Module 10: IoT and OT Attacks and Countermeasures

Scenario

The significant development of the paradigm of the Internet of Things (IoT) is contributing to the proliferation of devices in daily life. From smart homes to automated healthcare applications, IoT is ubiquitous. However, despite the potential of IoT to make our lives easier and more comfortable, we cannot underestimate its vulnerability to cyber-attacks. IoT devices lack basic security, which makes them prone to various cyber-attacks.

The objective of a hacker in exploiting IoT devices is to gain unauthorized access to users' devices and data. A hacker can use compromised IoT devices to build an army of botnets, which, in turn, is used to launch DDoS attacks.

Owing to a lack of security policies, smart devices are easy targets for hackers who can compromise these devices to spy on users' activities, misuse sensitive information (such as patients' health records, etc.), install ransomware to block access to the devices, monitor victims' activities using CCTV cameras, commit credit-card-related fraud, gain access to users' homes, or recruit the devices in an army of botnets to carry out DDoS attacks.

You must have sound knowledge of hacking IoT and OT platforms using various tools and techniques. The labs in this module will provide you with real-time experience in performing footprinting and analyzing traffic between IoT and OT devices.

Objectives

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

- Performing IoT and OT device footprinting
- Capturing and analyzing traffic between IoT devices

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning

- Launch attacks
- Gain remote access
- Maintain access

Lab Tasks

We will use numerous tools and techniques to hack the target IoT and OT platforms. Recommended labs that will assist you in learning various IoT platform hacking techniques include:

1. Perform footprinting using various footprinting techniques
    - Gather information using online footprinting tools
2. Capture and analyze IoT device traffic
    - Capture and analyze IoT traffic using Wireshark

Lab 1: Perform Footprinting using Various Footprinting Techniques

**Lab Scenario**

Here, the first step is to gather maximum information about the target IoT and OT devices by performing footprinting through search engines, advanced Google hacking, Whois lookup, etc.

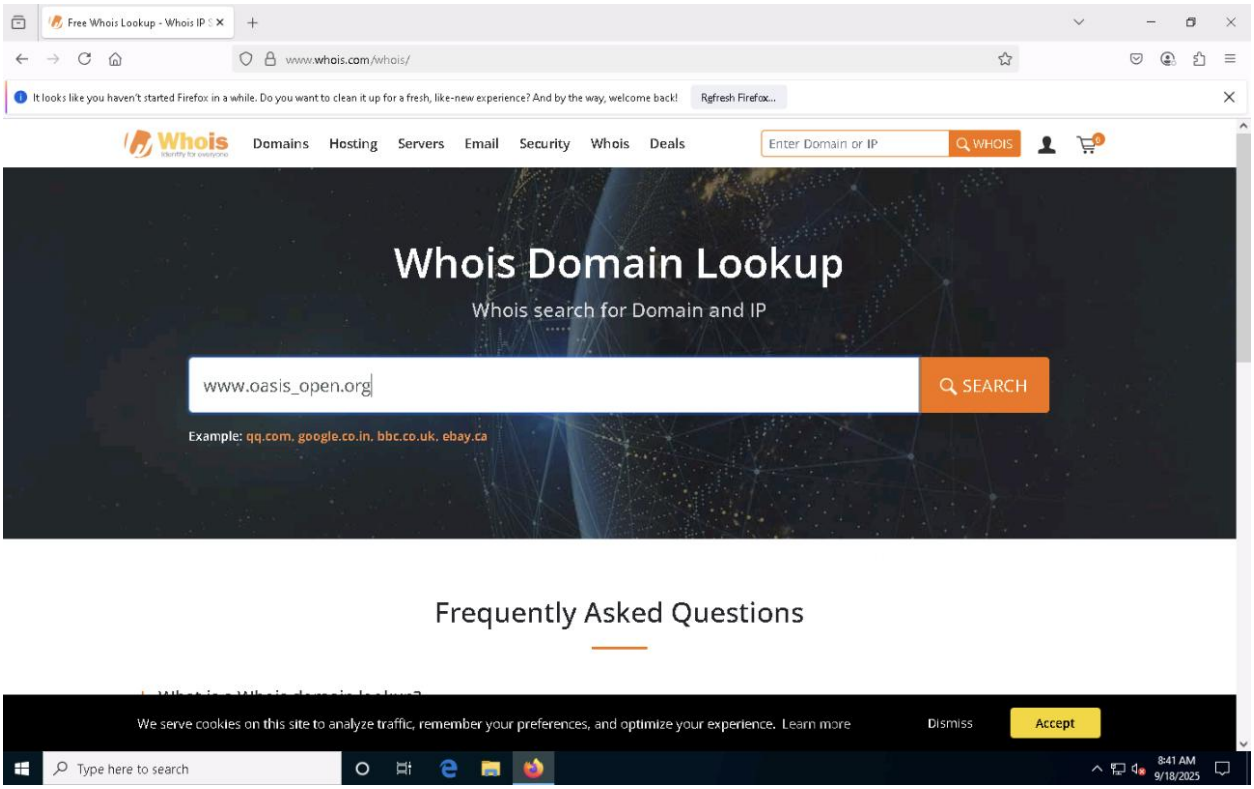
The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

