



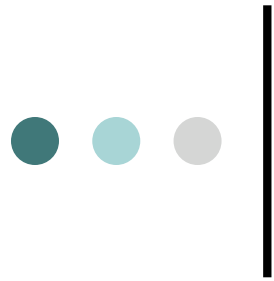
# Network Infrastructure Security

APRICOT 2005 Workshop

February 18-20, 2005

Merike Kaeo

[merike@doubleshotsecurity.com](mailto:merike@doubleshotsecurity.com)



# Agenda (Day 1)

- Threat Models
  - What Are We Protecting Against?
- Securing The Device
  - Physical and Logical Connections
    - User Authentication / Authorization
    - Access Control
  - Logging Information Integrity
  - System Image / Configuration Integrity
- LAB
  - Securing The Infrastructure Device
  - SSH on LINUX and to the Router



# Agenda (Day 2)

- Securing Data Traffic
  - Packet Filters
  - Encryption (IPsec vs SSL)
- Securing Routing Protocols
  - Route Authentication (MD5)
  - Filtering Policies
  - Flap Damping
  - Prefix Limits
- LAB



# Agenda (Day 3)

- Auditing Tools
  - Sniffers and Traffic Analyzers
  - Vulnerability Assessment (Nessus, NMAP)
- Logging Information
  - What To Log
  - Storing Logs
- Mitigating DoS Attacks
  - Blackhole /Sinkhole Routing
  - Rate Limiting
- LAB



# What Are Security Goals?

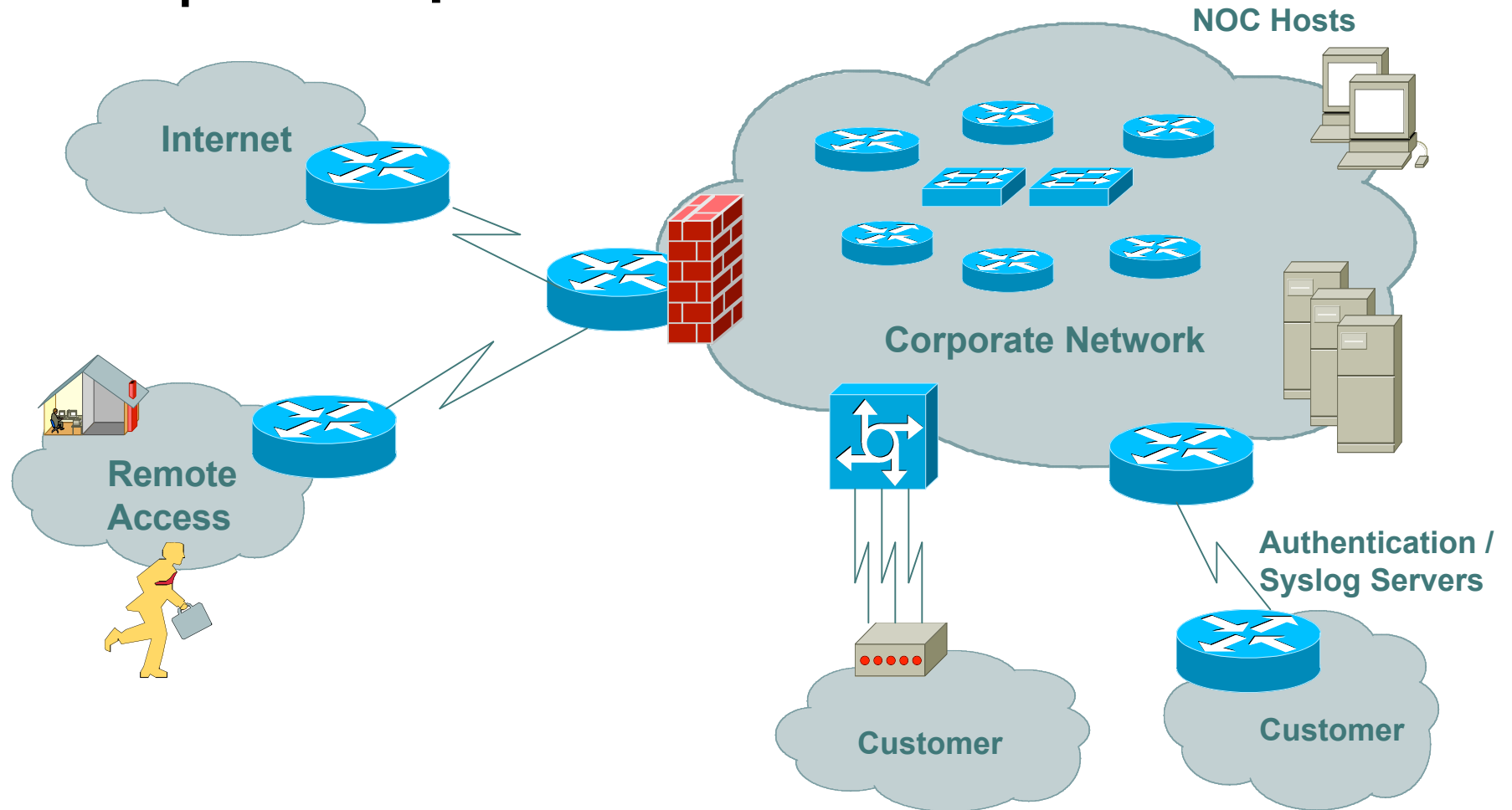
- Controlling Data / Network Access
- Preventing Intrusions
- Responding to Incidences
- Ensuring Network Availability
- Protecting information in Transit

