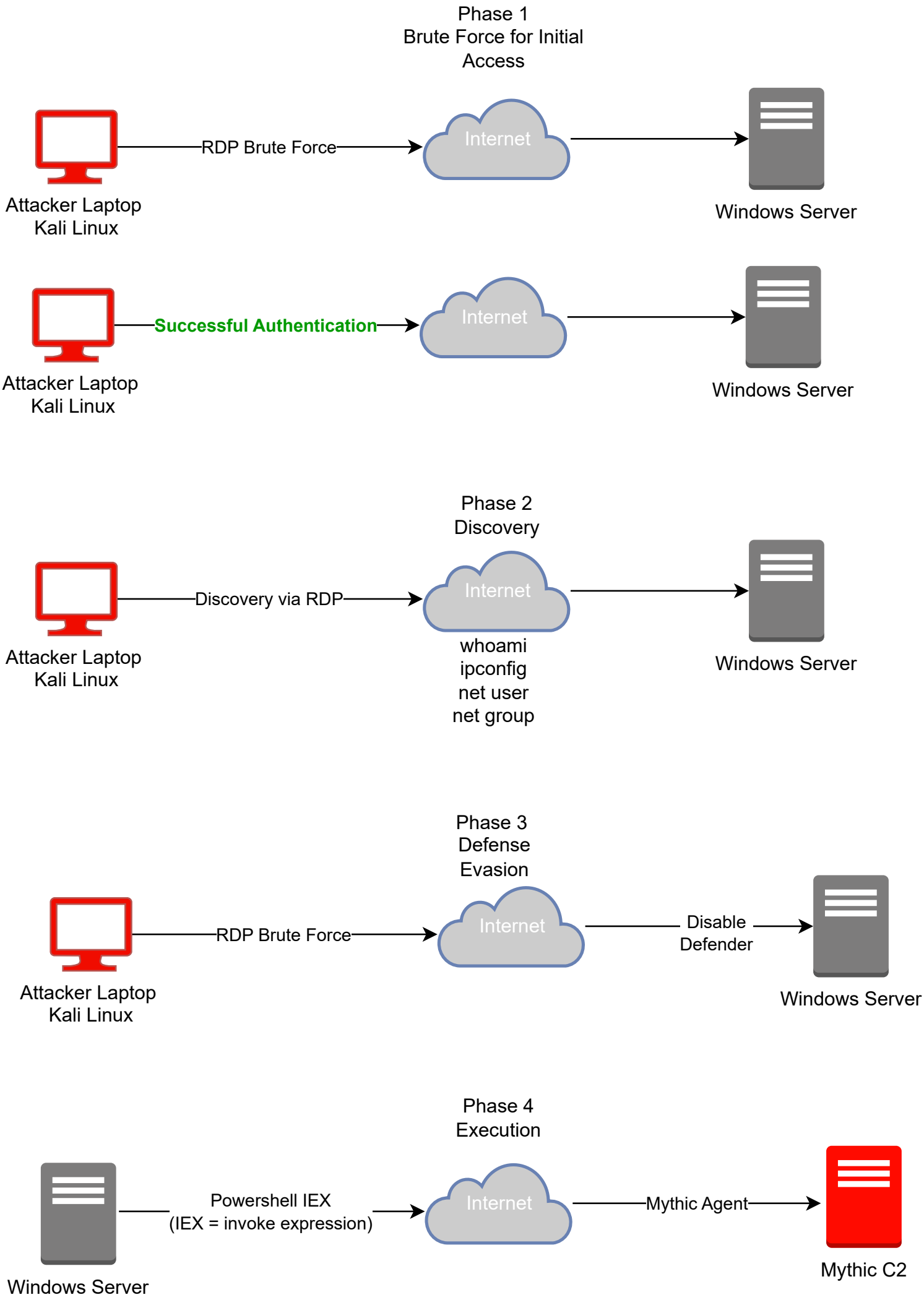
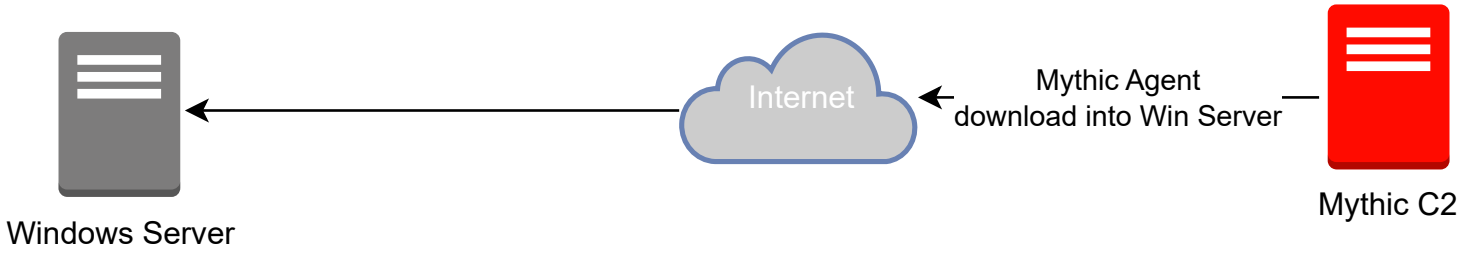
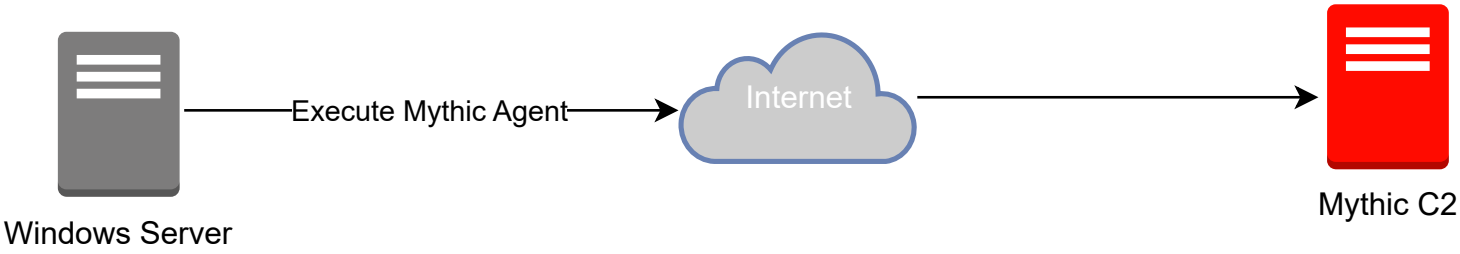
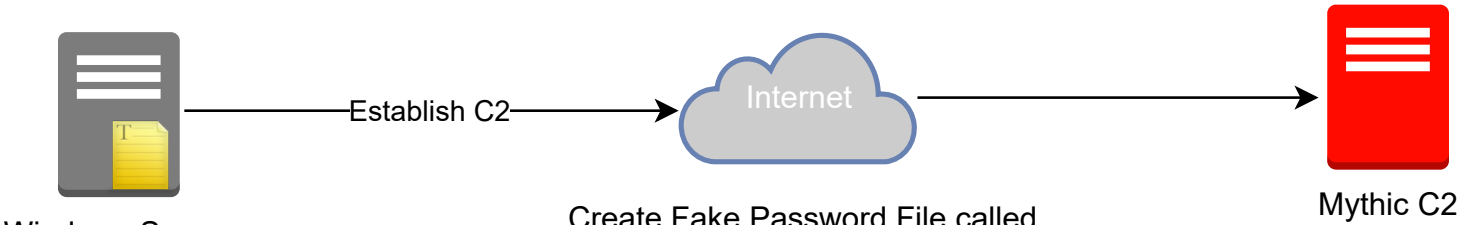