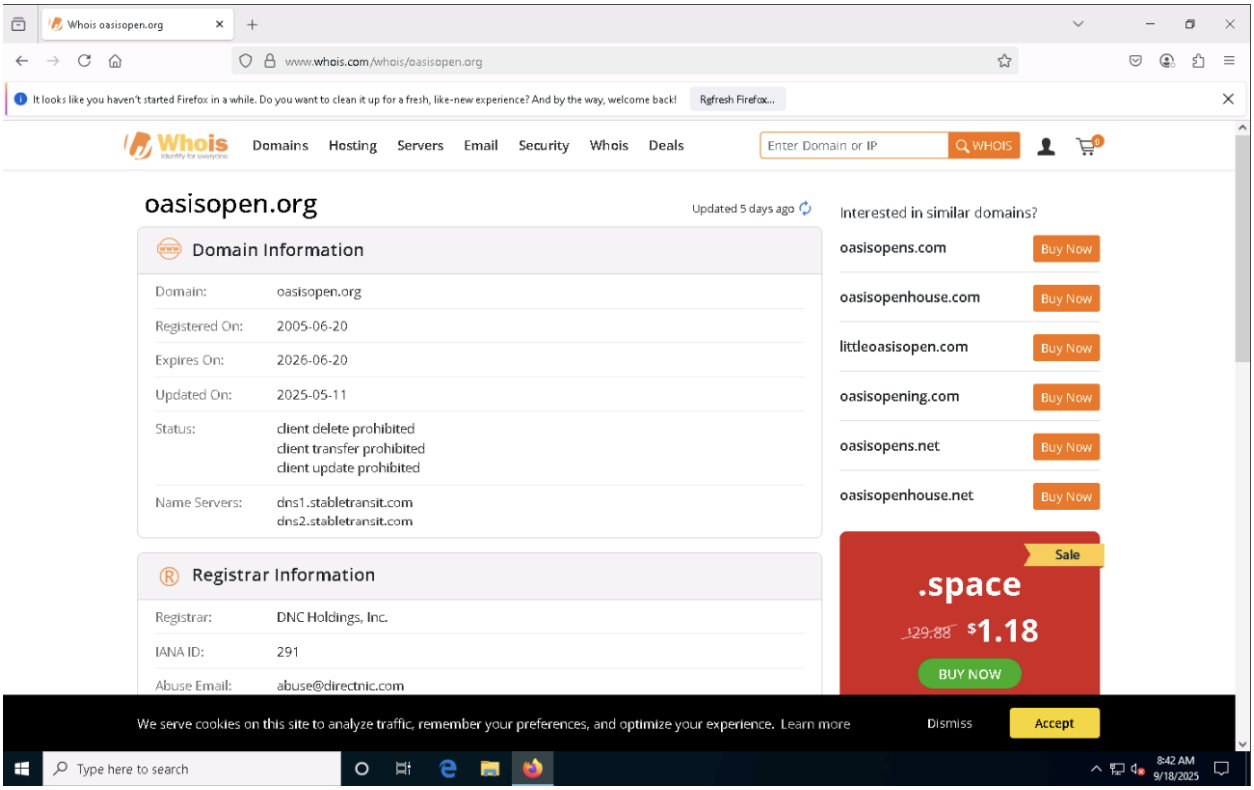
**Lab Objectives**

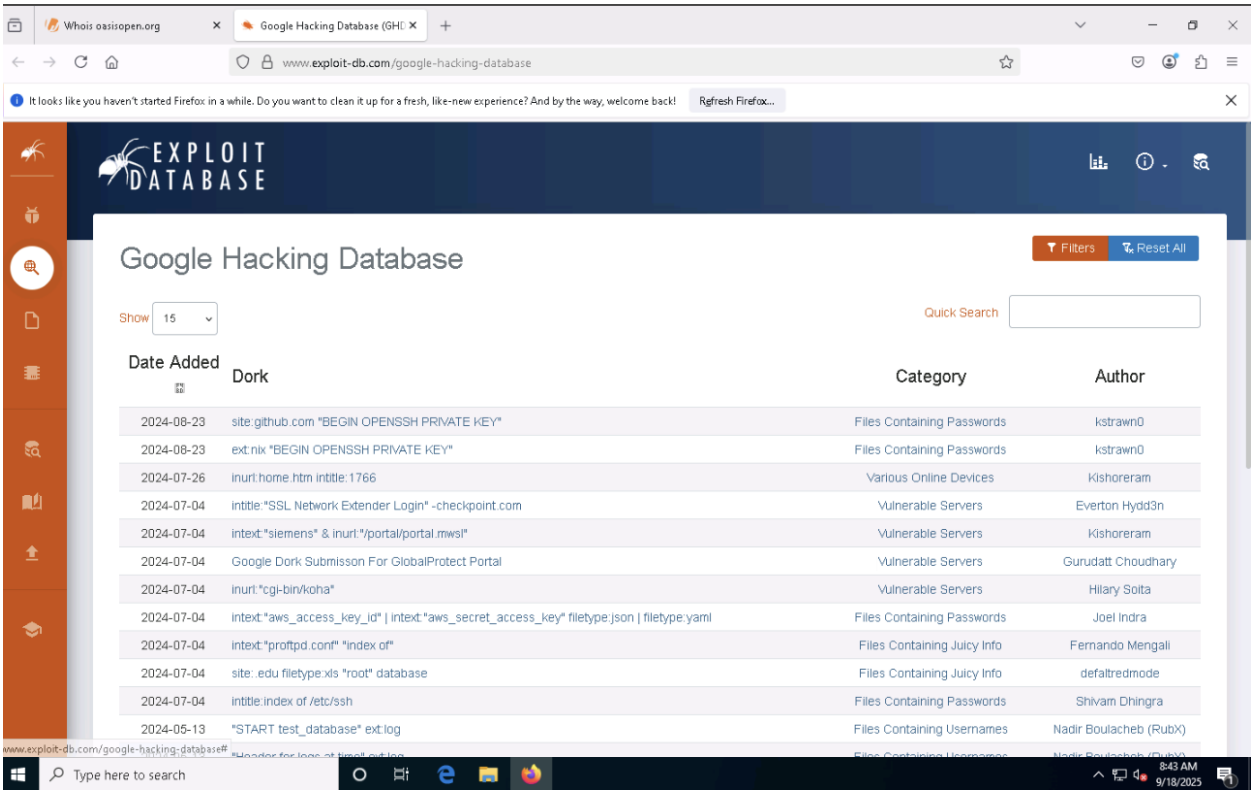
- Gather Information using Online Footprinting Tools

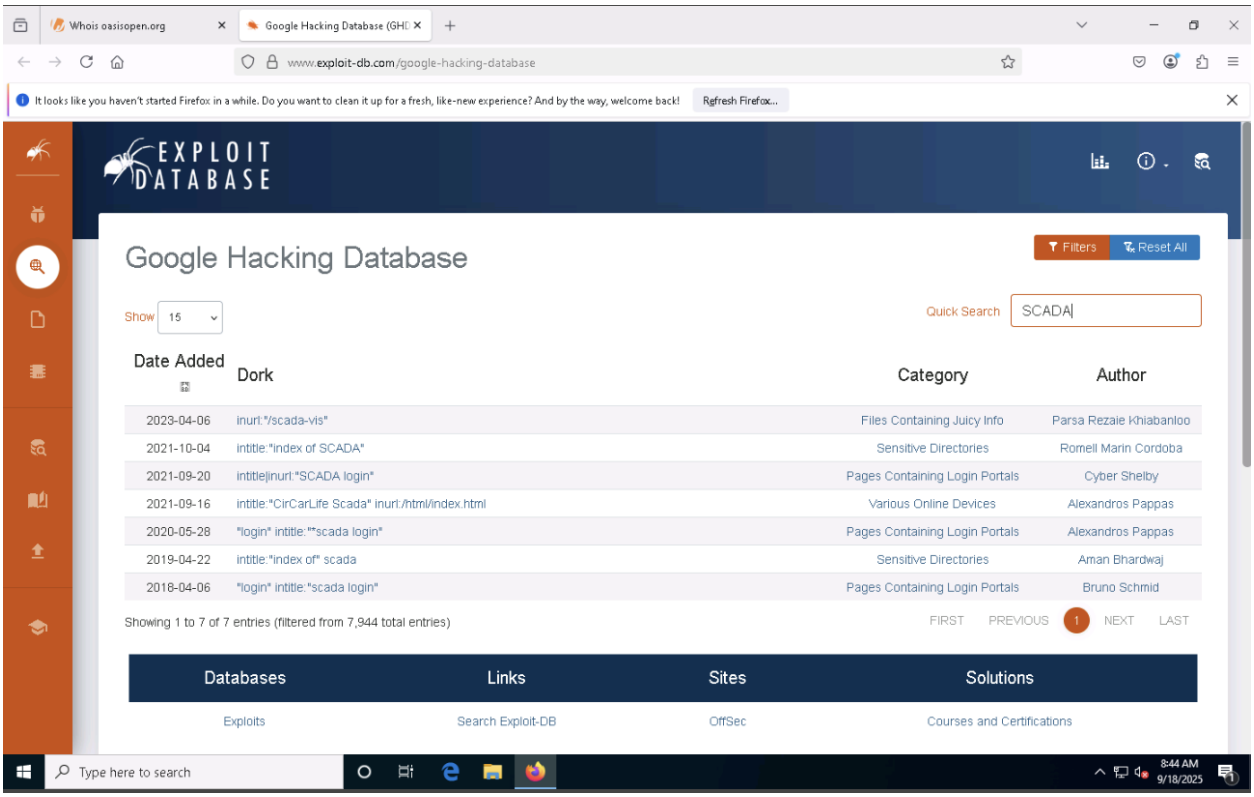
Task 1: Gather Information using Online Footprinting Tools

