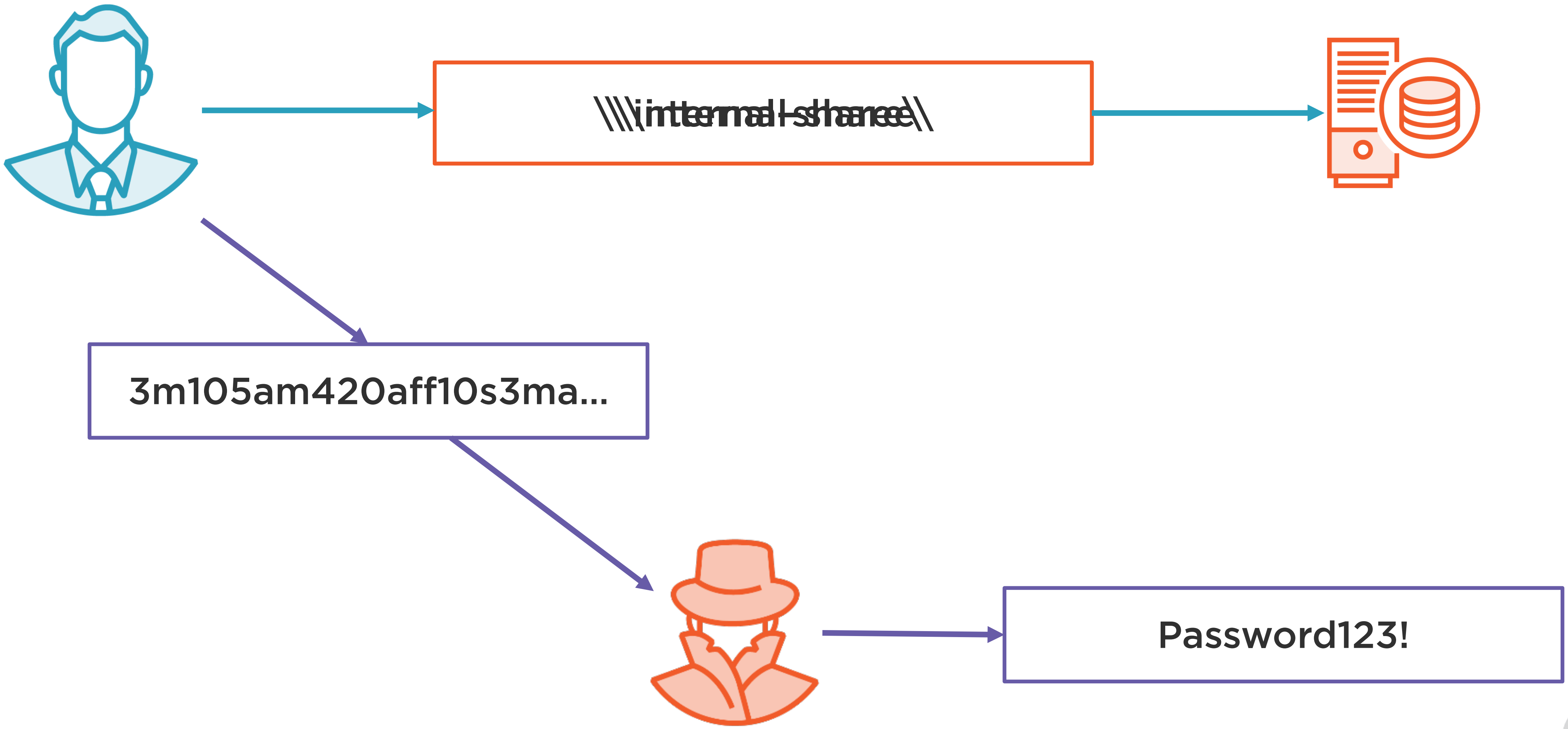
Credential Access with Responder

Ricardo Reimao
CYBER SECURITY CONSULTANT

LLMNR/NBT-NS Poisoning Attacks



\\internal-share\\

3m105am420aff10s3ma...

