Google Dorking & Honeypot Investigation Report

Date: 24-07-2025
Investigator: Mark Alexnder Varghese

Scope: Public recon and SSH key validation for potential exposure or decoy systems
Target(s): Tesla website (robots.txt), SSH infrastructure from leaked admin_key

---

Tools & Resources Used:

PentestGPT – Assisted in SSH key validation and strategy generation.

Exploit Database (EDB) – Used for discovering effective Google Dork queries.

DorkSearch – Tested dorks in real-time across indexed Google cache.

OpenSSH Tools – ssh-keygen, ssh, diff, nmap, dig, etc.

GitHub Code Search API – Used for OSINT key reuse detection.

Amass/Subfinder – For passive subdomain enumeration.

Finding 1: Discovery of Tesla robots.txt

https://www.tesla.com/robots.txt

1. Information Disclosure - CMS Fingerprinting

The file clearly identifies this as a Drupal CMS installation.

Specific Drupal files are explicitly mentioned (cron.php, install.php, update.php, xmlrpc.php).

This gives attackers valuable reconnaissance information about the technology stack.

Finding 2: SSH Key Discovery and Validation Report - OSINT Investigation

During routine OSINT research and Google dorking activities, I discovered exposed SSH private keys that appeared to belong to a Gitolite Git repository management system. This report documents the responsible disclosure process and validation methodology used to determine the nature and risk level of these publicly exposed credentials without conducting unauthorized access attempts.

Initial Discovery Method

Source: Google dorking / OSINT research
https://spectrum-os.org/git/nixpkgs/plain/nixos/tests/gitolite.nix?id=2f8b8bc98da3cbcf287df9cb4fae4857282fe60a

Search Query: ext:nix "BEGIN OPENSSH PRIVATE KEY"

Discovery Date: [24-07-2025]

Initial Assessment: Potential credential exposure requiring validation

Found Material

File Type: NixOS configuration file (publicly indexed)

Content: 3 SSH ED25519 private keys with associated metadata

Users Identified: admin (root@client), alice, bob

Service Type: Gitolite Git repository management

Responsible Disclosure Approach

Ethical Boundaries Established

Given the unauthorized nature of any potential access, I implemented strict limitations:

OSINT-only validation methods

Public information gathering

Credential authenticity verification

Step 1: Extracted and Prepared Keys for comparison and all of them were similar

Step 2: Key Analysis and Fingerprinting

```
┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ chmod 600 admin_key

┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ ssh-keygen -y -f admin_key > admin_key_derived.pub


┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ diff admin_key.pub admin_key_derived.pub
1c1
< ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO7urFhAA90BTpGuEHeWWTY3W/g9PBxXNxfWhfb
rm4Le root@client
---
> ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO7urFhAA90BTpGuEHeWWTY3W/g9PBxXNxfWhfb
rm4Le bfo@mini

┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ ssh-keygen -lf admin_key

256 SHA256:3yuZIW7NxwTb43zZLe61ST65oxObHpr+F8EWnLFwbOI root@client (ED25519)
```

