Routing On The Internet

Routers handle packets navigation throughout the internet.
Each router maintains a routing table – specifying its’ connections and available destinations.
Our attacks allows the injection of false information to routers’ routing table, thus disrupting correct flow of information.

False Adjacency Attack

Attack Goal – Establishing an adjacency with a phantom router.
Motivation – Being adjacent is a powerful position.
Attack Method
• Exploits a weakness to become a master in the adjacency bring up process.
• This allows to form an adjacency without receiving victims’ replies.
Attack scenario implemented using Scapy and works on the simulated network with no adjustments to theoretical attack.
Effect – Loss of communication between hosts.

Adjacency Corrumpption Attack

Attack Goal – Controlling the fightback mechanism.
Motivation – Knowing when fightback occurs helps to overcome it.
Attack Method
• Exploit a weakness in the checksum mechanism to force the victim to initiate fight back with known checksum.
• Send an LSA disguised as the legitimate fight back.
Attack scenario implementation using Scapy works on the simulated network.
Expected effect - Loss of communication between hosts.

OSPF Routing Protocol - Key Features

Open Shortest Path First
Dijkstra Algorithm based routing topology
Link State Advertisement Protocol
Most protocol data is exchanged exclusively over adjacencies
Built in fight-back mechanism to avoid persistence of false information.

OSPF Routing Protocol- Key Features- Adjacency

Adjacency Bring-up protocol
Each router broadcasts hello messages.
Each router forms adjacencies with its’ neighbors by synchronizing their knowledge of the network topology (Link State Database).

Tools Used

OMNET++ and INET - network simulator frameworks
GNS3 - Cisco Network Simulator
VPCS - Virtual PC Simulator
Scapy - Python Based Packet Handler
Wireshark - Network Protocol Analyzer

Summary

We presented two new ways to exploit vulnerabilities in the OSPF protocol specification.
The attacks are successful on the most recent version of Cisco IOS – 15.0(1)M.
We have proven the ability of a single router to effectively and persistently falsify other routers’ routing table.