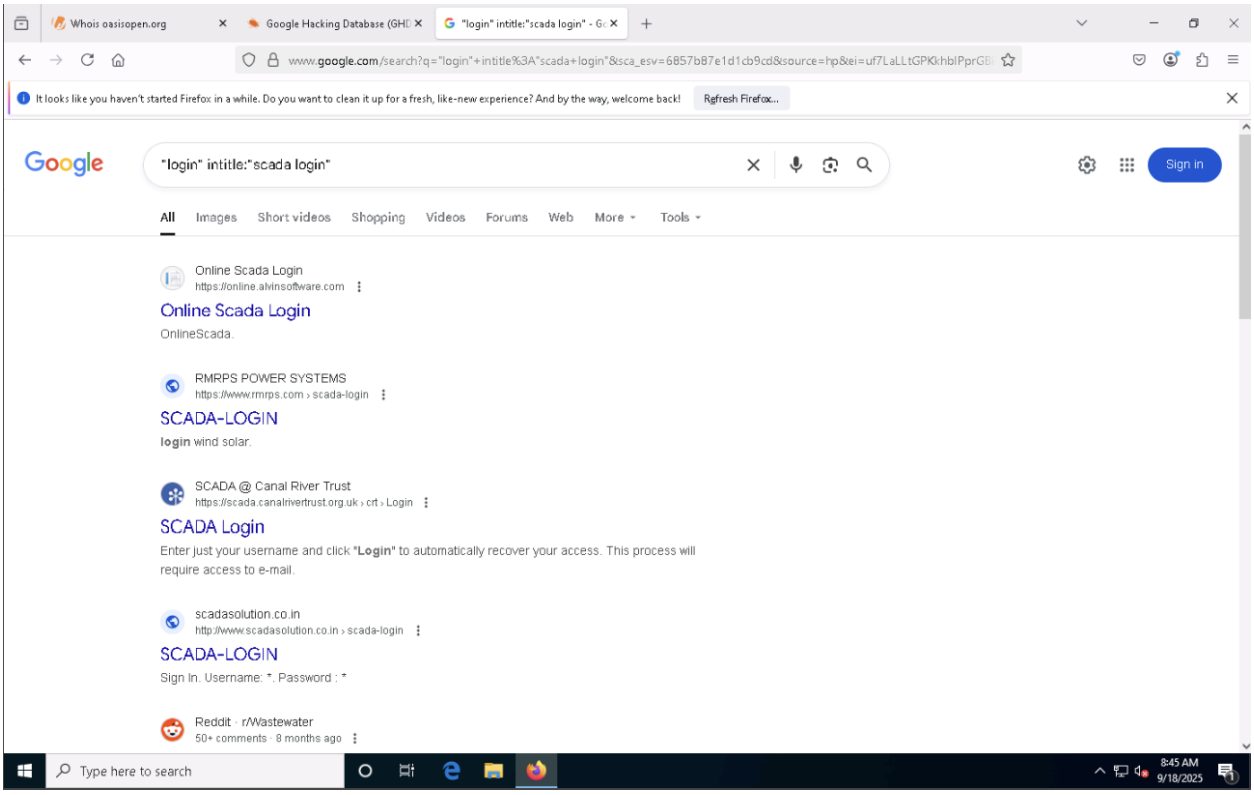
The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

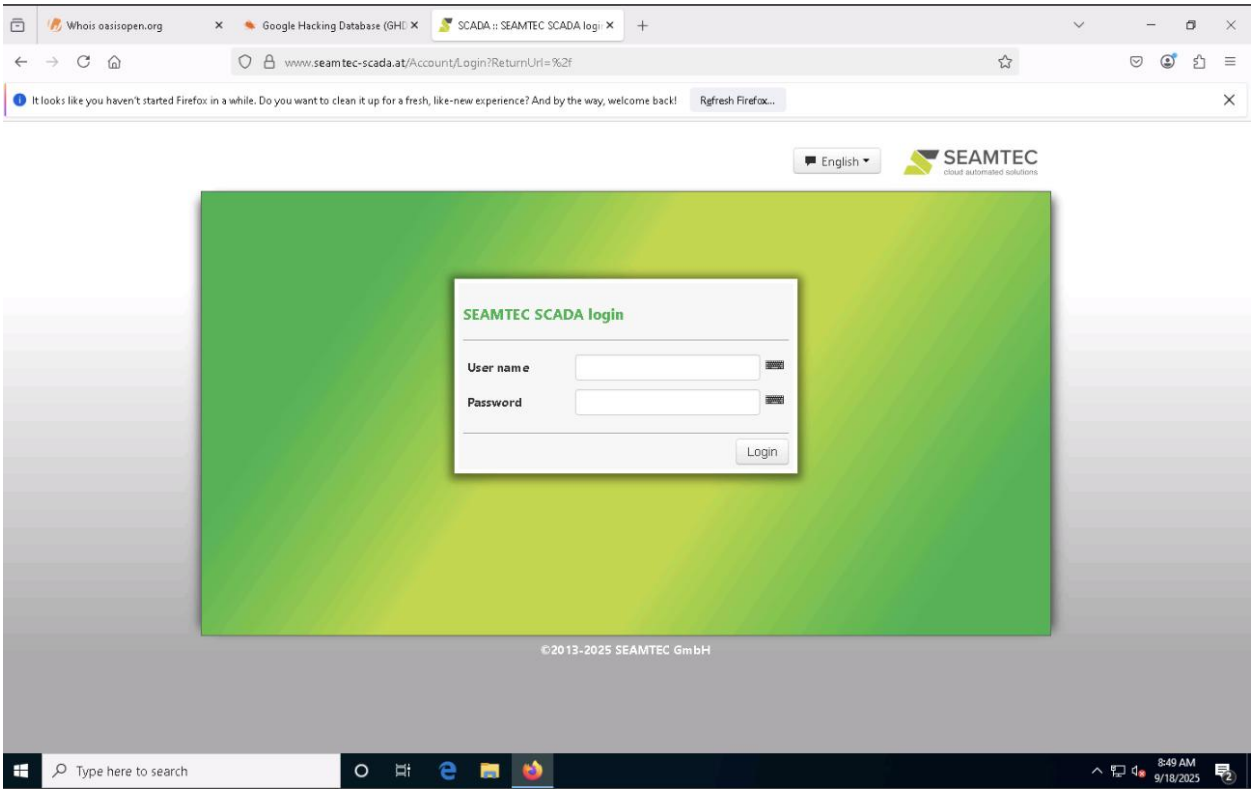

Free Whois Lookup - Whois IP
www.whois.com/whois/
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Enter Domain or IP
WHOIS
Whois Domain Lookup
Whois search for Domain and IP
www.oasis_open.org
SEARCH
Example: qq.com. google.co.in. bbc.co.uk. ebay.ca
Frequently Asked Questions
We serve cookies on this site to analyze traffic, remember your preferences, and optimize your experience. Learn more
Dismiss
Accept
Type here to search
8:41 AM
9/18/2025


