Detecting Responder-like Attacks

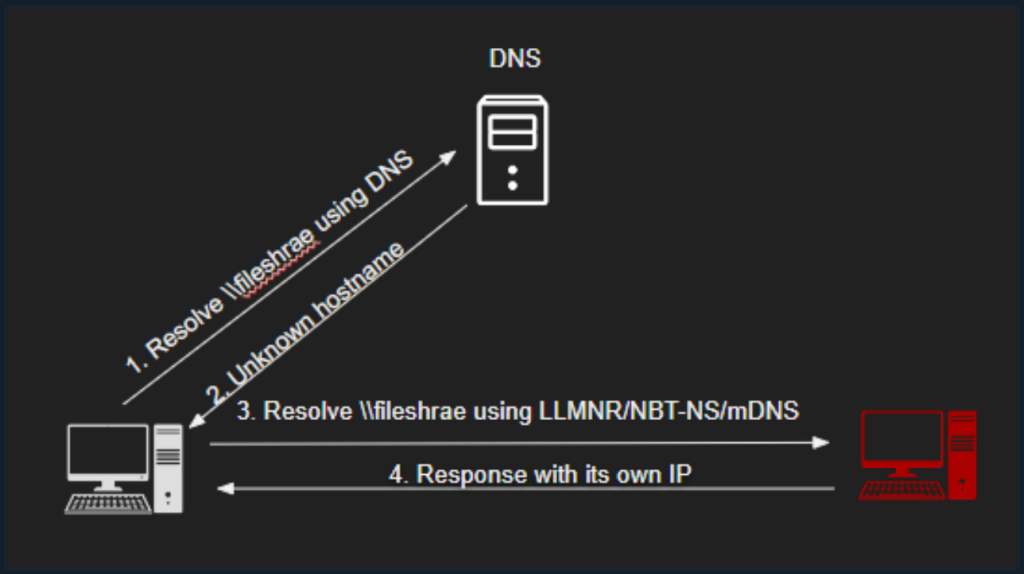
LLMNR/NBT-NS/mDNS Poisoning

`LLMNR (Link-Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) poisoning`, also referred to as NBNS spoofing, are network-level attacks that exploit inefficiencies in these name resolution protocols. Both `LLMNR` and `NBT-NS` are used to resolve hostnames to IP addresses on local networks when the fully qualified domain name (FQDN) resolution fails. However, their lack of built-in security mechanisms renders them susceptible to spoofing and poisoning attacks.

Typically, attackers employ the Responder tool to execute LLMNR, NBT-NS, or mDNS poisoning.

Attack Steps:

- A victim device sends a name resolution query for a mistyped hostname (e.g., `fileshrae`).
- DNS fails to resolve the mistyped hostname.
- The victim device sends a name resolution query for the mistyped hostname using LLMNR/NBT-NS.
- The attacker's host responds to the LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic, pretending to know the identity of the requested host. This effectively poisons the service, directing the victim to communicate with the adversary-controlled system.



The result of a successful attack is the acquisition of the victim's NetNTLM hash, which can be either cracked or relayed in an attempt to gain access to systems where these credentials are valid.

Responder Detection Opportunities

Detecting LLMNR, NBT-NS, and mDNS poisoning can be challenging. However, organizations can mitigate the risk by implementing the following measures:

- Deploy network monitoring solutions to detect unusual LLMNR and NBT-NS traffic patterns, such as an elevated volume of name resolution requests from a single source.
- Employ a honeypot approach - name resolution for non-existent hosts should fail. If an attacker is present and spoofing LLMNR/NBT-NS/mDNS responses, name resolution will succeed. https://www.praetorian.com/blog/a-simple-and-effective-way-to-detect-broadcast-

