Reactions and Responses
IP Spoofing Stimuli

• Why would an attacker spoof his source address?
  – Hide the attacker’s activity
    • nmap decoy option
  – Hide the attacker’s identity

• To be able to view the responses, the attacker
  – Positioned between the location of this spoofed IP address and the targeted machine
  – Subvert one or more intermediate routers
IP Spoofing Stimuli - Spoofing ICMP/UDP Datagrams

- ICMP and UDP and connectionless and stateless

- It is often impossible to determine whether a received UDP or ICMP packet has been forged just by looking at the received packet in isolation
Spoofing TCP Connections

• TCP
  – connection-oriented
  – Maintain state

• How will the attacker respond to the SYN-ACK packet?
  – Switching to promiscuous mode
  – Predict the TCP sequence numbers used by the target machines
  – Subvert routers between the attacker’s host and the target host
  – The attacker might not intend to respond to the SYN-ACK packet
    • Half-open port scan
    • SYN flooding attack
IP Spoofing Responses – Spoofed ICMP Packets

• Attacker sends an ICMP echo request
  – An ICMP echo reply to the spoofed IP address
  – An ICMP Destination Unreachable message to the spoofed address if inbound ICMP echo request packets are rejected

• For the spoofed machine
  – Discard the received unwarranted ICMP echo reply
Spoofed UDP Packets
Response to TCP SYN Packets

Attacker sends SYN packet with spoofed source address to target.

Is the port open on the target system?

Target sends a SYN-ACK to spoofed address.

Does the spoofed IP address exist?

Spoofed host sends a RST packet back to the target system.

Intermediate router sends ICMP destination unreachable packet to target. Target ignores ICMP error messages and resends SYN-ACK packet until TCP timeout. Target then sends RST to spoofed address.

Intermediate router sends ICMP destination unreachable packets to target. Target ignores ICMP error messages and resends SYN-ACK packet until TCP timeout. Target then sends RST to spoofed address.

Should be “RST-ACK”
Example Traces

- Port closed
  - Spoofed IP address does not exist

```plaintext
10:50:20.723225 nonexistent.spoofed.host.51801 > the.victim.machine.ssh: 
  S 4192915610:4192915610(0) win 4096
10:50:20.724391 the.victim.machine.ssh > nonexistent.spoofed.host.51801: R 0:0(0)
  ack 4192915611 win 0 (DF)
  spoofed.host unreachable (DF)
```
Example Traces

What intrusion activities can you derive from this trace?

- Port open
- Spoofed IP address exists
Example Traces

- A normal connection attempt to a closed port
Example Traces

1

Port open
Spoofed IP does not exist

2
Example Traces – Con’t

3

11:23:06.693735 the.victim.machine.telneta > nonexistent.spoofed.host.34913:
3190922609:3190922609(0) ack 1788196385 win 9112 <mss 536> (DF)
spoofed.host unreachable (DF)

• Port open
Spoofed IP does not exist
Finally, the victim host sends a RST packet.
Spoofed TCP ACK Packets

- Attacker sends ACK packet with spoofed source address.
- Does the target system exist?
  - YES: Target sends a RST-ACK to spoofed address.
  - NO: Intermediate router sends ICMP destination unreachable packet to spoofed address.
- Does the spoofed IP address exist?
  - YES: Spoofed host silently discards RST-ACK packet.
  - NO: Intermediate router sends ICMP destination unreachable packet to target system.
    - Target silently discards this ICMP error message.
- Intermediate router silently discards ICMP error message.
  - In accordance with RFC1812, the router does not generate its own ICMP destination unreachable message.
Third-Party Effects

• What if it is your IP address that the attacker chooses to spoof?
Third-Party ICMP Packets

• If you receive ICMP echo reply packets, without sending ICMP echo requests, your IP address has probably been spoofed.

• Smurf attack
  – You receive ICMP echo reply packets from many hosts at the same time
  – The attacker sends an ICMP echo request packet to the broadcast address of a suitably exposed network. The source address is spoofed to be yours
Third-Party TCP Packets

• Unexpected inbound SYN-ACK packets followed by outbound RST packets
  – Probably, attacker sending a SYN packet using your address as the source address to an open port

• Unexpected inbound RST-ACK packets
  – Probably, the spoofed packet is sent to a closed port