Whois oasisopen.org
www.whois.com/whois/oasisopen.org
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
Whois
Domains
Hosting
Servers
Email
Security
Whois
Deals
Enter Domain or IP
WHOIS
oasisopen.org
Updated 5 days ago
Domain Information
Domain: oasisopen.org
Registered On: 2005-06-20
Expires On: 2026-06-20
Updated On: 2025-05-11
Status: client delete prohibited
client transfer prohibited
client update prohibited
Name Servers: dns1.stabletransit.com
dns2.stabletransit.com
Registrar Information
Registrar: DNC Holdings, Inc.
IANA ID: 291
Abuse Email: abuse@directnic.com
Interested in similar domains?
oasisopens.com Buy Now
oasisopenhouse.com Buy Now
littleoasisopen.com Buy Now
oasisopening.com Buy Now
oasisopens.net Buy Now
oasisopenhouse.net Buy Now
Sale
.space
$29.88 $1.18
BUY NOW
We serve cookies on this site to analyze traffic, remember your preferences, and optimize your experience. Learn more
Dismiss
Accept
Type here to search
8:42 AM
9/18/2025


Whois oasisopen.org
Google Hacking Database (GHD
www.exploit-db.com/google-hacking-database
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
EXPLOIT DATABASE
Google Hacking Database
Filters
Reset All
Show 15
Quick Search
Date Added
Dork
Category
Author
2024-08-23 site:github.com "BEGIN OPENSSH PRIVATE KEY" Files Containing Passwords kstrawn0
2024-08-23 ext:nix "BEGIN OPENSSH PRIVATE KEY" Files Containing Passwords kstrawn0
2024-07-26 inurl:home.htm intitle:1766 Various Online Devices Kishoreram
2024-07-04 intitle:"SSL Network Extender Login" -checkpoint.com Vulnerable Servers Everton Hydd3n
2024-07-04 intext:"siemens" & inurl:"/portal/portal.mwsl" Vulnerable Servers Kishoreram
2024-07-04 Google Dork Submisson For GlobalProtect Portal Vulnerable Servers Gurudatt Choudhary
2024-07-04 inurl:"cgi-bin/koha" Vulnerable Servers Hilary Soita
2024-07-04 intext:"aws_access_key_id" | intext:"aws_secret_access_key" filetype:json | filetype:yaml Files Containing Passwords Joel Indra
2024-07-04 intext:"proftpd.conf" "index of" Files Containing Juicy Info Fernando Mengali
2024-07-04 site:.edu filetype:xls "root" database Files Containing Juicy Info defaltredmode
2024-07-04 intitle:index of /etc/ssh Files Containing Passwords Shivam Dhingra
2024-05-13 "START test_database" ext:log Files Containing Usernames Nadir Boulacheb (RubX)
Type here to search
8:43 AM
9/18/2025


Whois oasisopen.org
Google Hacking Database (GHD
www.exploit-db.com/google-hacking-database
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
EXPLOIT DATABASE
Google Hacking Database
Filters
Reset All
Show 15
Quick Search
SCADA
Date Added
Dork
Category
Author
2023-04-06 inurl:"/scada-vis" Files Containing Juicy Info Parsa Rezaie Khiabanloo
2021-10-04 intitle:"index of SCADA" Sensitive Directories Romell Marin Cordoba
2021-09-20 intitle|inurl:"SCADA login" Pages Containing Login Portals Cyber Shelby
2021-09-16 intitle:"CirCarLife Scada" inurl:/html/index.html Various Online Devices Alexandros Pappas
2020-05-28 "login" intitle:""scada login" Pages Containing Login Portals Alexandros Pappas
2019-04-22 intitle:"index of" scada Sensitive Directories Aman Bhardwaj
2018-04-06 "login" intitle:"scada login" Pages Containing Login Portals Bruno Schmid
Showing 1 to 7 of 7 entries (filtered from 7,944 total entries)
FIRST PREVIOUS 1 NEXT LAST
Databases
Links
Sites
Solutions
Exploits
Search Exploit-DB
OffSec
Courses and Certifications
Type here to search
8:44 AM
9/18/2025




**Lab Summary: Shodan Search Engine – Task Not Completed**

This task was designed to demonstrate the use of the Shodan search engine to identify exposed devices and services on the Internet, including SCADA/ICS systems, using filters such as port:1883 for MQTT or port:502 for Modbus. The steps involved logging into Shodan, conducting targeted searches, and analyzing metadata for devices accessible over public IPs.

However, I chose not to complete this task due to the requirement to register for a Shodan account. Creating yet another third-party login solely for this lab was not feasible or necessary for my current learning objectives. As a result, I did not proceed with the login process or conduct the intended device enumeration tasks. All other windows were closed, and no data was collected from the Shodan interface.

This task remains incomplete by design, as part of a conscious decision to avoid additional account creation.

Lab 2: Capture and Analyze IoT Device Traffic

**Lab Scenario**

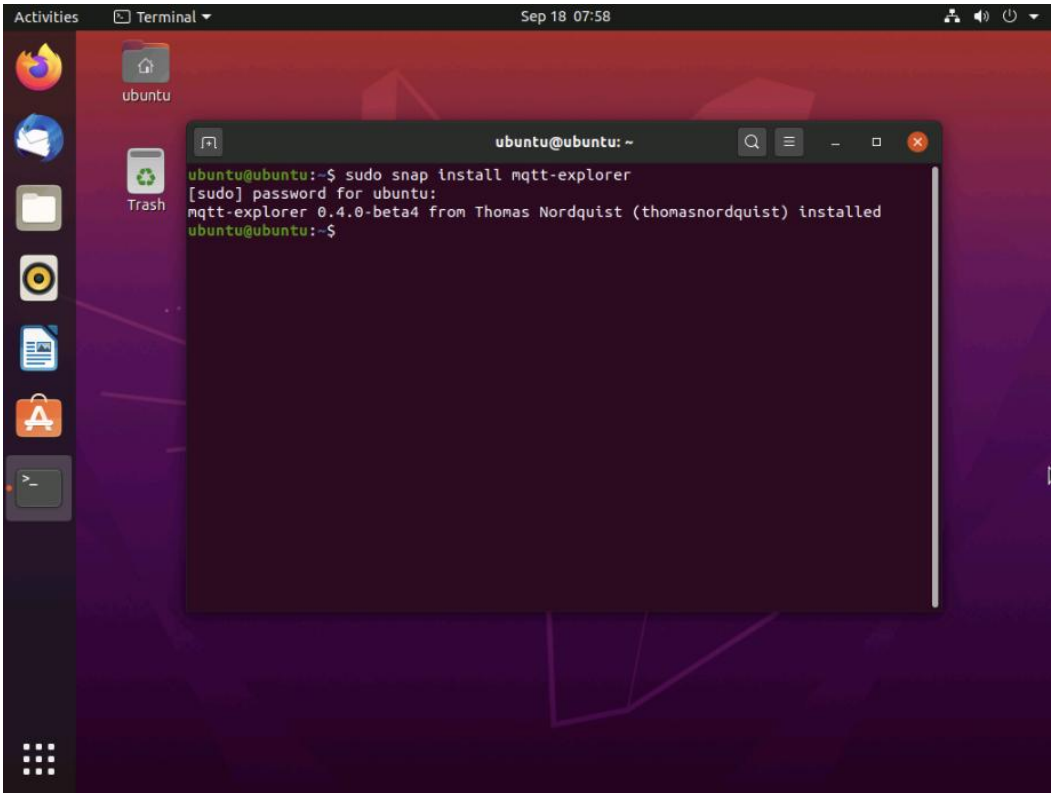
You must have sound knowledge to capture and analyze the traffic between IoT devices. Using various tools and techniques, you can capture the valuable data flowing between the IoT devices, analyze it to obtain information on the communication protocol used by the IoT devices, and acquire sensitive information such as credentials, device identification numbers, etc.