name-resolution-poisoning-bnrp/

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> $logfile = 'C:\tmp\poisoning.csv'
PS C:\Users\Administrator> $requestHosts = @('CORP-TX-FILE-01','COPY-NY-DC-02') #False hostnames to requ
est
PS C:\Users\Administrator> $interval = 30 #The minimum number of seconds to wait between requests
PS C:\Users\Administrator> $jitter = 30 #The maximum value for a random number of seconds to add to the
interval
PS C:\Users\Administrator> while($true){
>>      Start-Sleep ($interval + (Get-Random ($jitter + 1)))
>>      try {
>>          $ErrorActionPreference = 'stop'
>>          $request = Get-Random $requestHosts
>>          $ipAddr = (Resolve-DnsName -LlmnrNetbiosOnly -Name $request).IPAddress.tostring()
>>          $ErrorActionPreference = "continue"
>>          $event = [pscustomobject]@{
>>              date = Get-Date -format o
>>              host = $env:COMPUTERNAME
>>              request = $request
>>              attacker_ip = $ipAddr
>>              message = "LLMNR/NBT-NS spoofing by $ipAddr detected with $request request"
>>          }
>>          Write-Output $event.message
>>          $event | Export-Csv -Path $logfile -Append -NoTypeInformation
>>      } catch [System.Management.Automation.RuntimeException],
>> [System.ComponentModel.Win32Exception] {
>>      #Suppress output of timeout errors
>>      } finally {
>>          $ErrorActionPreference = "continue"
>>      }
>> }
LLMNR/NBT-NS spoofing by 10.0.10.5 detected with COPY-NY-DC-02 request
```

A PowerShell script similar to the above can be automated to run as a scheduled task to aid in detection. Logging this activity might pose a challenge, but the `New-EventLog` PowerShell cmdlet can be used.

Detecting Responder-like Attacks

```
PS C:\Users\Administrator> New-EventLog -LogName Application -Source LLMNRDetection
```

To create an event, the `Write-EventLog` cmdlet should be used:

Detecting Responder-like Attacks

```
PS C:\Users\Administrator> Write-EventLog -LogName Application -Source LLMNRDetection -EventId 1900
```

Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at http://[Target IP]:8000 and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

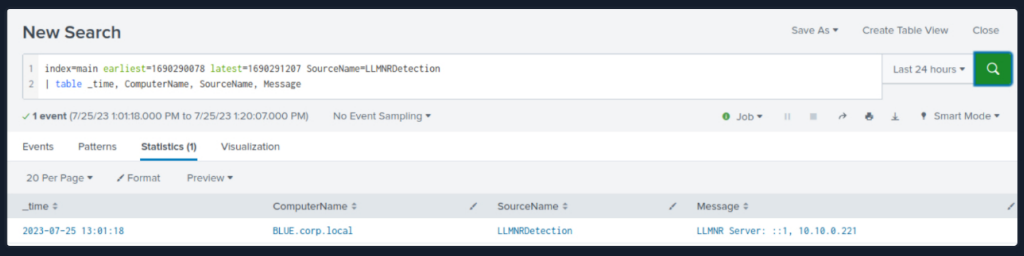
Detecting Responder-like Attacks With Splunk

Now let's explore how we can identify the Responder-like attacks previously discussed, using Splunk and logs from a PowerShell script similar to the one above.

Timeframe: `earliest=1690290078 latest=1690291207`

Detecting Responder-like Attacks

```
index=main earliest=1690290078 latest=1690291207 SourceName=LLMNRDetection
| table _time, ComputerName, SourceName, Message
```

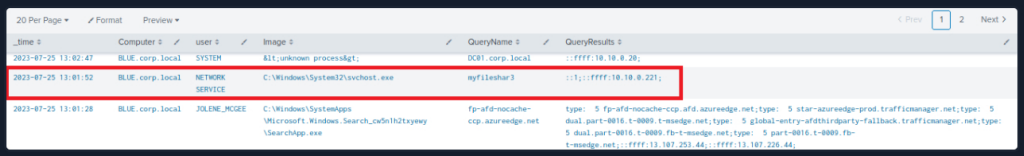


Sysmon Event ID 22 can also be utilized to track DNS queries associated with non-existent/mistyped file shares.

Timeframe: `earliest=1690290078 latest=1690291207`

Detecting Responder-like Attacks