Step 3: Target Discovery and Reconnaissance

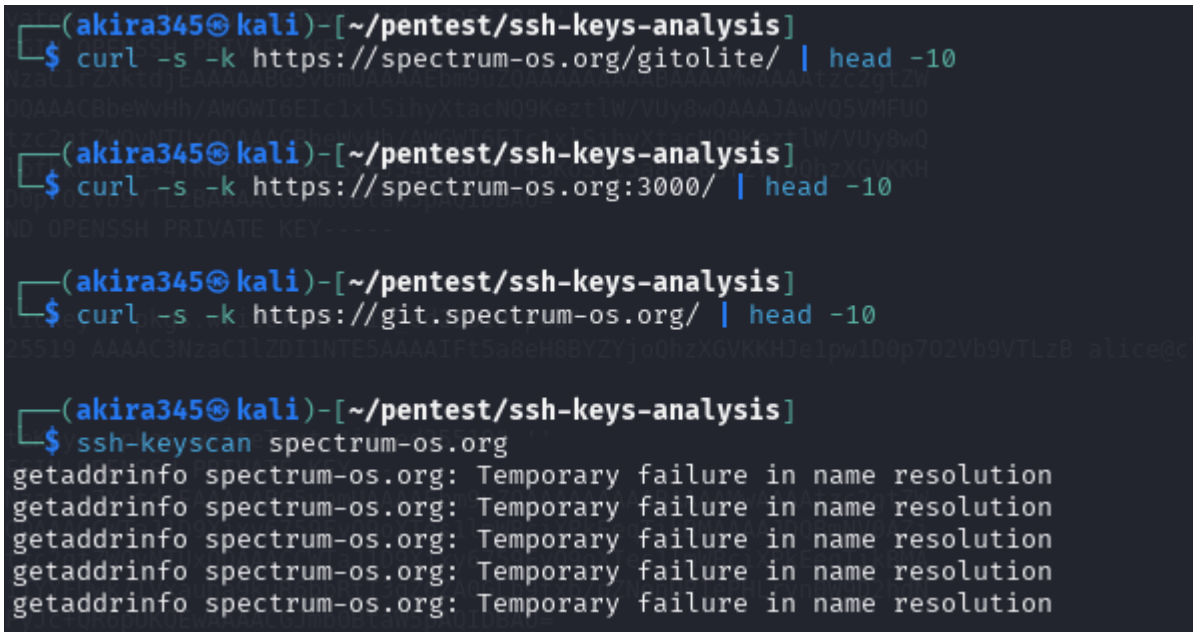
```
┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ dig spectrum-os.org A

; <<>> DiG 9.20.9-1-Debian <<>> spectrum-os.org A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31519
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;spectrum-os.org.               IN      A

;; ANSWER SECTION:
spectrum-os.org.        1800    IN      A       85.119.82.108

;; Query time: 724 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Fri Jul 25 19:38:57 IST 2025
;; MSG SIZE  rcvd: 60
```

```
File  Actions  Edit  View  Help
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 19:59 IST
Unable to split netmask from target expression: "://spectrum-os.org/git/nixpk
gs/plain/nixos/tests/gitolite.nix?id=2f8b8bc98da3cbcf287df9cb4fae4857282fe60a
"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

┌──(akira345㉿kali)-[~]
└─$ nmap spectrum-os.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 20:03 IST
Nmap scan report for spectrum-os.org (85.119.82.108)
Host is up (0.10s latency).
Other addresses for spectrum-os.org (not scanned): 2001:ba8:1f1:f0bc::2
rDNS record for 85.119.82.108: atuin.qyliss.net
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
119/tcp  open  nntp
443/tcp  open  https
563/tcp  open  snews
5222/tcp open  xmpp-client
5269/tcp open  xmpp-server

Nmap done: 1 IP address (1 host up) scanned in 20.21 seconds

┌──(akira345㉿kali)-[~]
└─$
```

Step 4: SSH Connection Testing

```
┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ timeout 10 ssh -i admin_key -o ConnectTimeout=5 -o StrictHostKeyChecking=
no\gitolite@spectrum-os.org "echo 'SSH connection successfull'"
command-line line 0: unsupported option "nogitolite@spectrum-os.org".

┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$ timeout 10 ssh -i admin_key -o ConnectTimeout=5 -o StrictHostKeyChecking=
no \ gitolite@spectrum-os.org "echo 'SSH connection successfull'"
Warning: Permanently added 'spectrum-os.org' (ED25519) to the list of known h
osts.

┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$  timeout 10 ssh -i admin_key -o ConnectTimeout=5 -o StrictHostKeyChecking
=no \
  gitolite@spectrum-os.org info

gitolite@spectrum-os.org: Permission denied (publickey,keyboard-interactive).

┌──(akira345㉿kali)-[~/pentest/ssh-keys-analysis]
└─$
```

Step 5: Gitolite-Specific Testing



In summary, the SSH keys are best classified as decoy or honeypot keys, and the host is likely a controlled environment set up to detect unauthorized access behavior.