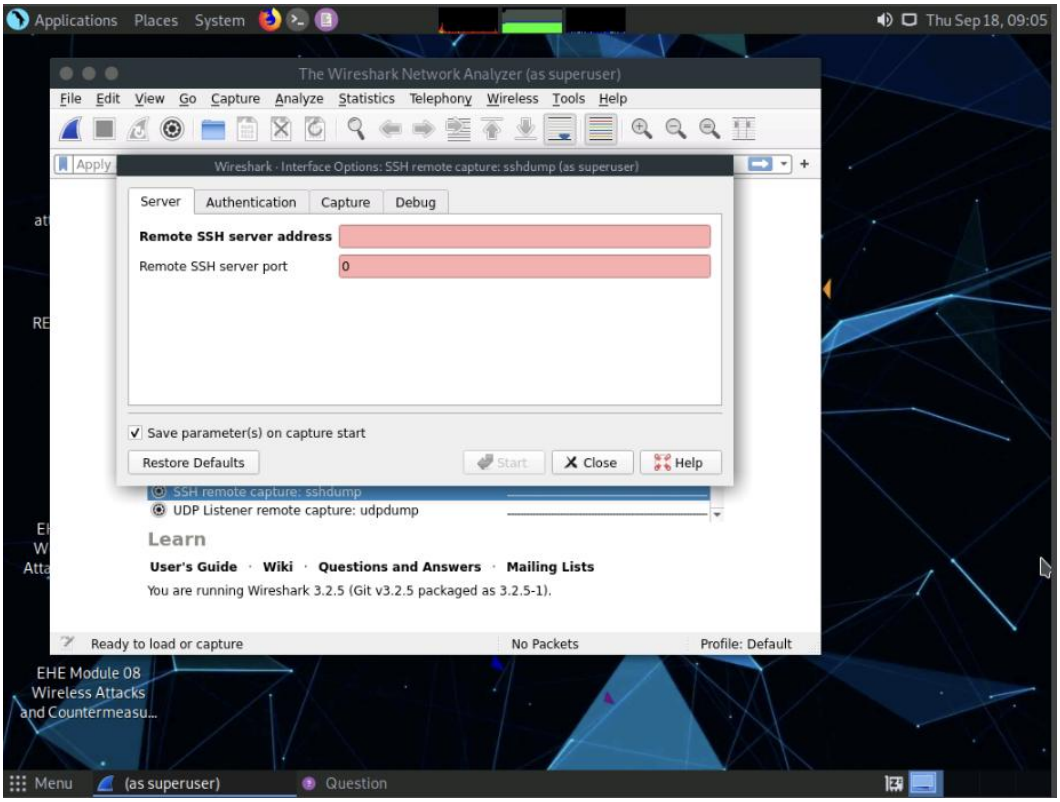
**Lab Objectives**

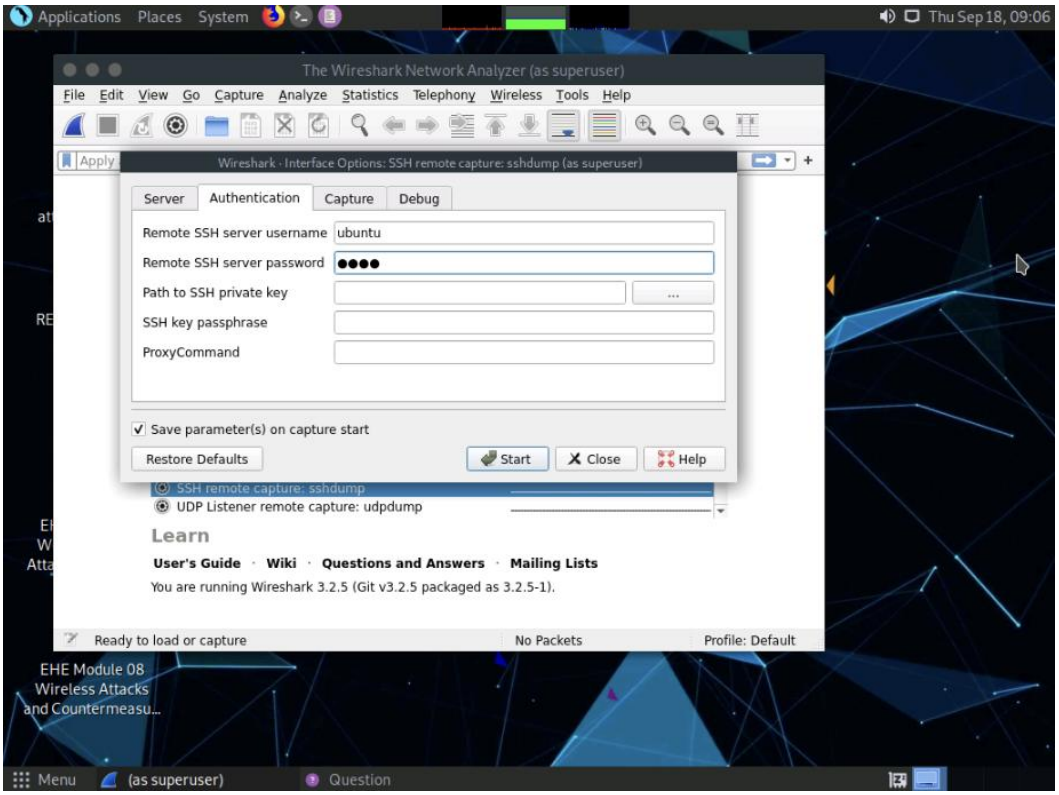
- Capture and Analyze IoT Traffic using Wireshark

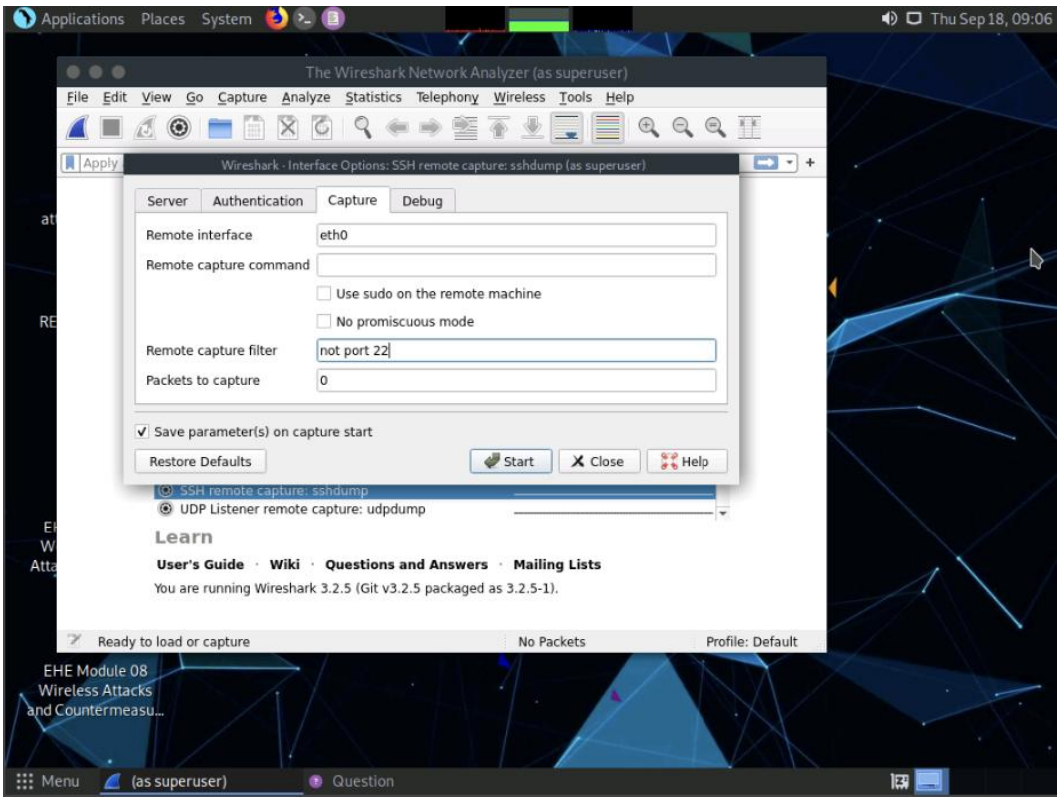
Task 1: Capture and Analyze IoT Traffic using Wireshark

