Report their IP addresses and vendor information. `OTLab13{XXX.XX.XX.XX:<Vendor>, XXX.XX.XX.XX:<Vendor>, XXX.XX.XX.X:<Vendor>}`
8. For the OT-ICS device whose IP address has two identical digits in the last octet, identify the industrial protocol in use and extract the device's serial number. `OTLab13{XXXxxx, <Serial>}`
9. Another host on the industrial network exposes a web-based management interface. Explore the interface and retrieve the protected flag. `OTLab13{Xxxxxxx_Xxxxxxxxxxx}`
10. A suspicious message is being transmitted on the industrial network indicating an



operational issue. Intercept the message and identify the sender, recipient, and message content. `OTLab13{<Sender_IP>:<Recipient_IP>:Xxxxxxxxxxxxx_Xxxxx_Xxx}`

11. In the DMZ, an operational status message was transmitted and stored as a log record. Locate the record and identify the sender and the message content. `OTLab13{<Sender_IP>:Xxx_Xxx_Xxxxxx_X_Xx_Xxxxxxx}`

Note: Some OT-ICS devices are based on Conpot, which remaps standard protocol and service ports to non-privileged ports. Refer to the link for a list of some default and remapped ports.

Tools

The following tools are recommended for completing OTLab 13: `curl`, `ifconfig`, `ip`, `netdiscover`, `nmap`, `ssh`, and `tcpdump`.

Nomenclature

- DMZ: Demilitarized zone.
- ICS: Industrial control system.
- IP: Internet protocol.
- IT: Information technology.
- MAC: Media access control.
- OT: Operational technology.
- OUI: Organizationally unique identifier.
- SSH: Secure shell.