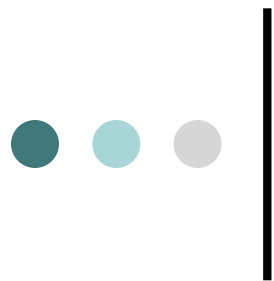


# First Step.....Security Policy

- What are you trying to protect?
  - What data is confidential?
  - What resources are precious?
- What are you trying to protect against?
  - Unauthorized access to confidential data?
  - Malicious attacks on network resources?
- How can you protect your site?

# Typical Network Components





# Security Services We Need To Consider

- User Authentication
- User Authorization
- Data Origin Authentication
- Access Control
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation



# Varying Degrees of Robustness for Security Elements

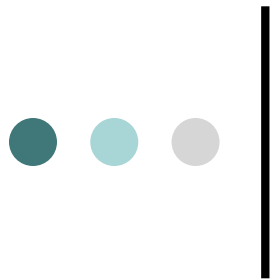
Will I Go Bankrupt ?



- Spend More Money
- Spend More Time

Is It An Embarrassment ?

**NEED TO DO A RISK ANALYSIS !**



# Risk Mitigation vs Cost of Security

***Risk mitigation:*** the process of selecting appropriate controls to reduce risk to an acceptable level.

The ***level of acceptable risk*** is determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy.

**Assess the cost of certain losses and do not spend more to protect something than it is actually worth.**



# The Security Practices Should Include.....

- Physical security controls
  - Media
  - Equipment location
  - Environmental safeguards
- Logical security controls
  - Subnet boundaries
  - Routing boundaries
  - Logical access control (preventative / detective)
- System and data integrity
  - Firewalls
  - Network services
- Data confidentiality



# The Security Practices Should Include....

- Mechanisms to verify and monitor security controls
  - Accounting
  - Management
  - Intrusion detection
- Policies and procedures for staff that is responsible for the corporate network
  - Secure backups
  - Equipment certification
  - Use of Portable Tools
  - Audit Trails
  - Incident Handling
- Appropriate security awareness training for users of the corporate network



