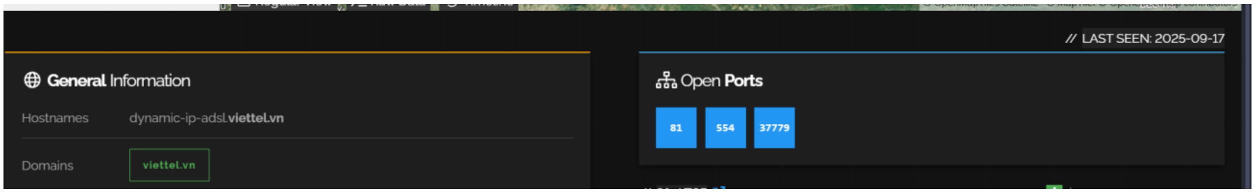
Question 1

1a: Find a device where there is at least one open port and the domain name (URL)
is displayed. If you find multiple such devices, just choose one arbitrarily. Take a screenshot highlighting the domain name and the open ports. Attach the screenshot in
your submission



// LAST SEEN: 2025-09-17

General Information

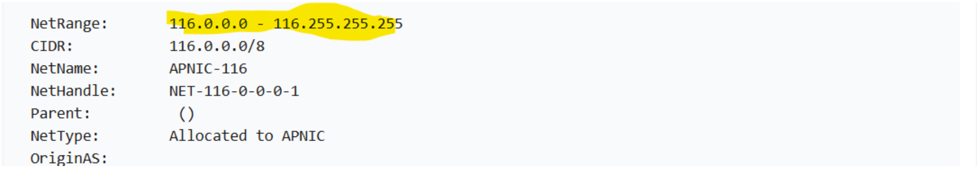
Hostnames dynamic-ip-adsl.viettel.vn

Domains viettel.vn

Open Ports

81 554 37779

1b: Using WHOIS (https://who.is/) or Netcraft (https://sitereport.netcraft.com/), find
the IP address of the domain name you found in Task 1. Take a screenshot highlighting
the IP address and attach it in your submission. Go through the complete report you
retrieved from WHOIS or Netcraft. Do some research online about the vulnerabilities or
weakness the device has. Briefly describe all the security weakness or vulnerabilities you
found.

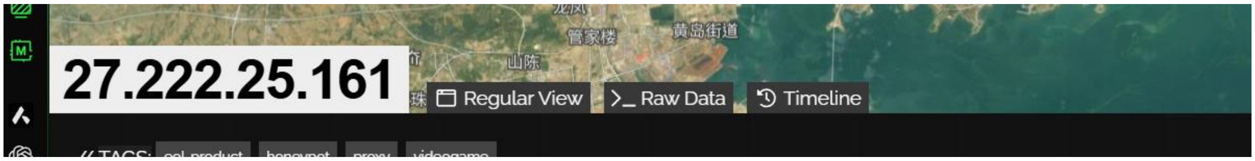


```
NetRange:       116.0.0.0 - 116.255.255.255
CIDR:           116.0.0.0/8
NetName:        APNIC-116
NetHandle:      NET-116-0-0-0-1
Parent:          ()
NetType:        Allocated to APNIC
OriginAS:
```

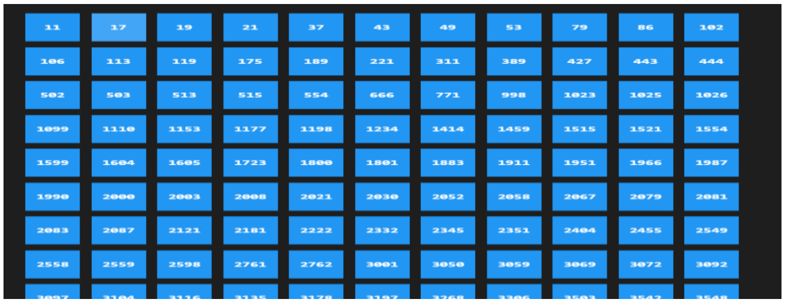
Weakness and vulnerabilities with this device stem from it having it be addressed from an ADSL address. Which means it has endpoints that in many cases expose secured web services. In doing this the vulnerabilities of the device include the use of default passwords, lack of encryption, outdated firmware/software, and exposure to well-known exploits.

