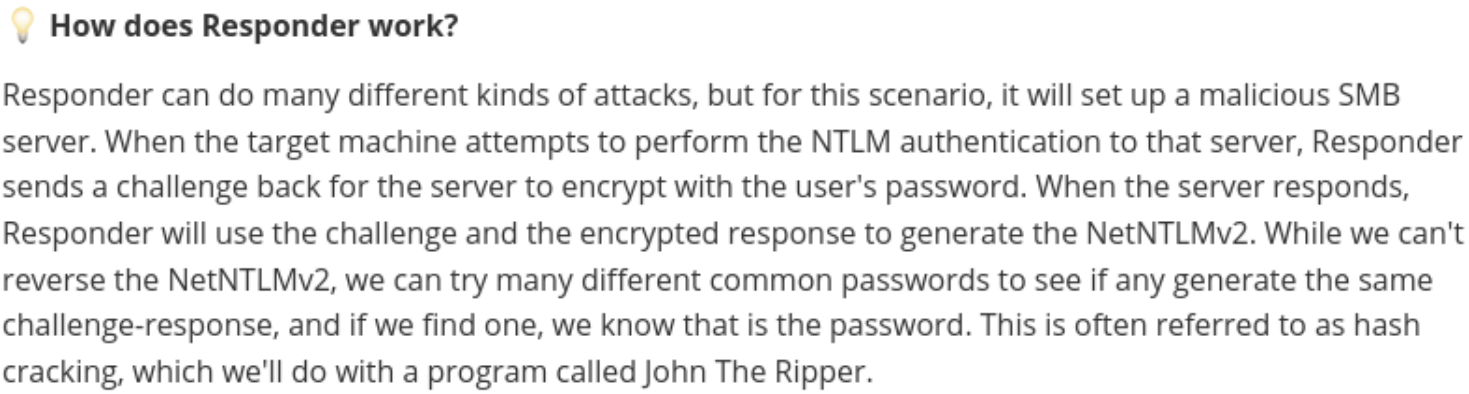
Responder

NetNTLMv2

A NetNTLMv2 challenge / response is a string specifically formatted to include the challenge and response.

Responder



NTLM

NTLM is a collection of authentication protocols created by Microsoft. It is a challenge-response
authentication protocol used to authenticate a client to a resource on an Active Directory domain.
It is a type of single sign-on (SSO) because it allows the user to provide the underlying authentication factor
only once, at login.

How does NTLM authentication work?

NTLM uses a **challenge-response protocol** to check a network user's authenticity. To do so, the client and host go through several steps:

1. The client sends a **username** to the host.
2. The host responds with a **random number** (i.e. the challenge).
3. The client then generates a **hashed password value** from this number and the user's password, and then sends this back as a response.
4. The host knows the user's password and generates a hashed password value which it can then **compare to the client's response**.
5. If both **values match**, the authenticity of the client is confirmed, and network access is granted. If there is no match between the values, the client will be denied access.

WinRM

💡 **Windows Remote Management**, or WinRM, is a Windows-native built-in remote management protocol that basically uses Simple Object Access Protocol to interact with remote computers and servers, as well as Operating Systems and applications. WinRM allows the user to :
→ Remotely communicate and interface with hosts
→ Execute commands remotely on systems that are not local to you but are network accessible.
→ Monitor, manage and configure servers, operating systems and client machines from a remote location.

As a pentester, this means that if we can find credentials (typically username and password) for a user who has remote management privileges, we can potentially get a PowerShell shell on the host.

Named Virtual Hosting

Name-Based Virtual Hosting is a method for hosting multiple domain names on one machine.
The /etc/hosts file is used to resolve a hostname into an IP address :

```
echo "10.129.128.223    unika.htb" | sudo tee -a /etc/hosts
```

FLI

Local File Inclusion (LFI) vulnerability if the page input is not sanitized.
Leads to reading file on host server:

```
http://unika.htb/index.php?
page=../../../../../../../../windows/system32/drivers/etc/hosts
```