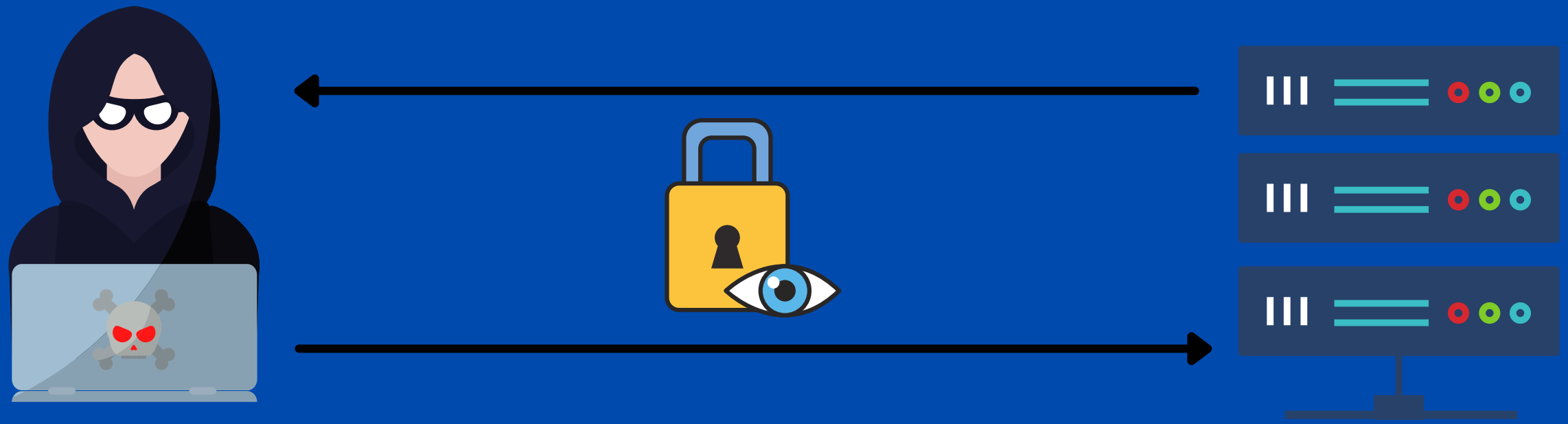
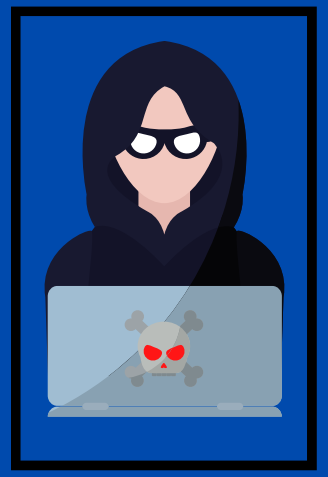
What is LLMNR Poisoning?





What is LLMNR?

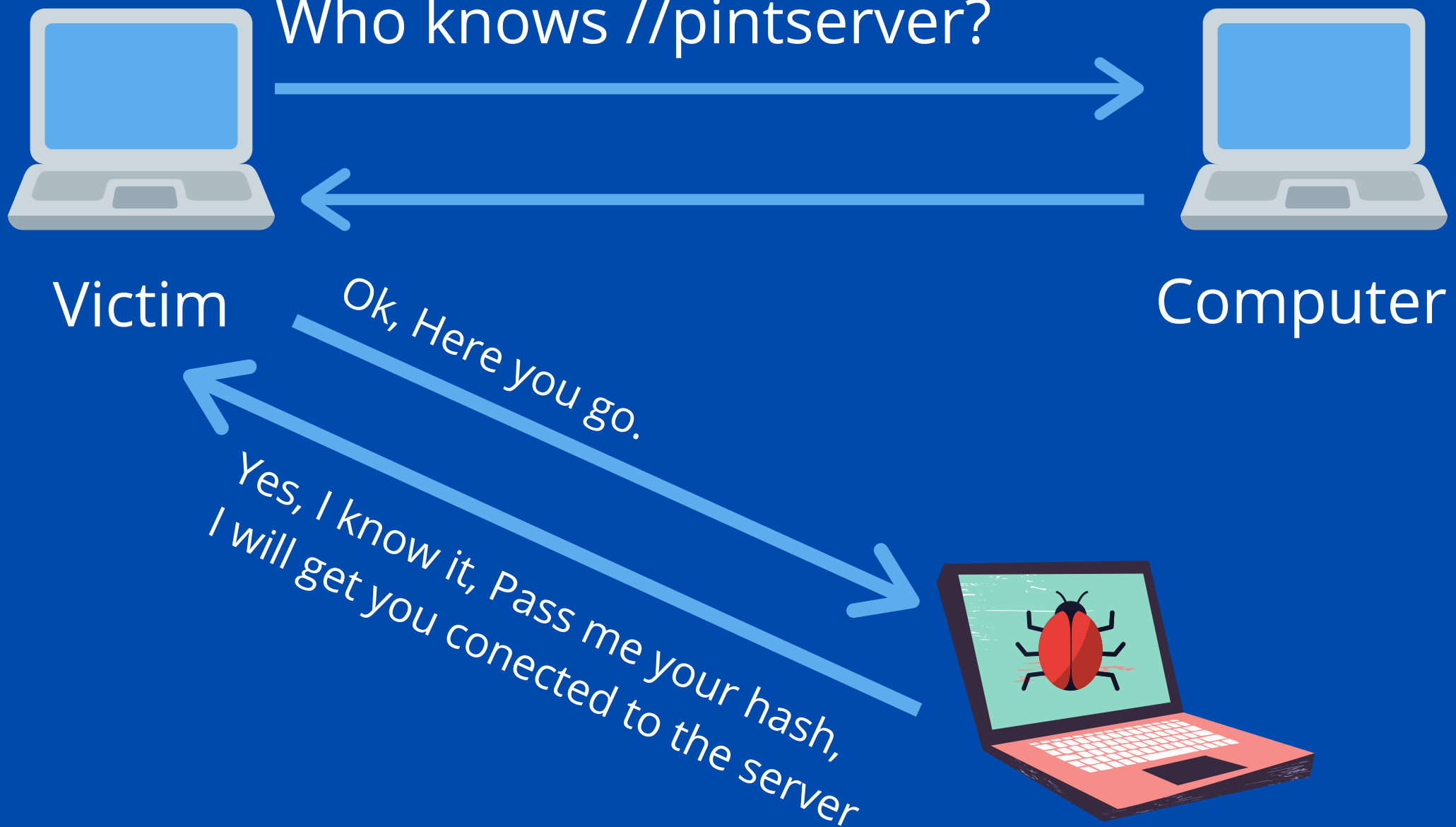
- LLMNR (Link Local Multicast Name Resolution), Is a component in Windows, Which is used to identify hosts in a network when DNS fails to do so.
- In a network, If a machine tries to resolve a particular host and DNS fails to do so, The machine will communicate with other machines in the network using LLMNR and ask if anyone knows the particular host.

Victim

Connect me to //pintserver

Sorry! Couldn't locate //pintserver

DNS Server


Who knows //pintserver?
Victim
Computer 1
Ok, Here you go.
Yes, I know it, Pass me your hash,
I will get you conected to the server
Attacker