Password123!

```
                                         __
.----.-----.-----.-----.-----.-----.--|  |.-----.----.
|   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
|__| |_____|_____|   __|_____|__|__|_____||_____|__|
                 |__|
```

Founder: Laurent Gaffie
https://g-laurent.blogspot.com

A LLMNR, NBT-NS, and MDNS poisoner that captures hashes and passwords from several protocols, such as SMB, MSSQL, HTTP, LDAP, FTP, etc.

Open source tool (GNU v3.0)
https://github.com/lgandx/Responder

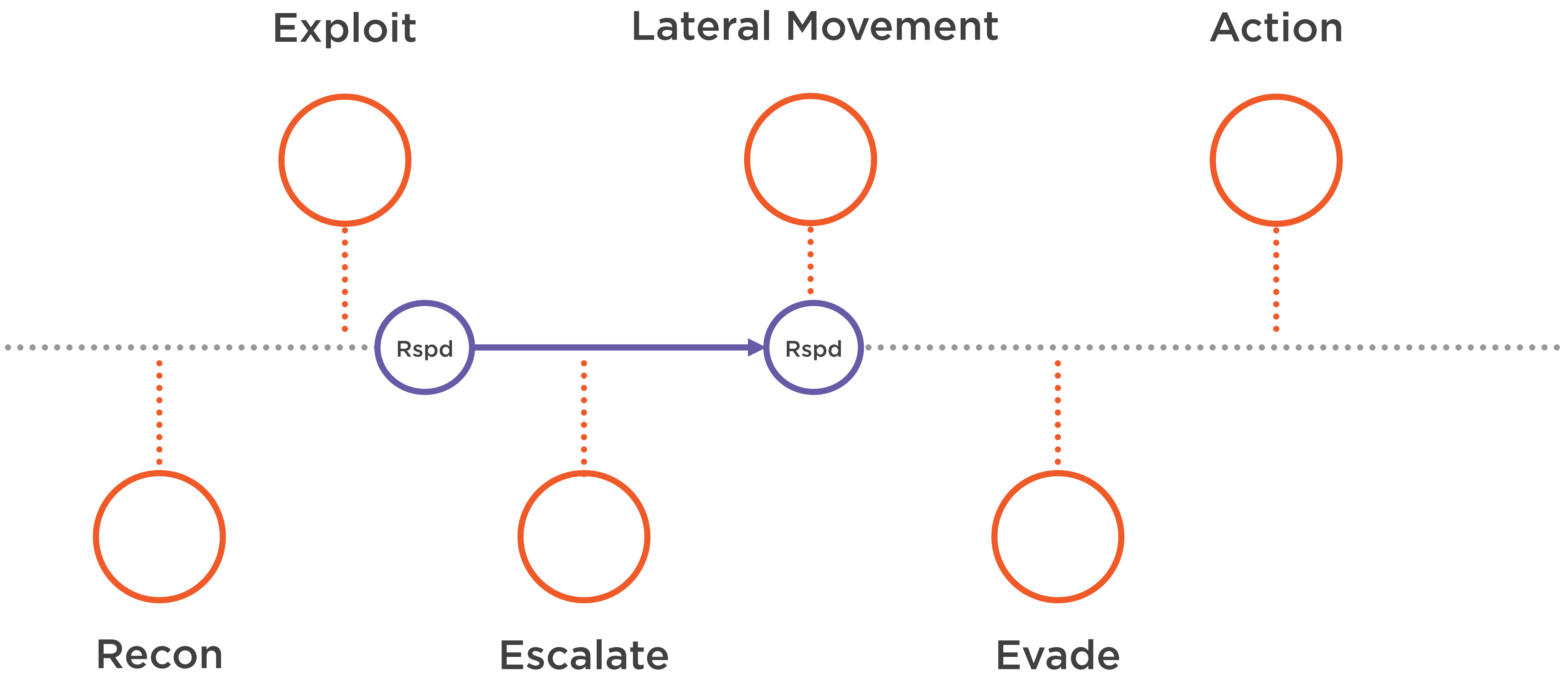
Easy to install and use

Hashes compatible with Hashcat

Support several protocols

- SMB
- FTP
- HTTP
- MSSQL
- etc.