Question 2

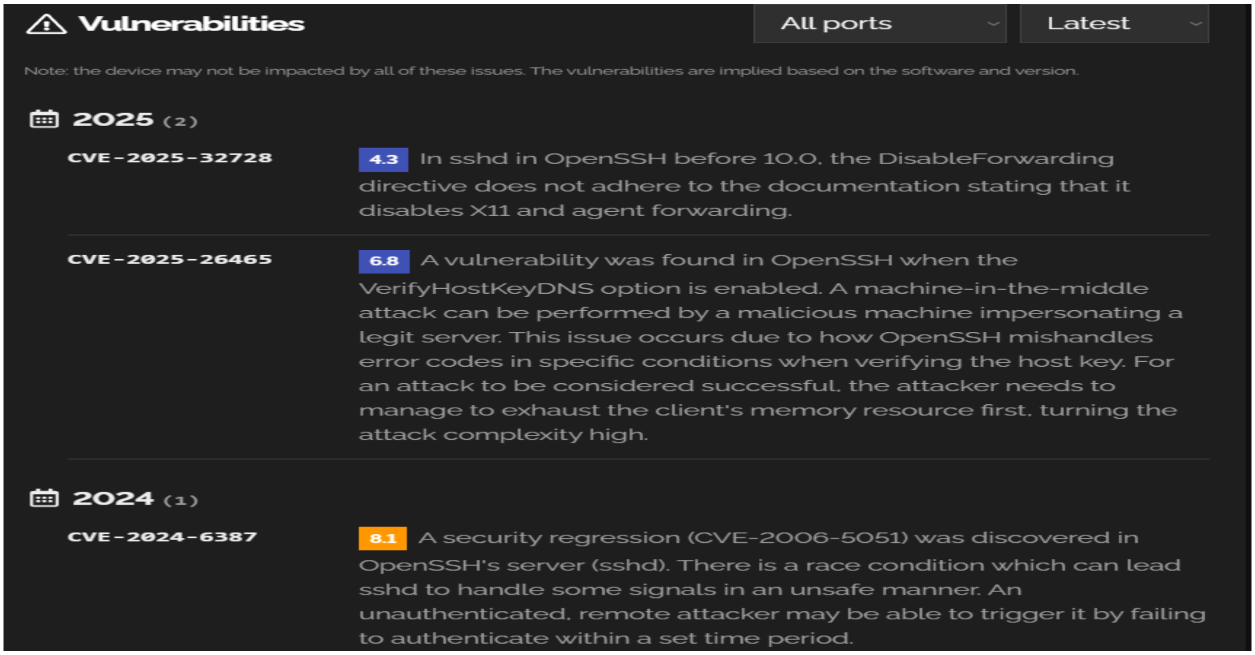
2a



27.222.25.161



11	17	19	21	37	43	49	53	79	86	102
106	113	119	175	189	221	311	389	427	443	444
502	503	513	515	554	666	771	998	1023	1025	1026
1099	1110	1153	1177	1198	1234	1414	1459	1515	1521	1554
1599	1604	1605	1723	1800	1801	1883	1911	1951	1966	1987
1990	2000	2003	2008	2021	2030	2052	2058	2067	2079	2081
2083	2087	2121	2181	2222	2332	2345	2351	2404	2455	2549
2558	2559	2598	2761	2762	3001	3050	3059	3069	3072	3092



⚠ Vulnerabilities

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

2025 (2)

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-2025-26465 — 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 mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

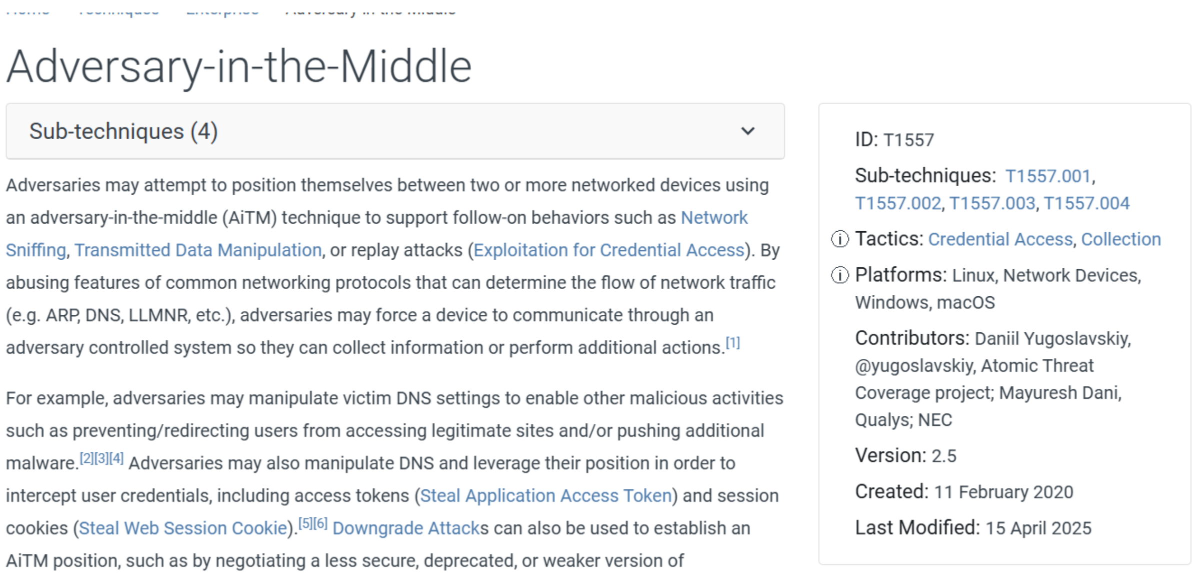
2024 (1)

CVE-2024-6387 — 8.1 A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

2b the device using the IP address **27.222.25.161** is most likely a **residential router or personal computer** connected through China Unicom's network in Qingdao, Shandong Province. Given that it is part of a dynamic IP range, it is typically assigned to individual users rather than enterprises, which makes it more susceptible to opportunistic attacks. Common vulnerabilities for such devices include **exposed open ports**, weak or default passwords on routers, outdated firmware, and susceptibility to malware or botnet infections. Additionally, if the device hosts any services, it could be vulnerable to **port scanning, DDoS amplification, and spoofing attacks**. Users on such dynamic IPs are often unaware of these weaknesses, leaving personal data, devices, and network security at risk.

2c The attack performed was the machine-in-the-middle attack

The vulnerability described is due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. An attacker could create a fake machine that would impersonate a legit server.



Adversary-in-the-Middle

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.[1]

For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.[2][3][4] Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials, including access tokens (Steal Application Access Token) and session cookies (Steal Web Session Cookie).[5][6] Downgrade Attacks can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of

ID: T1557

Sub-techniques: T1557.001, T1557.002, T1557.003, T1557.004

ⓘ Tactics: Credential Access, Collection

ⓘ Platforms: Linux, Network Devices, Windows, macOS

Contributors: Daniil Yugoslavskiy, @yugoslavskiy, Atomic Threat Coverage project; Mayuresh Dani, Qualys; NEC

Version: 2.5

Created: 11 February 2020

Last Modified: 15 April 2025