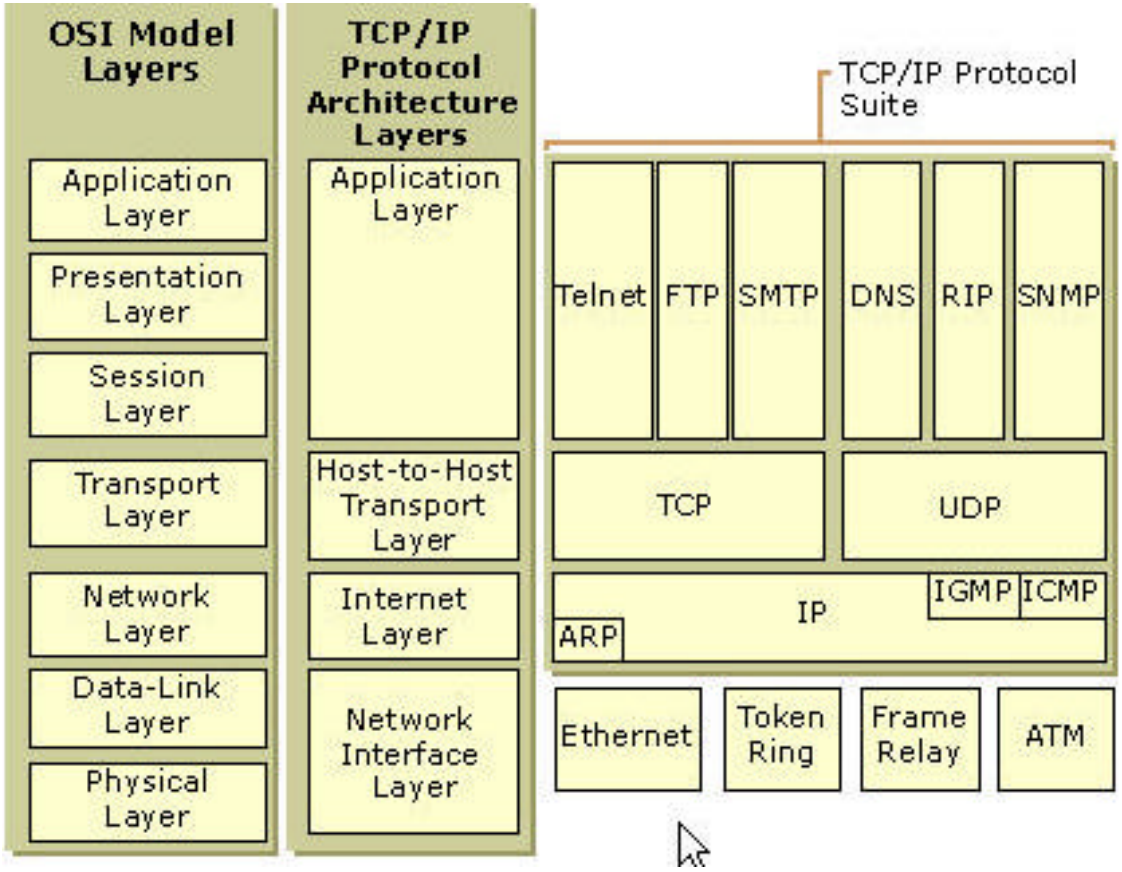
System and Network Hacking

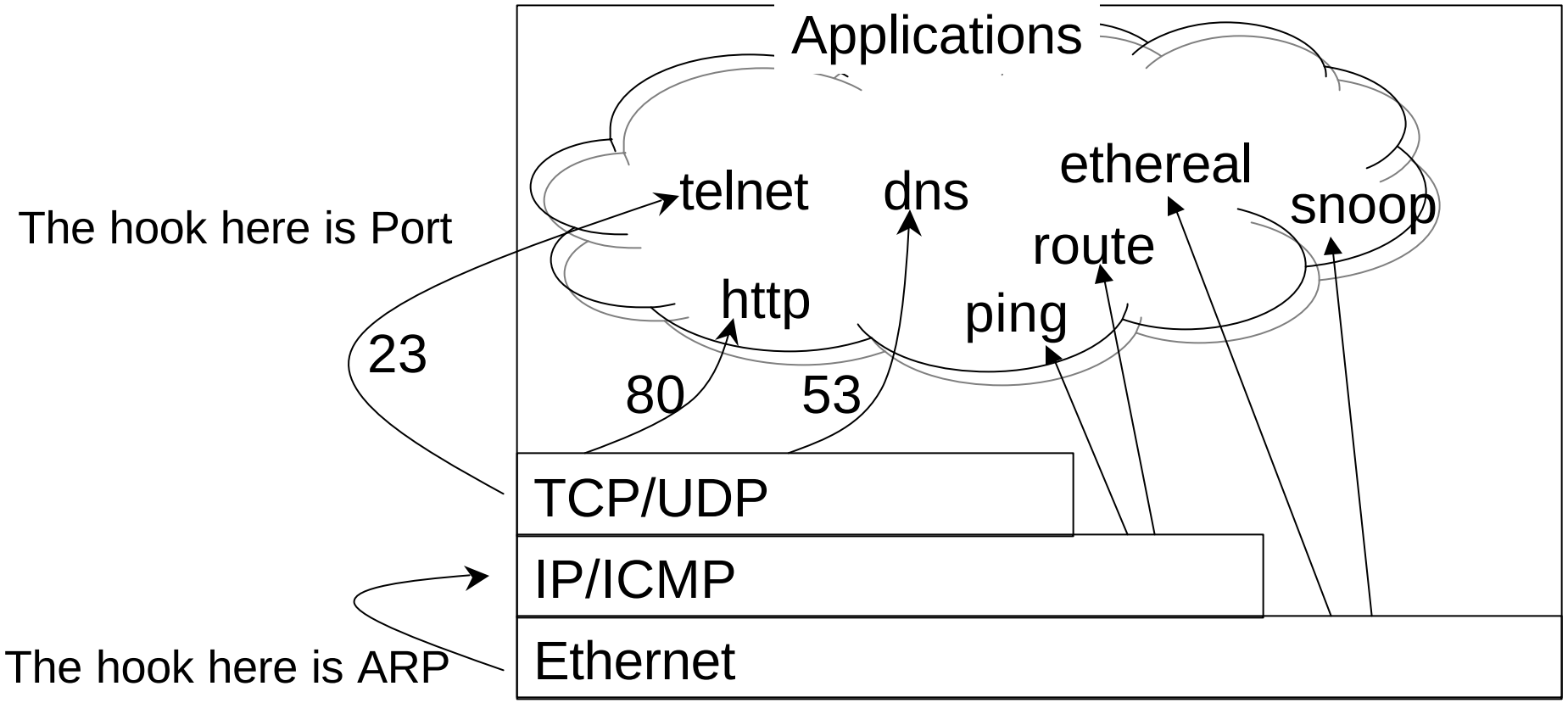
David Askey

TechNow, Inc.

TCP/IP Protocol Stack



TCP/IP Protocol Stack



Architectural Vulnerabilities

- Two most critical rules of security
  - Authentication
  - Authorization
- Without authentication you can spoof anything or anybody
- Authorization is worthless with weak or no authentication
- TCP/IP has weak authentication by design

Architectural Vulnerabilities

- TCP/IP identifies parties by addresses
- Each layer has addressing
  - Ethernet (MAC) addresses
  - IP Addresses
  - Port Addresses
  - Application Addresses (NFS block, User, etc.)