Kill Chain

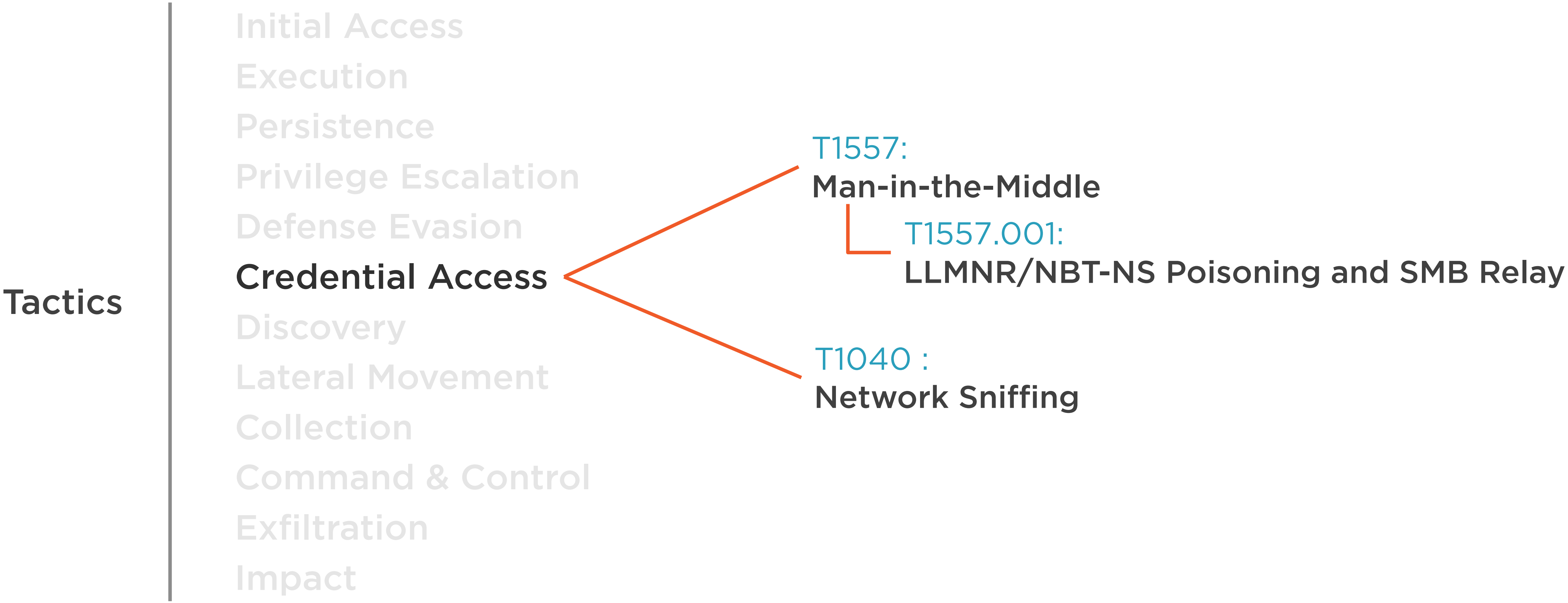

Exploit
Lateral Movement
Action
Rspd
Rspd
Recon
Escalate
Evade

MITRE ATT&CK

Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

MITRE ATT&CK



Tactics

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact

T1557:
Man-in-the-Middle

T1557.001:
LLMNR/NBT-NS Poisoning and SMB Relay

T1040 :
Network Sniffing

Staying Legal

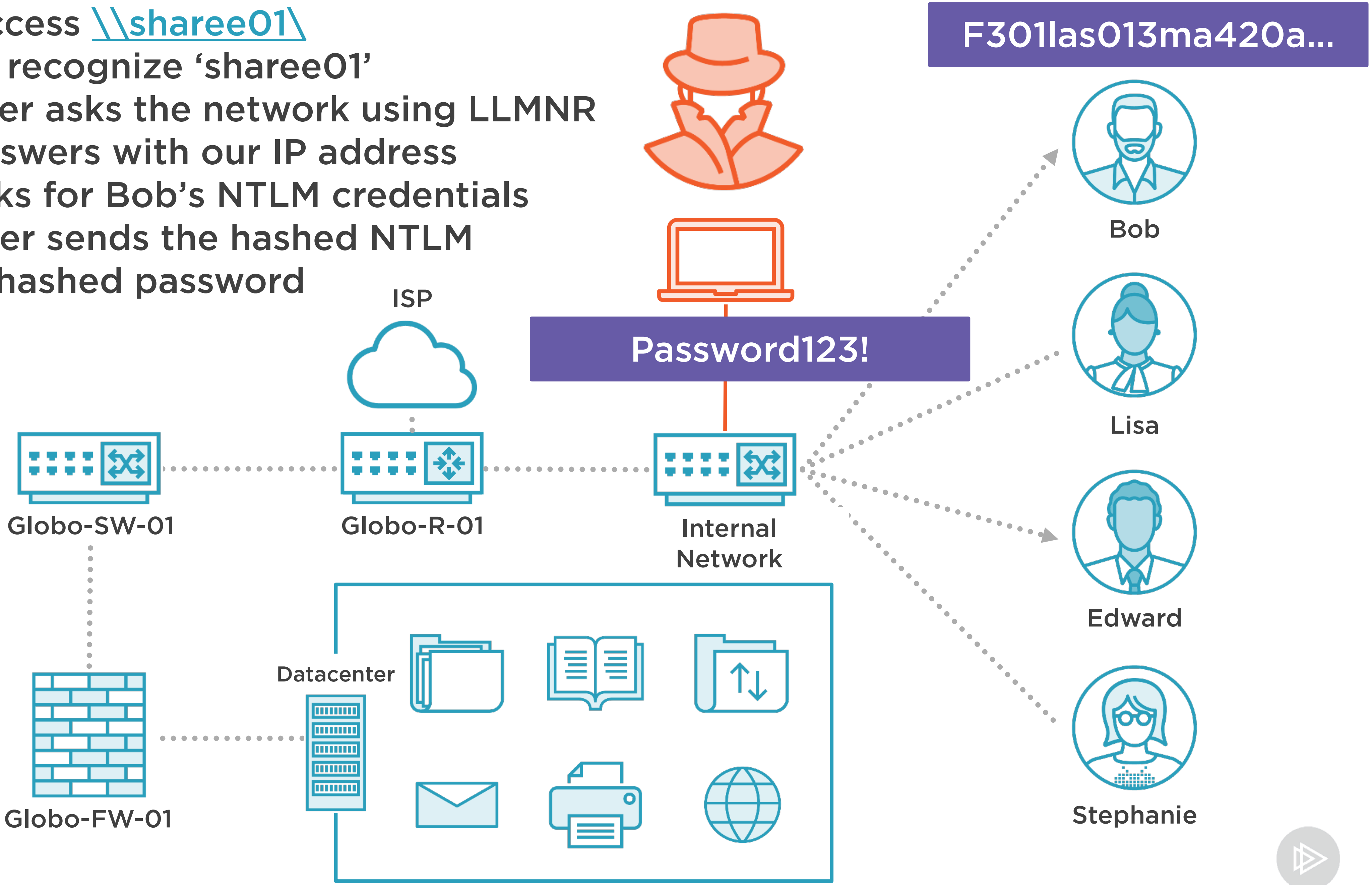
Stealing credentials without authorization is ILLEGAL in most countries

Letter of engagement, detailing dates and scope of what will be executed

Formal document, signed by the client, authorizing the types of attack you may perform

Always consult the client before any attack that may impact the network

1) Bob tries to access \\sharee01\
2) DNS does not recognize ‘sharee01’
3) Bob’s computer asks the network using LLMNR
4) Our laptop answers with our IP address
5) Our laptop asks for Bob’s NTLM credentials
6) Bob’s computer sends the hashed NTLM
7) We crack the hashed password



