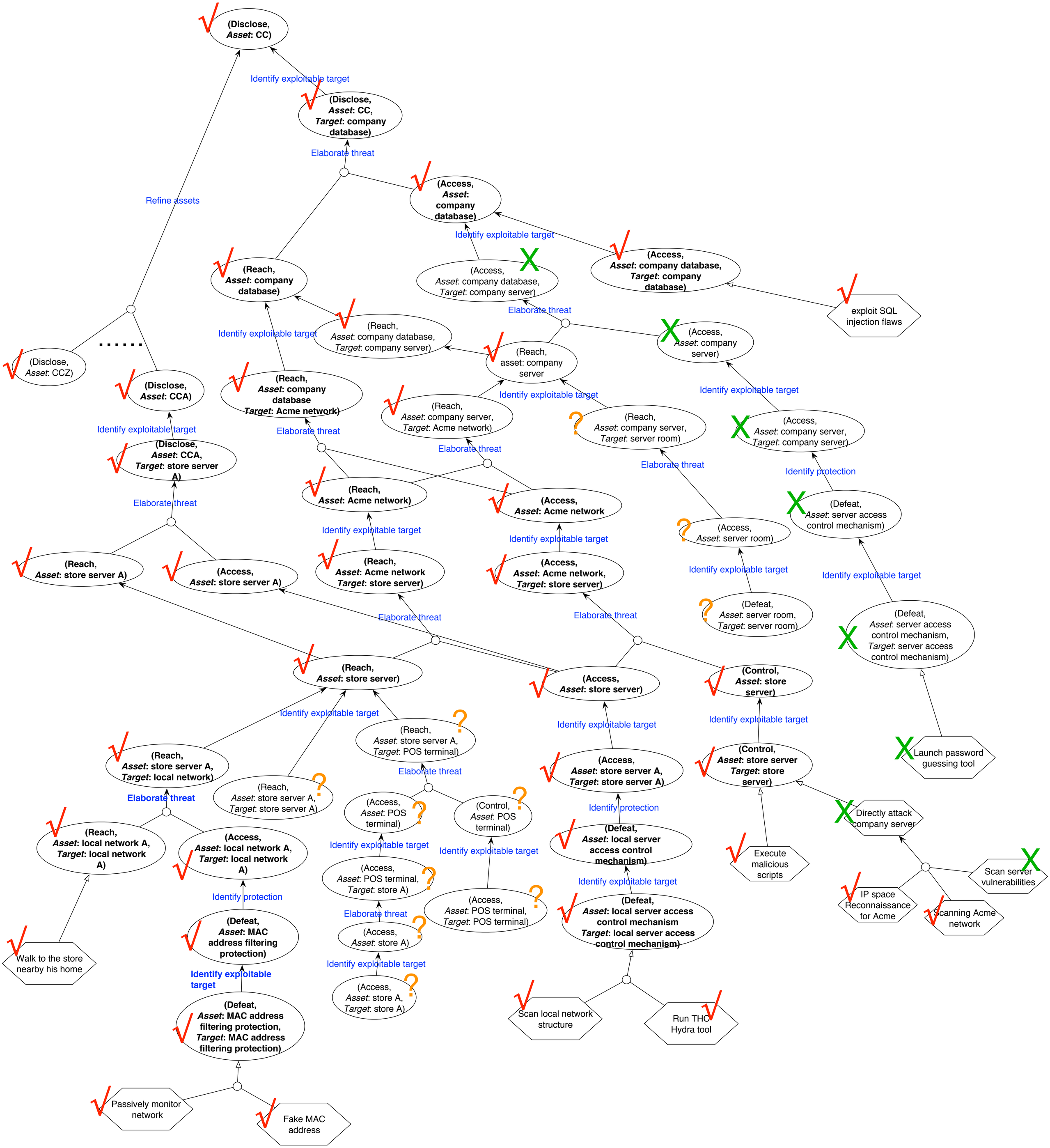
(Disclose, Asset: CC)
Identify exploitable target
(Disclose, Asset: CC, Target: company database)
Elaborate threat
Refine assets
(Access, Asset: company database)
Identify exploitable target
(Access, Asset: company database, Target: company server)
(Access, Asset: company database, Target: company database)
exploit SQL injection flaws
(Reach, Asset: company database)
Identify exploitable target
(Reach, Asset: company database, Target: company server)
Elaborate threat
(Reach, asset: company server
(Access, Asset: company server)
(Disclose, Asset: CCZ)
(Disclose, Asset: CCA)
(Reach, Asset: company database Target: Acme network)
Identify exploitable target
(Reach, Asset: company server, Target: Acme network)
Identify exploitable target
(Reach, Asset: company server, Target: server room)
Identify exploitable target
(Access, Asset: company server, Target: company server)
Identify exploitable target
(Disclose, Asset: CCA, Target: store server A)
Elaborate threat
Elaborate threat
Elaborate threat
Elaborate threat
(Reach, Asset: Acme network)
(Access, Asset: Acme network
Identify exploitable target
Identify exploitable target
(Access, Asset: server room)
Identify protection
(Defeat, Asset: server access control mechanism)
(Reach, Asset: store server A)
(Access, Asset: store server A)
(Reach, Asset: Acme network Target: store server)
(Access, Asset: Acme network, Target: store server)
Identify exploitable target
Identify exploitable target
(Defeat, Asset: server room, Target: server room)
(Defeat, Asset: server access control mechanism, Target: server access control mechanism)
Elaborate threat
Elaborate threat
(Reach, Asset: store server)
(Access, Asset: store server)
(Control, Asset: store server)
Identify exploitable target
Identify exploitable target
Identify exploitable target
(Reach, Asset: store server A, Target: POS terminal)
(Reach, Asset: store server A, Target: local network)
(Reach, Asset: store server A, Target: store server A)
(Access, Asset: store server A, Target: store server A)
(Control, Asset: store server Target: store server)
Launch password guessing tool
Elaborate threat
Elaborate threat
(Access, Asset: POS terminal)
(Control, Asset: POS terminal)
Identify protection
Directly attack company server
(Reach, Asset: local network A, Target: local network A)
(Access, Asset: local network A, Target: local network A)
Identify exploitable target
Identify exploitable target
(Defeat, Asset: local server access control mechanism)
Execute malicious scripts
Scan server vulnerabilities
Identify protection
(Access, Asset: POS terminal, Target: store A)
(Access, Asset: POS terminal, Target: POS terminal)
Identify exploitable target
IP space Reconnaissance for Acme
Scanning Acme network
Walk to the store nearby his home
(Defeat, Asset: MAC address filtering protection)
Elaborate threat
(Access, Asset: store A)
Identify exploitable target
(Defeat, Asset: local server access control mechanism Target: local server access control mechanism)
Identify exploitable target
(Defeat, Asset: MAC address filtering protection, Target: MAC address filtering protection)
(Access, Asset: store A, Target: store A)
Scan local network structure
Run THC Hydra tool
Passively monitor network
Fake MAC address