Phase 1
Brute Force for Initial Access
RDP Brute Force
Internet
Attacker Laptop
Kali Linux
Windows Server
Successful Authentication
Internet
Attacker Laptop
Kali Linux
Windows Server
Phase 2
Discovery
Discovery via RDP
Internet
whoami
ipconfig
net user
net group
Attacker Laptop
Kali Linux
Windows Server
Phase 3
Defense Evasion
RDP Brute Force
Internet
Disable Defender
Attacker Laptop
Kali Linux
Windows Server
Phase 4
Execution
Powershell IEX
(IEX = invoke expression)
Internet
Mythic Agent
Windows Server
Mythic C2

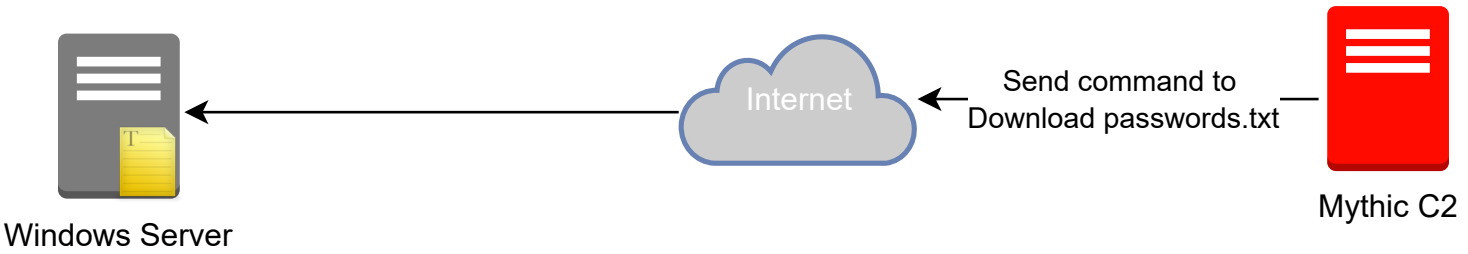




Phase 5
Command and
Control



Create Fake Password File called
(wait for it), passwords.txt

This file will be sitting in the
Windows Server, and will be the
target asset via C2

Phase 6
Exfiltration