# Definitions (rfc 2828)

**Threat:** A threat is a potential for a security violation, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

**Threat Action (attack):** an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system

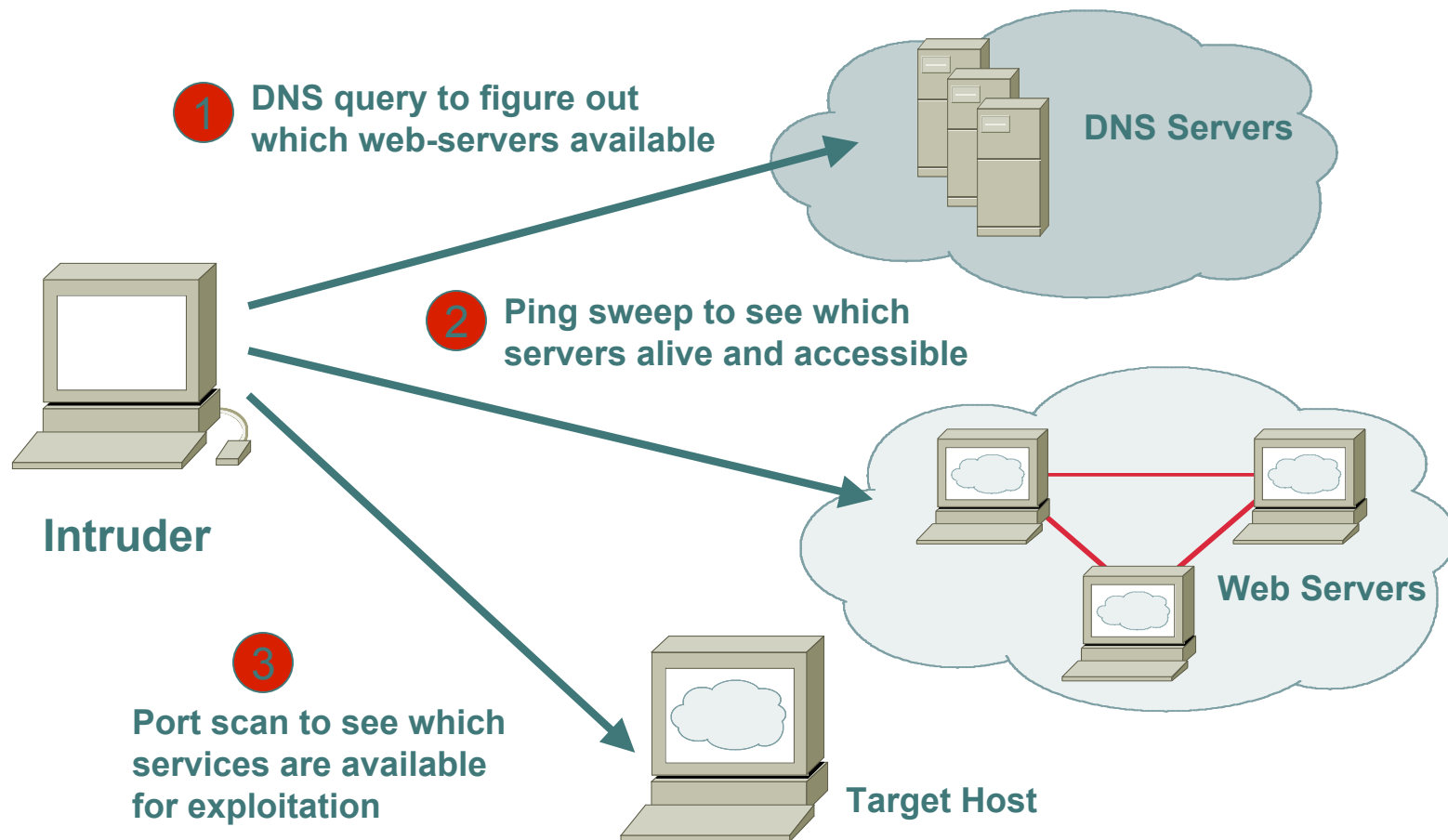
**Threat Consequence:** The threat consequences are the security violations which results from a threat action, i.e. an attack.