Architectural Vulnerabilities

- TCP/IP determines addressing through resolution
- Ethernet: Address Resolution Protocol (ARP)
- IP: Domain Name Service (DNS)

Architectural Vulnerabilities

- Resolution: Who is www.technow.com
  - Internet packet delivery is limited to IP Addresses
    - DNS resolves IP Address
    - Placed in cache on client and server
  - Local subnet packet delivery is limited to Ethernet Addresses
    - ARP resolves Ethernet Address
    - Placed in ARP cache for communicating nodes

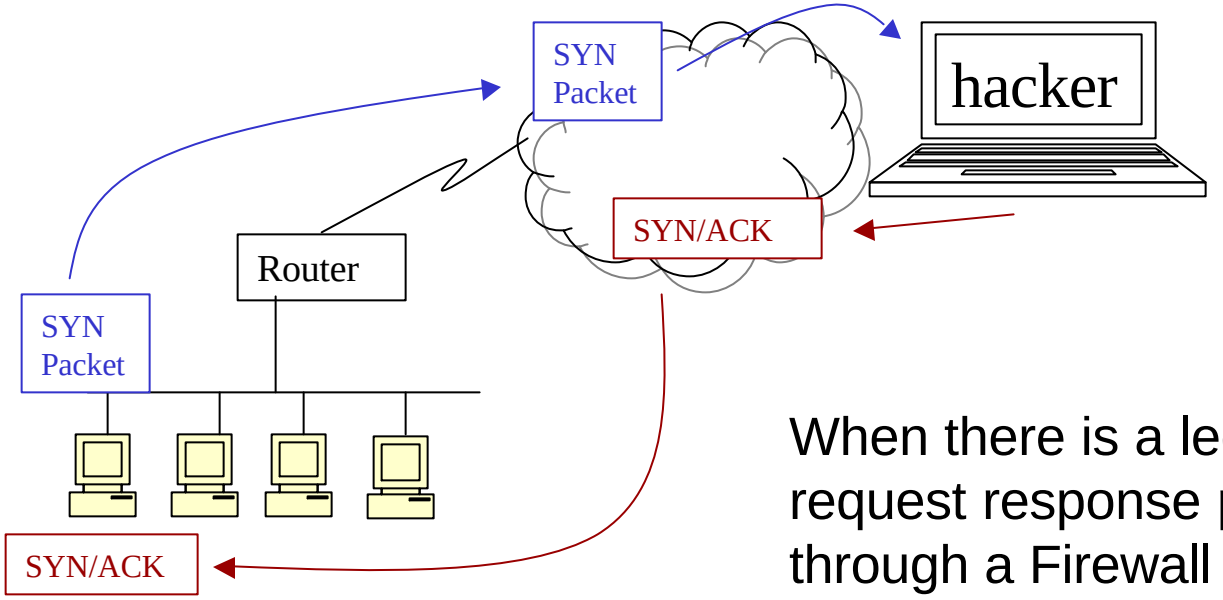
Architectural Vulnerabilities

- Since TCP/IP identifies parties by addresses the hacker attempts to spoof addresses
- Address resolution within TCP/IP, DNS and ARP are not authenticated
- You can easily masquerade as some other person or node
- ARP spoofing circumvents switches

TCP/IP Exploits

- MAC Layer (Ethernet) TCP/IP exploits
- TCP Session hijacking
- TCP Session Application viewing
- TCP Password Monitoring
- Back Channels
- Denial of Service Attacks
- Packet Generation Attacks and Replays

Legitimate Packets



When there is a legitimate internal request response packets are allowed through a Firewall or a Router