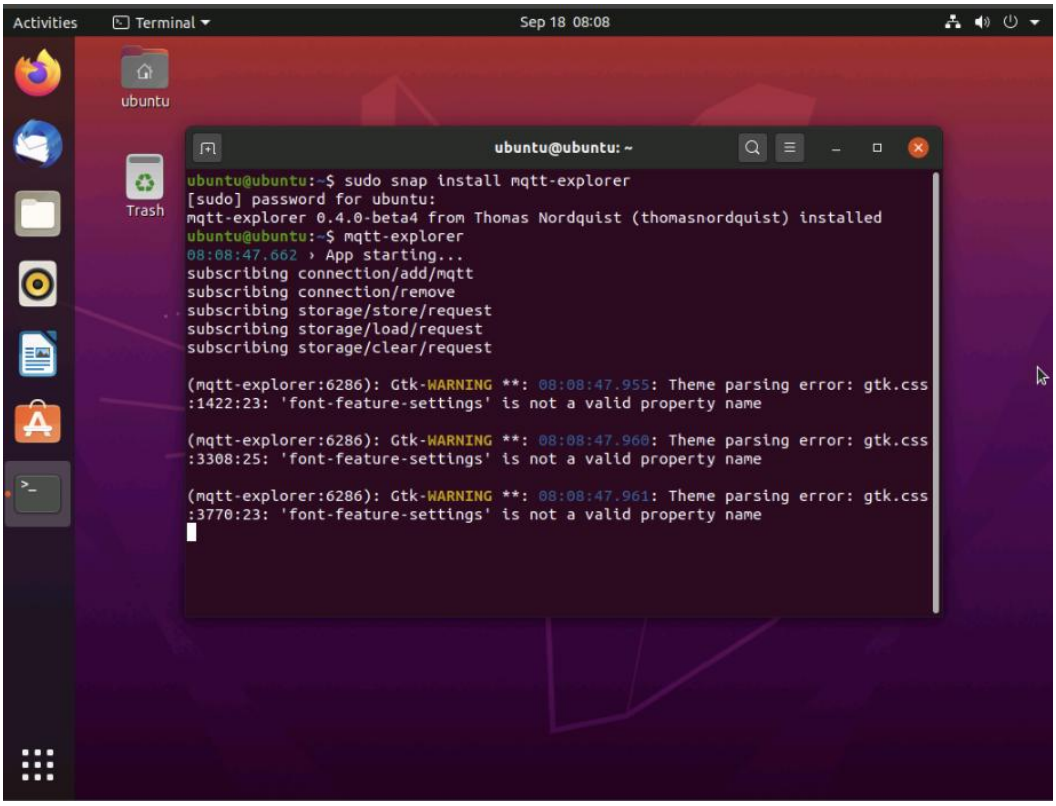
Wireshark is a free and open-source packet analyzer. It facilitates network troubleshooting, analysis, software and communications protocol development, and education. It is used to identify the target OS and sniff/capture the response generated from the target machine to the machine from which a request originates.

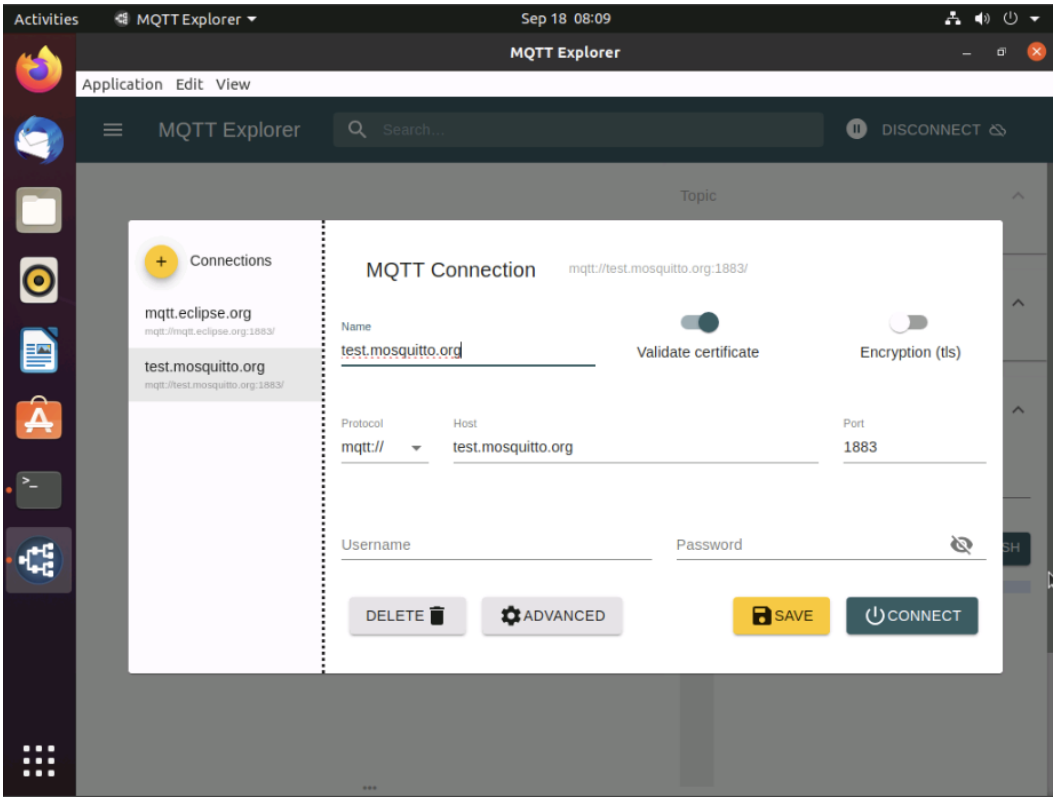

Activities
Terminal
Sep 18 07:58
ubuntu
Trash
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ sudo snap install mqtt-explorer
[sudo] password for ubuntu:
mqtt-explorer 0.4.0-beta4 from Thomas Nordquist (thomasnordquist) installed
ubuntu@ubuntu:~$