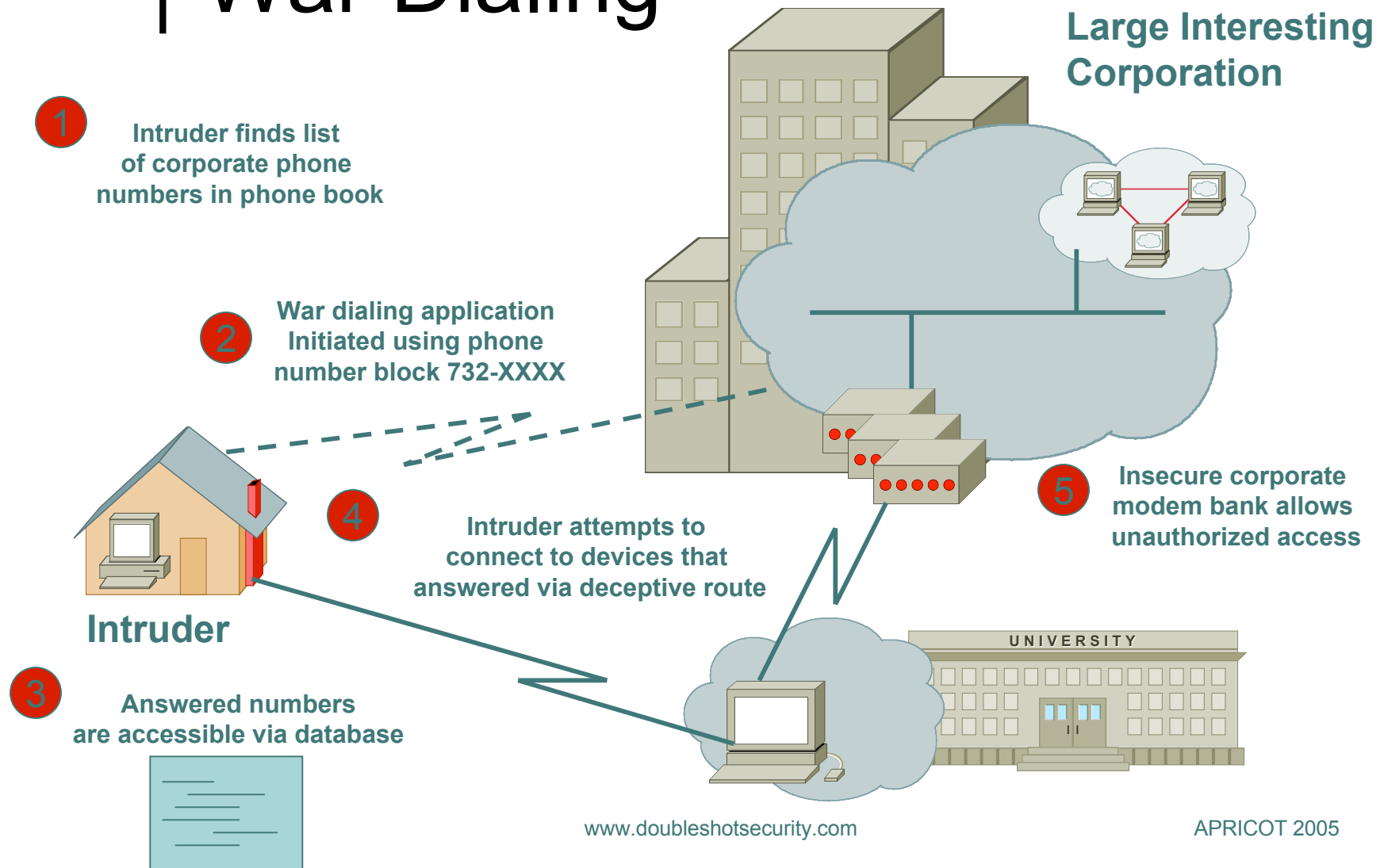
# Network Attack Sources

- Passive vs Active
  - Eavesdropping
  - Scanning by injecting traffic
- On-Path vs Off-Path
- Insider vs Outsider
  - Trusted/authorized individual causing security compromise ?
- Deliberate vs Unintentional
  - Unintentional causes same problems as deliberate attack

# Example Active Reconnaissance Attempt



# Off-Path, Outsider Attack: War Dialing







# Threat Consequences

- (Unauthorized) Disclosure
  - A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
- Deception
  - A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
- Disruption
  - A circumstance or event that interrupts or prevents the correct operation of system services and functions.
- Usurpation
  - A circumstance or event that results in control of system services or functions by an unauthorized entity.