If an internal node has been compromised, you are cooked

Subseven, reverse telnet, browsers

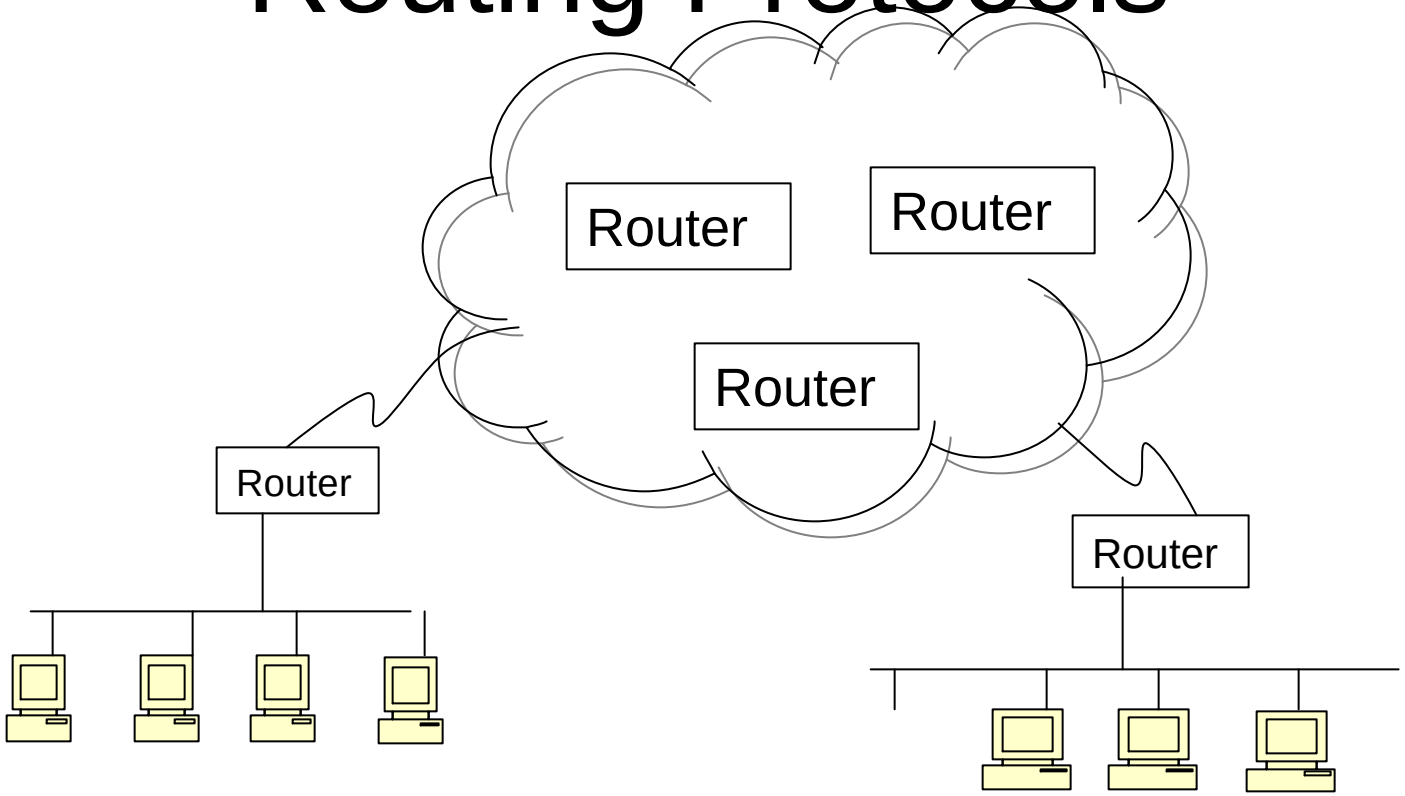
Back Doors into Networks

- Utilize an internal compromised node
  - The internal node connects to internet
  - Seen as legitimate traffic
  - Return traffic from hacker is considered “Authorized”
  - Can tunnel within specific protocols to circumvent proxy based firewalls

