

Lab 3 Passive Reconnaissance

Question 1:

Task 1:

Shodan search results for IP 92.68.247.49. The interface shows a map of Rotterdam and a sidebar with general information. The 'Open Ports' section is highlighted in yellow, displaying three ports: 80, 4443, and 8080. Below this, a 'Hikvision IP Camera' entry is visible with the text '<empty title>' and 'HTTP/1.1 200 OK'. The search bar contains '92.68.247.49' and the page is titled 'shodan.io/host/92.68.247.49'.

Task 2:

who.is WHOIS Domain Lookup page for kpn.net. The page title is 'WHOIS Domain Lookup' and the subtitle is 'Look up registration details, contacts, and nameservers for any domain name'. A search bar contains 'kpn.net' and the results show 'kpn.net' with 'WHOIS Information' and 'IP Address: 52.209.121.26' highlighted in yellow. Below the IP address are buttons for 'Whois', 'RDAP', 'DNS Records', 'Uptime', 'Diagnostics', and 'Hide Contact Info'. The page is titled 'who.is' and the search bar contains 'kpn.net'.

The IP addresses for the nameservers are exposed which can allow for attacks such as DNS spoofing or flooding of the nameservers. The registrar name being available can be a vulnerability because attackers can use the information for social engineering or finding vulnerabilities in the registrar's system. The expiration date of the domain being this year is a weakness because an attacker can prepare to take over the domain as soon as it expires.

Question 2:

Task 1:

The screenshot displays a Shodan search result for the IP address 154.41.194.149. The page is divided into several sections:

- Host Information:** City: Washington; Organization: Cogent Communications - IPENG; ISP: Cogent Communications; ASN: AS174.
- Port Grid:** A grid of 20 blue buttons representing open ports: 4848, 5007, 5560, 7001, 7434, 8009, 8080, 8090, 8140, 8575, 9095, 9943, 10250, 10554, 16010, 21379, 31337, 55442, 55554, 61616.
- Vulnerabilities:** Filtered by 'All ports' and 'Latest'. Two CVEs are listed:
 - CVE-2025-32728 (4.3):** In sshd in OpenSSH before 10.0, the DisableForwarding directive does not adhere to the documentation stating that it disables X11 and agent forwarding.
 - CVE-2025-26466 (6.9):** A flaw was found in the OpenSSH package. For each ping packet the SSH server receives, a pong packet is allocated in a memory buffer and stored in a queue of...
- Scan Results:**
 - Port 502 / TCP:** Shows three Modbus devices with their Slave ID Data and Device Identification. The Slave ID Data is highlighted in yellow.
 - Port 2222 / TCP:** Shows an OpenSSH 9.9 service with key type: ecdsa-sha2-nistp256 and key: AAAAE2VjZmhlbXNoYTIibmlzdhYNTYAAAIBmlzdhYNTYAAABBLPjXp2zeJ9CSUSgRvKdnpui.

154.41.194.149

SHODAN Explore Downloads Pricing Type / to search Account

154.41.194.149 Regular View Raw Data Timeline Whois

// TAGS: **ics** // LAST SEEN: 2026-02-16

General Information

Country: **United States**

City: **Washington**

Organization: **Cogent Communications - IPENG**

ISP: **Cogent Communications**

ASN: **AS174**

Open Ports

427	465	502	2067	2181	2222	3790	4242	4443	4444
4848	5007	5560	7001	7434	8009	8080	8090	8140	8575
9095	9943	10250	10554	16010	21379	31337	55442	55554	61616

// 502 / TCP -1757586623 | 2026-02-16T22:35:02.817560

154.41.194.149

SHODAN Explore Downloads Pricing Type / to search Account

154.41.194.149 Regular View Raw Data Timeline Whois

Vulnerabilities All ports Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2025 (3)

CVE-2025-32728 **4.3** In sshd in OpenSSH before 10.0, the DisableForwarding directive does not adhere to the documentation stating that it disables X11 and agent forwarding.

CVE-2025-26466 **5.9** A flaw was found in the OpenSSH package. For each ping packet the SSH server receives, a pong packet is allocated in a memory buffer and stored in a queue of packages. It is only freed when the server/client key exchange has finished. A malicious client may keep sending such packages, leading to an uncontrolled increase in memory consumption on the server side. Consequently, the server may become unavailable, resulting in a denial of service attack.

CVE-2025-26465 **6.8** A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how

OpenSSH 9.9

SSH-2.0-OpenSSH_9.9
 Key type: ecdsa-sha2-nistp256
 Key: AAAAE2VjZmhlLXNOY1R0bmlzDHAYNTAAAAIbmlzDHAYNTAAAAIBBLPJXp2e39cSU5gRvkdhpui
 B7Kc1FRAT/h7s1tFRSvq+fjnyIRDNnsD4xH7Z/KJuzwT03qnlVLRlUeHTp0k/sw
 Fingerprint: 35:f1:36:a6:8b:ee:13:13:78:bc:56:03:ea:9d:ee:4e

Kex Algorithms:
 sntrup761x25519-sha512
 sntrup761x25519-sha512@openssh.com
 m1kem768x25519-sha256
 curve25519-sha256
 curve25519-sha256@libssh.org
 ecdh-sha2-nistp256
 ecdh-sha2-nistp384
 ecdh-sha2-nistp521
 diffie-hellman-group-exchange-sha256
 diffie-hellman-group16-sha512

// 2222 / TCP -1570029415 | 2026-02-16T17:44:11.642446

Task 2:

The device is a PM710 Power Meter that uses Modbus protocol and is manufactured by Schneider Electric. The power meter is part of the SCADA system. The power meter cannot encrypt or authenticate which results in the device being vulnerable to data theft and manipulation. Due to the lack of authentication, attackers can also modify and reconfigure the device for their own purposes. The device is vulnerable to denial of service attacks. The device

is very simple and is unable to filter the packets entering. Attackers will be able to flood the device easily with packets causing it to stop functioning.

Task 3:

The attack described in CVE-2025-26466 is a denial of service attack.

The screenshot shows the MITRE ATT&CK website interface. The left sidebar lists various categories under 'TECHNIQUES', including Enterprise, Mobile, ICS, Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement, Collection, and Command and Control. The main content area is divided into two sections: 'Mitigations' and 'Detection Strategy'. The 'Mitigations' table has columns for ID, Mitigation, and Description. The 'Detection Strategy' table has columns for ID, Name, Analytic ID, and Analytic Description. Both tables have rows highlighted in yellow.

ID	Mitigation	Description
M0815	Watchdog Timers	System and process restarts should be performed when a timeout condition occurs.

ID	Name	Analytic ID	Analytic Description
DET0723	Detection of Denial of Service	AN1856	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g., extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g., monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Monitor network data for uncommon data flows. Processes utilizing the network that do not

M0815 Watchdog Timers is a mitigation technique that uses watchdog timer devices. A watchdog timer allows the device to detect if a system is unresponsive. When watchdog timers are used, the organization can respond quickly to the attack. DET0723 Detection of Denial of Service involves monitoring the flow of traffic and the inspection of packets. Other aspects to monitor are application logging, network data, and operational data. The detection strategy monitors the device or system for any abnormalities which can indicate a denial of service attack is occurring.