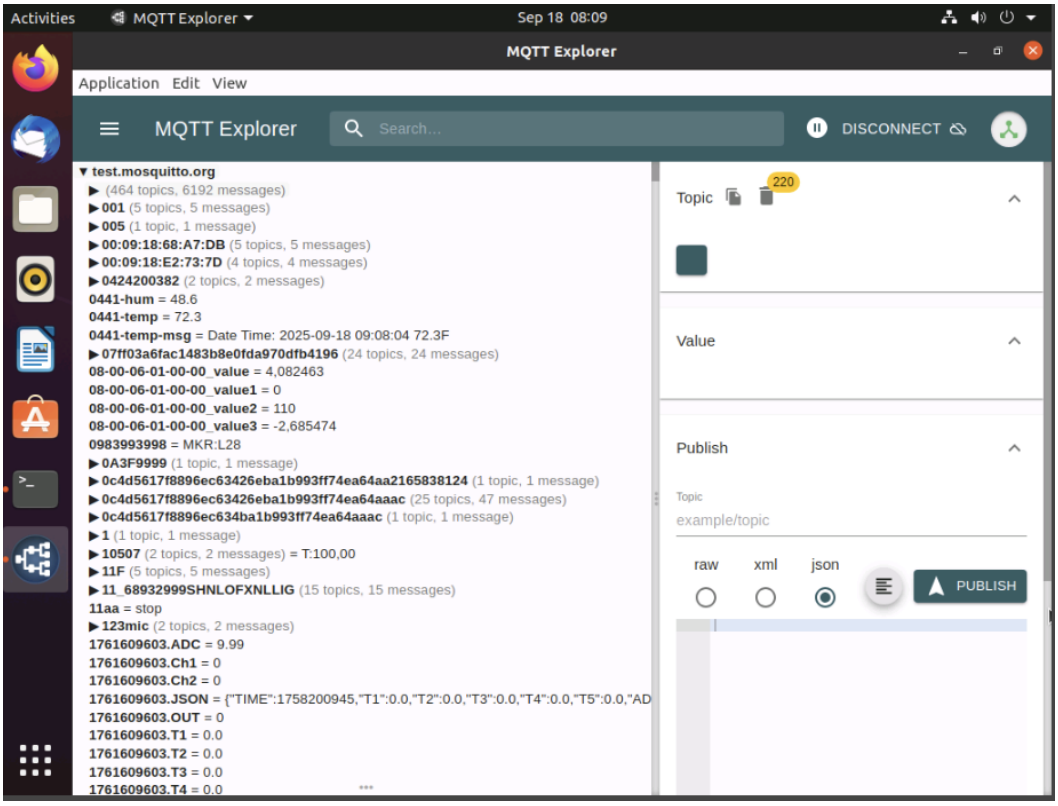

Applications
Places
System
Thu Sep 18, 09:05
The Wireshark Network Analyzer (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Interface Options: SSH remote capture: sshdump (as superuser)
Server
Authentication
Capture
Debug
Remote SSH server address
Remote SSH server port
0
Save parameter(s) on capture start
Restore Defaults
Start
Close
Help
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).
Ready to load or capture
No Packets
Profile: Default
EHE Module 08
Wireless Attacks
and Countermeasu...
Menu
(as superuser)
Question

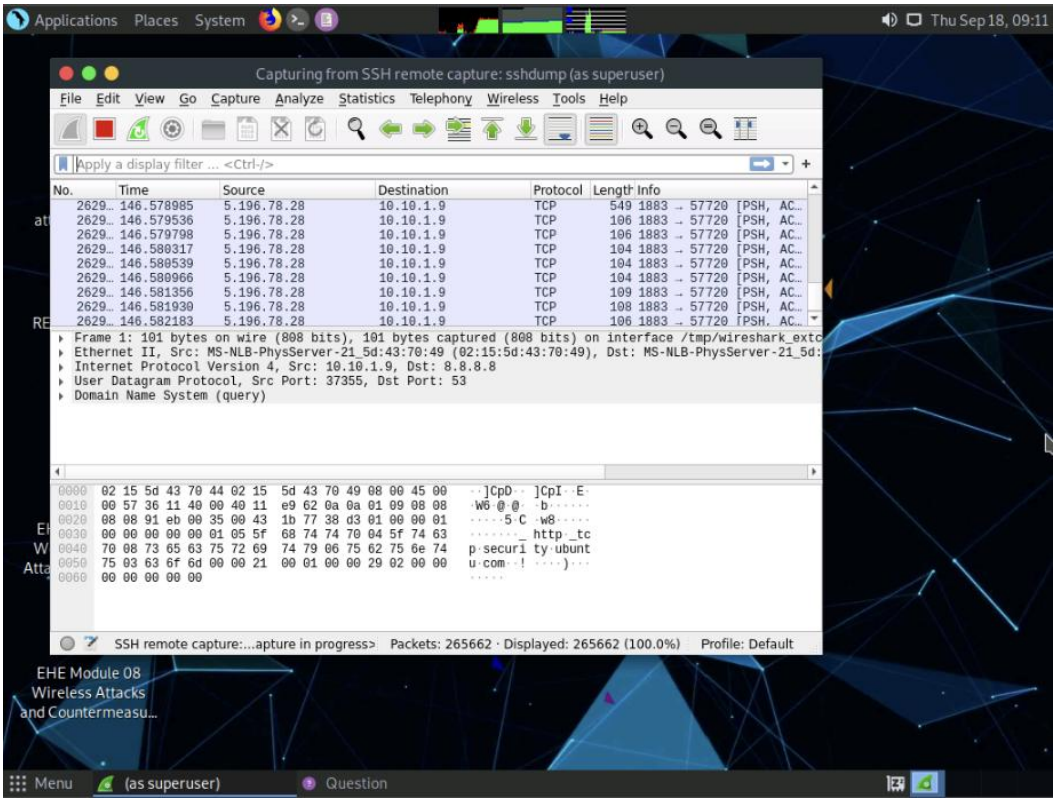

Applications Places System
Thu Sep 18, 09:06
The Wireshark Network Analyzer (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Interface Options: SSH remote capture: sshdump (as superuser)
Server Authentication Capture Debug
Remote SSH server username ubuntu
Remote SSH server password ●●●●
Path to SSH private key
SSH key passphrase
ProxyCommand
Save parameter(s) on capture start
Restore Defaults Start Close Help
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).
Ready to load or capture
No Packets
Profile: Default
EHE Module 08
Wireless Attacks
and Countermeasu...
Menu
(as superuser)
Question