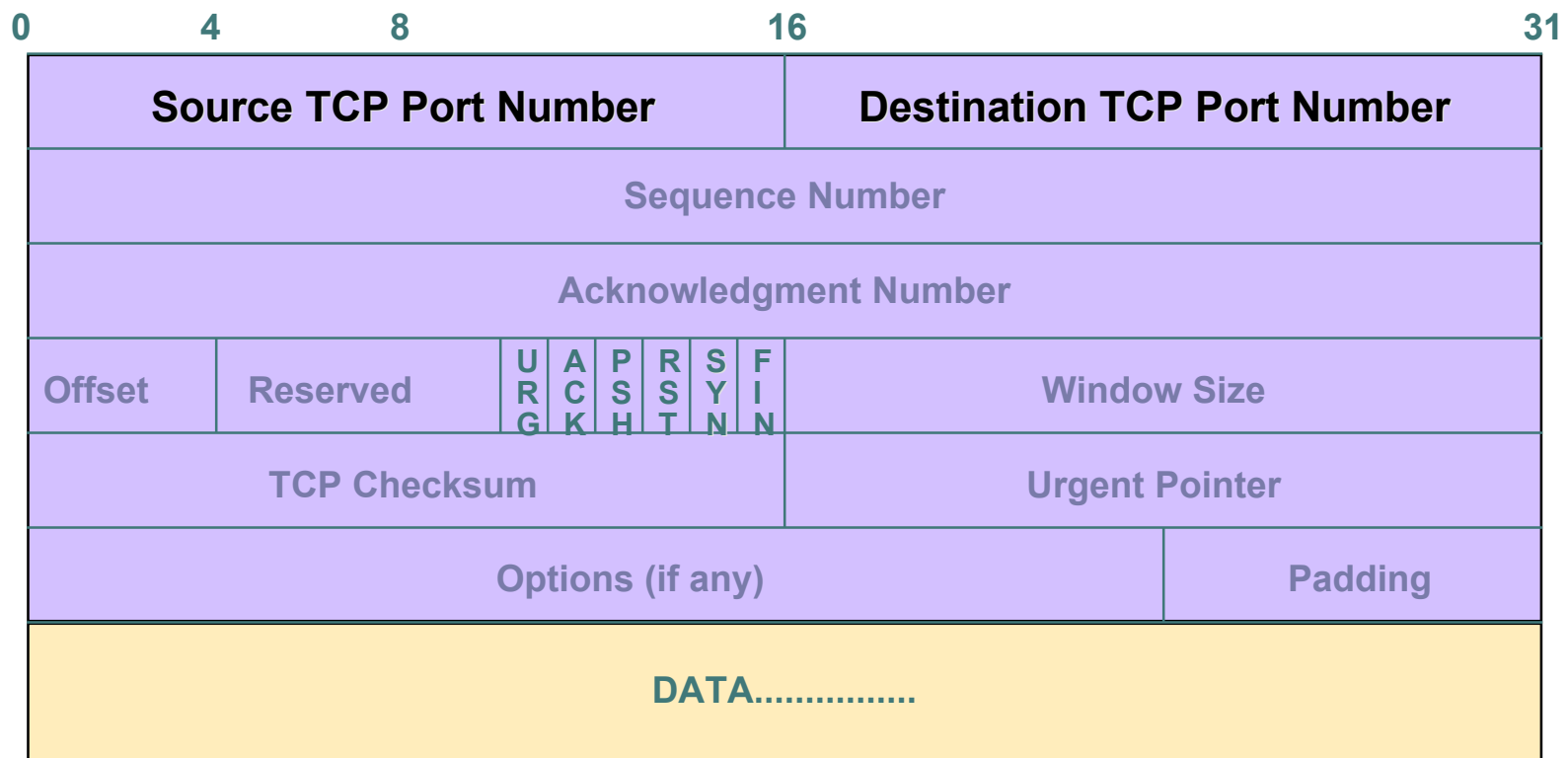


# Disruption Often Caused by DoS and DDoS Attacks

- TCP SYN
- TCP ACK
- UDP, ICMP, TCP floods
- Fragmented Packets
- IGMP flood
- Spoofed and un-spoofed