DEMO ONE

Network Backdoor

Routing Protocols

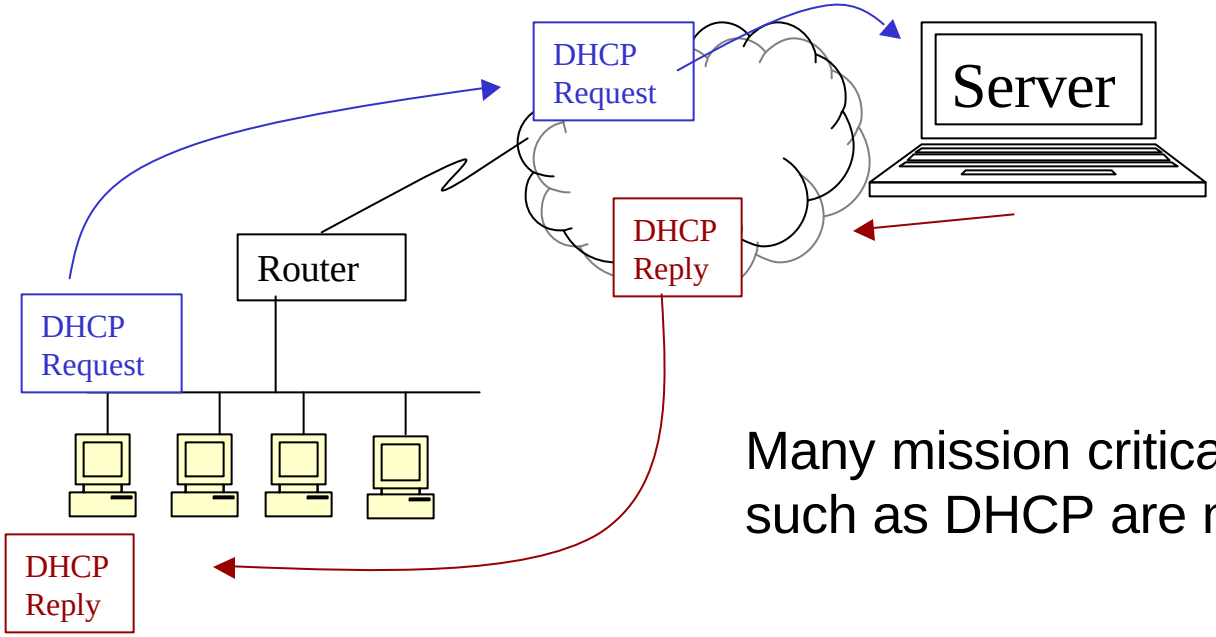


- Routers learn of other networks through routing protocols
- RIP, OSPF, IGRP, EIGRP
- Routing protocols do not provide authentication or need configuration
- You can send networks off a cliff

DEMO TWO

Router Attack

DHCP Packets



Many mission critical service requests such as DHCP are not authenticated

A rogue client
- could absorb all theavailable DHCP leases
- release existing leases

DEMO THREE

DHCP Attack

Session Hijacking

- The act of either packet insertion or taking control of a connection
- Typically requires clear sessions (not encrypt)
- Not detected by either of the originating parties
- In conjunction with ARP spoofing or IP spoofing/relays works across an enterprise

Packet Sniffing

- Can occur wherever networks are unencrypted (basically everywhere)
- Can easily circumvent switches
- Expose traffic to be process by specialized programs

DEMO FOUR

Password Capture
Webspy
Email Capture

Intrusion Detection

- Intrusion Detection System IDS
  - Software based
  - Automates the detection of suspicious activity
  - Uses examples (signatures) of known attacks
- Two primary purposes
  - Capture all network activity
  - Alert us to any suspicious activity

Snort Overview

- Network intrusion detection mode
  - The most complex and configurable configuration
  - Analyze network traffic for matches against a user defined rule set and perform several actions based upon what it sees

Snort Rules

- Divided into two logical sections
  - Rule Header and Rule Options

- Rule Header
  - Rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination ports information.

```
alert tcp any any -> 192.168.1.0/24 111
```

Snort Custom Data

- You can do a pattern match for text in the data.

- The following rule should be entered on a single line. 50 is P, 61 is a, 73 is s, 73 is s, …… 20 is a space

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:
    "telnet password"; content: "|50 61 73 73 77 6f 72 64 3a 20|";)
```

Snot

- Arbitrary packet generator
- Uses snort rules files as its source of packet information
- Can be used as an IDS evasion tool, by using specific decoy hosts
- Snort uses rules to monitor packets, Snot uses those same rules to generate packets

```
snot -r snort.rules -s 192.168.1.0/24 -d 192.168.3.0/29
```

DEMO FIVE

Distraction Attack with SNOT