Prerequisites

KALI

BY OFFENSIVE SECURITY

Kali Linux

Version: 2020.1 or superior

Up to date:

```
$ apt-get update
$ apt-get upgrade
```

Small Lab Environment

Windows 2019 Domain

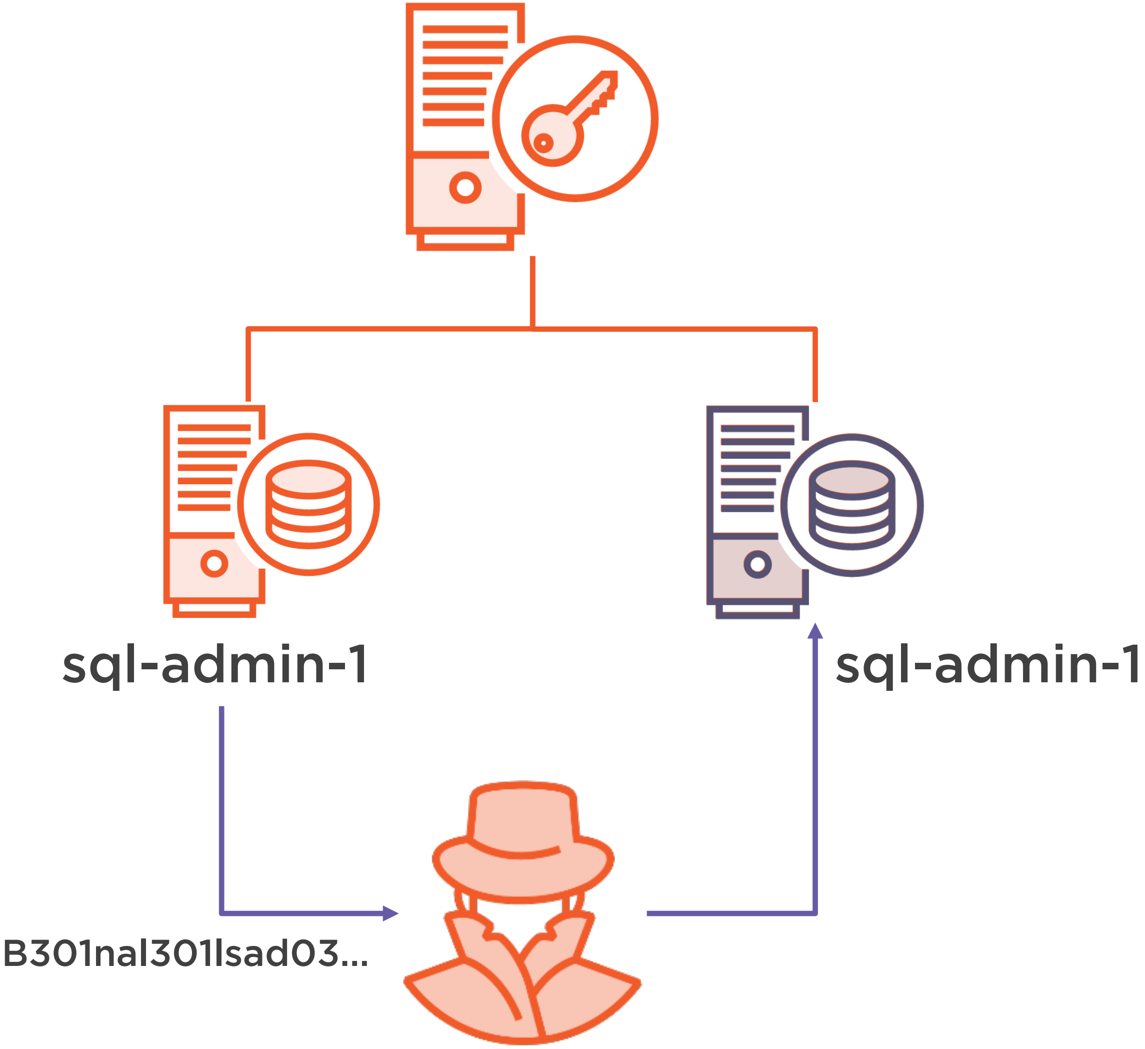
Including:

- Windows 2019 Domain Controller
- Windows 10 workstation
- Windows 2008 server

Demo Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment

Relaying NTLMv2 Credentials



More Information

Password Cracking Tools

John-The-Ripper
https://github.com/magnumripper/JohnTheRipper

Hashcat
https://hashcat.net/

Wordlists

SecLists
https://github.com/danielmiessler/SecLists

Official Documentation

Few other capabilities
https://github.com/lgandx/Responder

Remediation

Disable LLMNR and NBT-NS protocols
https://cccsecuritycenter.org/remediation/llmnr-nbt-ns

Thank you!

Ricardo Reimao
Cyber security consultant