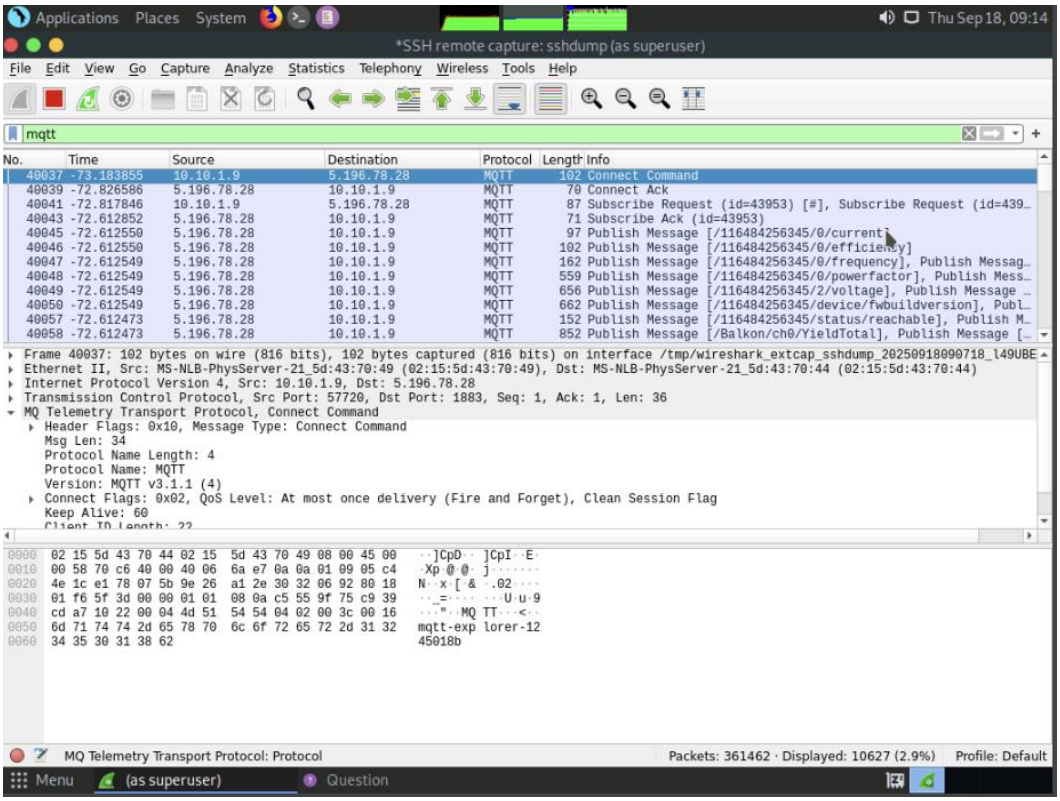

Applications Places System
Thu Sep 18, 09:06
The Wireshark Network Analyzer (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Interface Options: SSH remote capture: sshdump (as superuser)
Server Authentication Capture Debug
Remote interface eth0
Remote capture command
Use sudo on the remote machine
No promiscuous mode
Remote capture filter not port 22
Packets to capture 0
Save parameter(s) on capture start
Restore Defaults Start Close Help
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).
Ready to load or capture
No Packets
Profile: Default
EHE Module 08
Wireless Attacks
and Countermeasu...
Menu
(as superuser)
Question


Activities
Terminal
Sep 18 08:08
ubuntu
Trash
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ sudo snap install mqtt-explorer
[sudo] password for ubuntu:
mqtt-explorer 0.4.0-beta4 from Thomas Nordquist (thomasnordquist) installed
ubuntu@ubuntu:~$ mqtt-explorer
08:08:47.662 › App starting...
subscribing connection/add/mqtt
subscribing connection/remove
subscribing storage/store/request
subscribing storage/load/request
subscribing storage/clear/request
(mqtt-explorer:6286): Gtk-WARNING **: 08:08:47.955: Theme parsing error: gtk.css:1422:23: 'font-feature-settings' is not a valid property name
(mqtt-explorer:6286): Gtk-WARNING **: 08:08:47.960: Theme parsing error: gtk.css:3308:25: 'font-feature-settings' is not a valid property name
(mqtt-explorer:6286): Gtk-WARNING **: 08:08:47.961: Theme parsing error: gtk.css:3770:23: 'font-feature-settings' is not a valid property name


Activities
MQTT Explorer
Sep 18 08:09
MQTT Explorer
Application Edit View
MQTT Explorer
Search...
DISCONNECT
Topic
Connections
mqtt.eclipse.org
mqtt://mqtt.eclipse.org:1883/
test.mosquitto.org
mqtt://test.mosquitto.org:1883/
MQTT Connection
mqtt://test.mosquitto.org:1883/
Name
test.mosquitto.org
Validate certificate
Encryption (tls)
Protocol
mqtt://
Host
test.mosquitto.org
Port
1883
Username
Password
DELETE
ADVANCED
SAVE
CONNECT


Activities
MQTT Explorer
Sep 18 08:09
MQTT Explorer
Application Edit View
MQTT Explorer
Search...
DISCONNECT
test.mosquitto.org
(464 topics, 6192 messages)
001 (5 topics, 5 messages)
005 (1 topic, 1 message)
00:09:18:68:A7:DB (5 topics, 5 messages)
00:09:18:E2:73:7D (4 topics, 4 messages)
0424200382 (2 topics, 2 messages)
0441-hum = 48.6
0441-temp = 72.3
0441-temp-msg = Date Time: 2025-09-18 09:08:04 72.3F
07ff03a6fac1483b8e0fda970dfb4196 (24 topics, 24 messages)
08-00-06-01-00-00_value = 4,082463
08-00-06-01-00-00_value1 = 0
08-00-06-01-00-00_value2 = 110
08-00-06-01-00-00_value3 = -2,685474
0983993998 = MKR:L28
0A3F9999 (1 topic, 1 message)
0c4d5617f8896ec63426eba1b993ff74ea64aa2165838124 (1 topic, 1 message)
0c4d5617f8896ec63426eba1b993ff74ea64aaac (25 topics, 47 messages)
0c4d5617f8896ec634ba1b993ff74ea64aaac (1 topic, 1 message)
1 (1 topic, 1 message)
10507 (2 topics, 2 messages) = T:100,00
11F (5 topics, 5 messages)
11_68932999SHNLOFXNLLIG (15 topics, 15 messages)
11aa = stop
123mic (2 topics, 2 messages)
1761609603.ADC = 9.99
1761609603.Ch1 = 0
1761609603.Ch2 = 0
1761609603.JSON = {"TIME":1758200945,"T1":0.0,"T2":0.0,"T3":0.0,"T4":0.0,"T5":0.0,"AD
1761609603.OUT = 0
1761609603.T1 = 0.0
1761609603.T2 = 0.0
1761609603.T3 = 0.0
1761609603.T4 = 0.0
Topic
220
Value
Publish
Topic
example/topic
raw
xml
json
PUBLISH


Applications Places System
Thu Sep 18, 09:11
Capturing from SSH remote capture: sshdump (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface /tmp/wireshark_exto
Ethernet II, Src: MS-NLB-PhysServer-21_5d:43:70:49 (02:15:5d:43:70:49), Dst: MS-NLB-PhysServer-21_5d:
Internet Protocol Version 4, Src: 10.10.1.9, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 37355, Dst Port: 53
Domain Name System (query)
SSH remote capture:...apture in progress
Packets: 265662 · Displayed: 265662 (100.0%)
Profile: Default
EHE Module 08
Wireless Attacks
and Countermeasu...
Menu
(as superuser)
Question




**Module 10: IoT and OT Attacks and Countermeasures – Lab Summary**

This module introduced offensive security testing techniques against IoT (Internet of Things) and OT (Operational Technology) devices. These systems, increasingly embedded in homes, industries, and critical infrastructure, are often deployed with weak or default security configurations. The labs emphasized how attackers exploit insecure device interfaces, gather intelligence through passive and active reconnaissance, and intercept communications to extract sensitive information.

In Lab 1, I began the process of footprinting IoT and OT systems using open-source intelligence tools. The task focused on online methods such as advanced Google hacking, Whois lookups, and the Shodan search engine to extract metadata about exposed devices. While I reviewed the steps required to use Shodan to search for vulnerable endpoints (e.g., port:1883 for MQTT devices or SCADA identifiers like "Schneider Electric"), I did not complete the task. Creating a new Shodan account was not necessary for my objectives, and I opted out of registering for yet another third-party platform. No data was collected from Shodan during this task.

In Lab 2, I conducted IoT traffic analysis using Wireshark. This lab focused on capturing network traffic between connected devices to inspect packets for clues about

communication protocols (e.g., MQTT, Zigbee, BLE) and potentially exposed credentials or device IDs. Wireshark enabled inspection of packet headers, payloads, and flow characteristics, reinforcing how easily attackers can intercept sensitive data if encryption or segmentation is lacking. The exercise demonstrated the importance of defensive controls such as encrypted channels, proper device segmentation, and updated firmware in IoT/OT environments.

Together, these labs highlighted the real-world risks posed by insecure IoT deployments and the ease with which attackers can gather intelligence and conduct surveillance across poorly secured smart environments. The module also reinforced the critical role of reconnaissance and traffic analysis in any red team or penetration testing operation targeting embedded and connected devices.