```
index=main earliest=1690290078 latest=1690291207 EventCode=22
| table _time, Computer, user, Image, QueryName, QueryResults
```



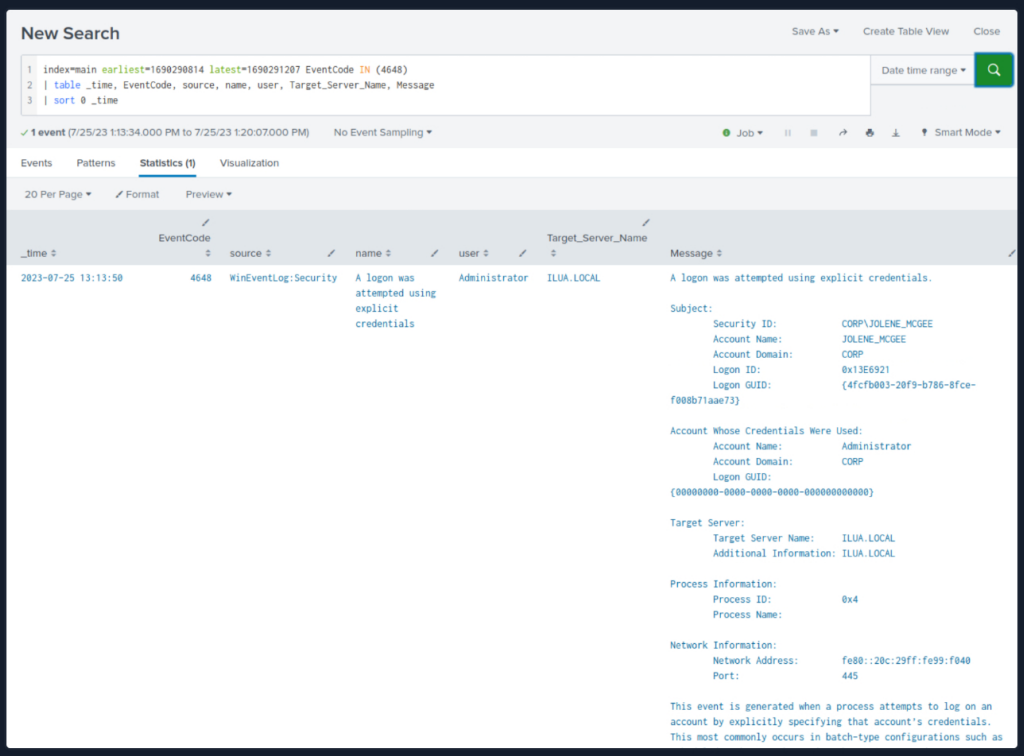
_time	Computer	user	Image	QueryName	QueryResults
2023-07-25 13:02:47	BLUE.corp.local	SYSTEM	<unknown process>	DC01.corp.local	::ffff:10.10.0.20;
2023-07-25 13:01:52	BLUE.corp.local	NETWORK SERVICE	C:\Windows\System32\svchost.exe	myfileshar3	::1;::ffff:10.10.0.221;
2023-07-25 13:01:28	BLUE.corp.local	JOLENE_MCGEE	C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe	fp-afd-nocache-ccp.azureedge.net	type: 5 fp-afd-nocache-ccp.afd.azureedge.net;type: 5 star-azureedge-prod.trafficmanager.net;type: 5 dual.part-0016.t-0009.t-msedge.net;type: 5 global-entry-afdthirdparty-fallback.trafficmanager.net;type: 5 dual.part-0016.t-0009.fb-t-msedge.net;type: 5 part-0016.t-0009.fb-t-msedge.net;::ffff:13.107.253.44;::ffff:13.107.226.44;

Additionally, remember that Event 4648 can be used to detect explicit logons to rogue file shares which attackers might use to gather legitimate user credentials.

Timeframe: `earliest=1690290814 latest=1690291207`

Detecting Responder-like Attacks

```
index=main earliest=1690290814 latest=1690291207 EventCode IN (4648)
| table _time, EventCode, source, name, user, Target_Server_Name, Message
| sort 0 _time
```



New Search

Save As · Create Table View · Close

```
1 index=main earliest=1690290814 latest=1690291207 EventCode IN (4648)
2 | table _time, EventCode, source, name, user, Target_Server_Name, Message
3 | sort 0 _time
```

Date time range

✓ 1 event (7/25/23 1:13:34.000 PM to 7/25/23 1:20:07.000 PM) · No Event Sampling · Job · Smart Mode

Events · Patterns · Statistics (1) · Visualization

20 Per Page · Format · Preview

_time	EventCode	source	name	user	Target_Server_Name	Message
2023-07-25 13:13:50	4648	WinEventLog:Security	A logon was attempted using explicit credentials	Administrator	ILUA.LOCAL	A logon was attempted using explicit credentials. Subject: Security ID: CORP\JOLENE_MCGEE Account Name: JOLENE_MCGEE Account Domain: CORP Logon ID: 0x13E6921 Logon GUID: {4fcfb003-20f9-b786-8fce-f008b71aae73} Account Whose Credentials Were Used: Account Name: Administrator Account Domain: CORP Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: ILUA.LOCAL Additional Information: ILUA.LOCAL Process Information: Process ID: 0x4 Process Name: Network Information: Network Address: fe80::20c:29ff:fe99:f040 Port: 445 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

◉ UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 140ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

+ 1 Modify and employ the provided Sysmon Event 22-based Splunk search on all ingested data (All time) to identify all share names whose location was spoofed by 10.10.0.221. Enter the missing share name from the following list as your answer. myshare, myfileshar3, _

f1nancefileshare

Submit

Previous Next

Mark Complete & Next