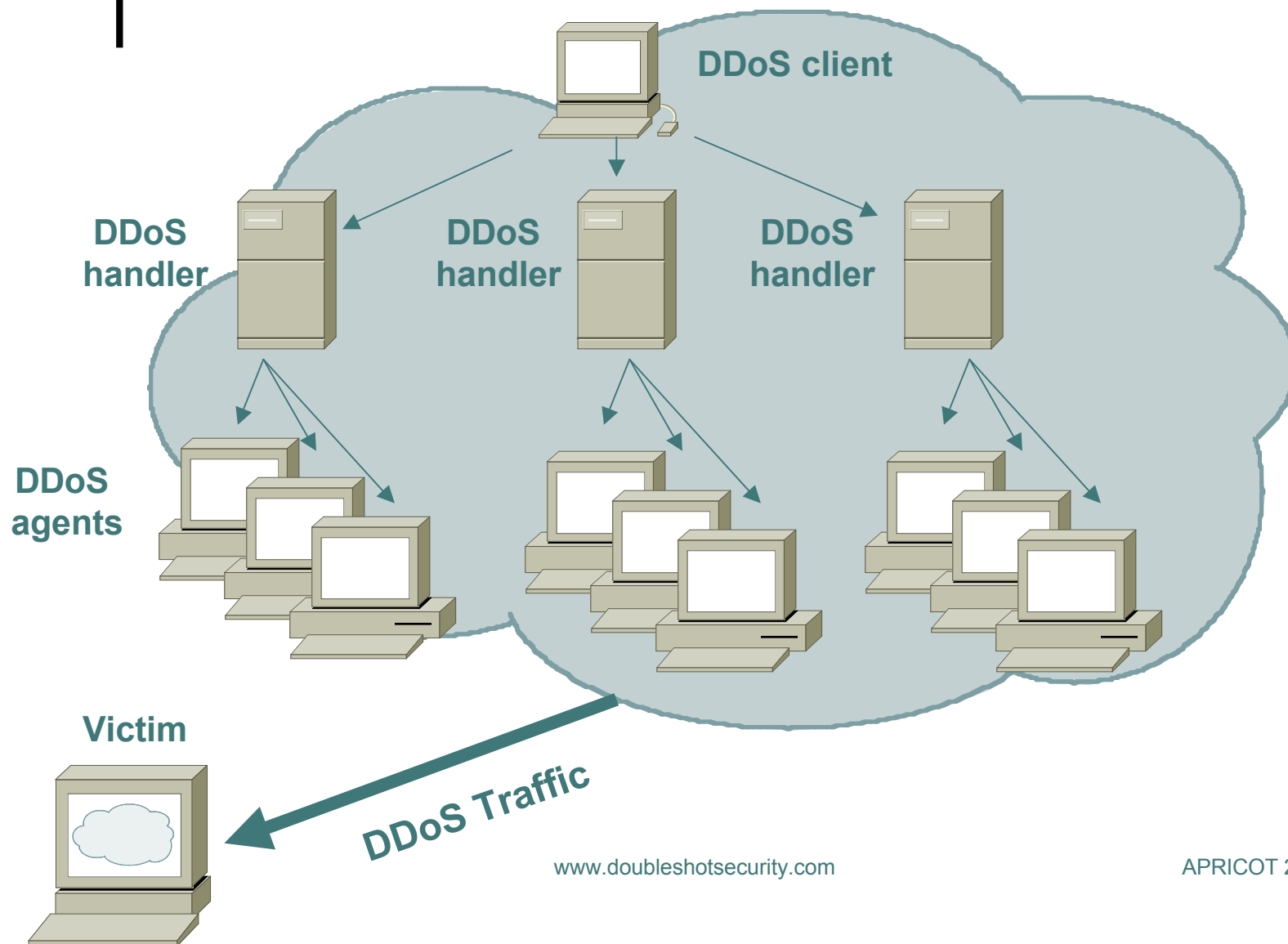


# TCP Packet Format

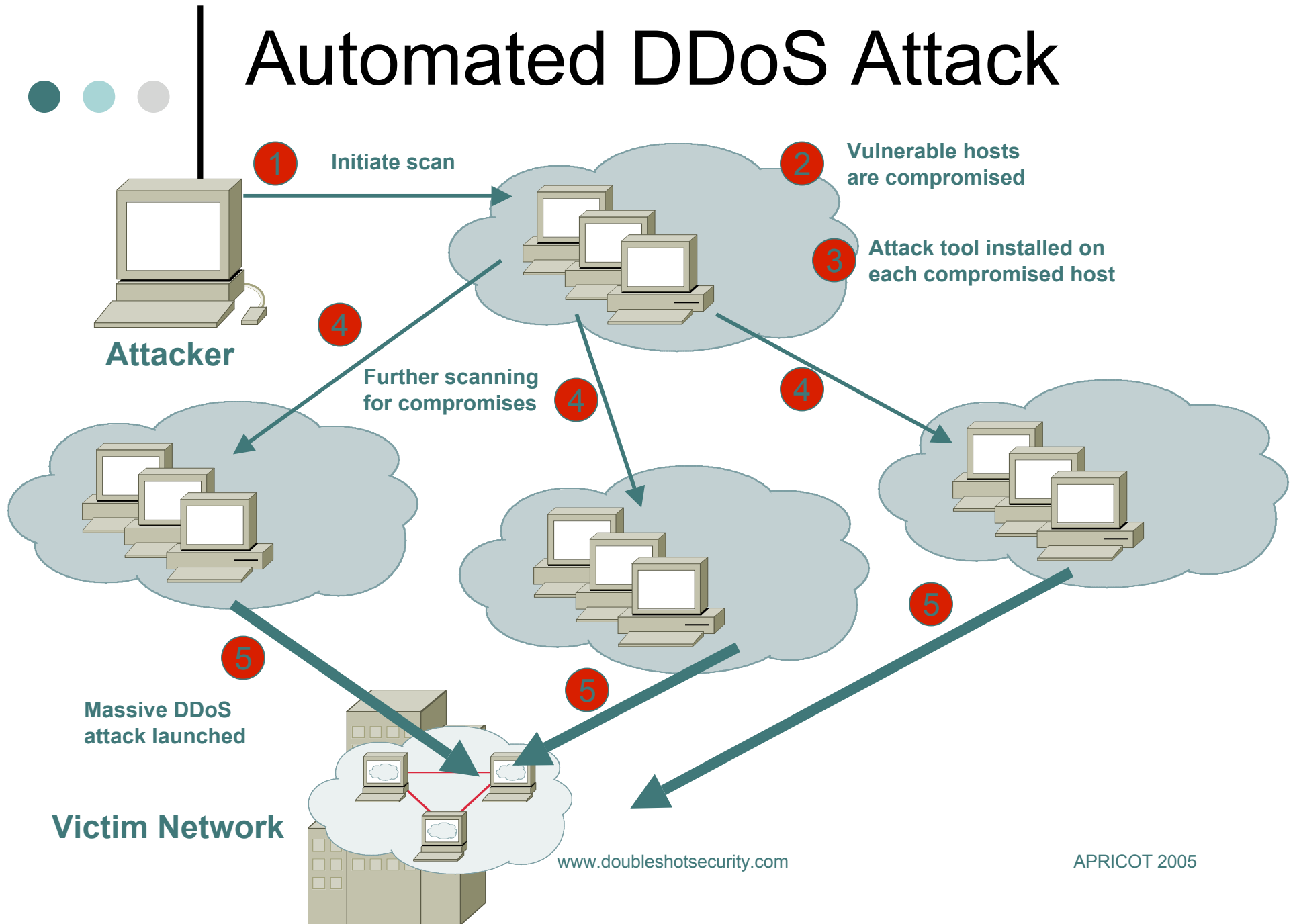


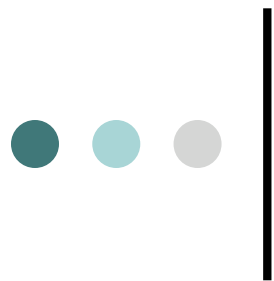


# Basics of a DDoS Attack



# Automated DDoS Attack





# DDoS Is A Huge Problem

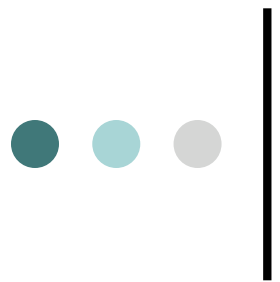
- Distributed and/or coordinated attacks
  - Increasing rate and sophistication
- Infrastructure protection
  - Coordinated attack against infrastructure
  - Attacks against multiple infrastructure components
- Overwhelming amounts of data
  - Huge effort required to analyze
  - Lots of uninteresting events



# What If Router Becomes Attack Target?

It allows an attacker to:

- Disable the router & network...
- Compromise other routers...
- Bypass firewalls, IDS systems, etc...
- Monitor and record all outgoing and incoming traffic...
- Redirect whatever traffic they desire...

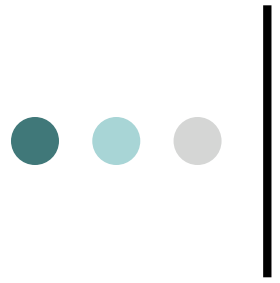


# Router CPU Vulnerabilities

## CPU Overload

- Attacks on applications on the Internet have affected router CPU performance leading to some BGP instability
- 100,000+ hosts infected with most hosts attacking routers with forged-source packets
- Small packet processing is taxing on many routers...even high-end
- Filtering useful but has CPU hit





# Securing The Device

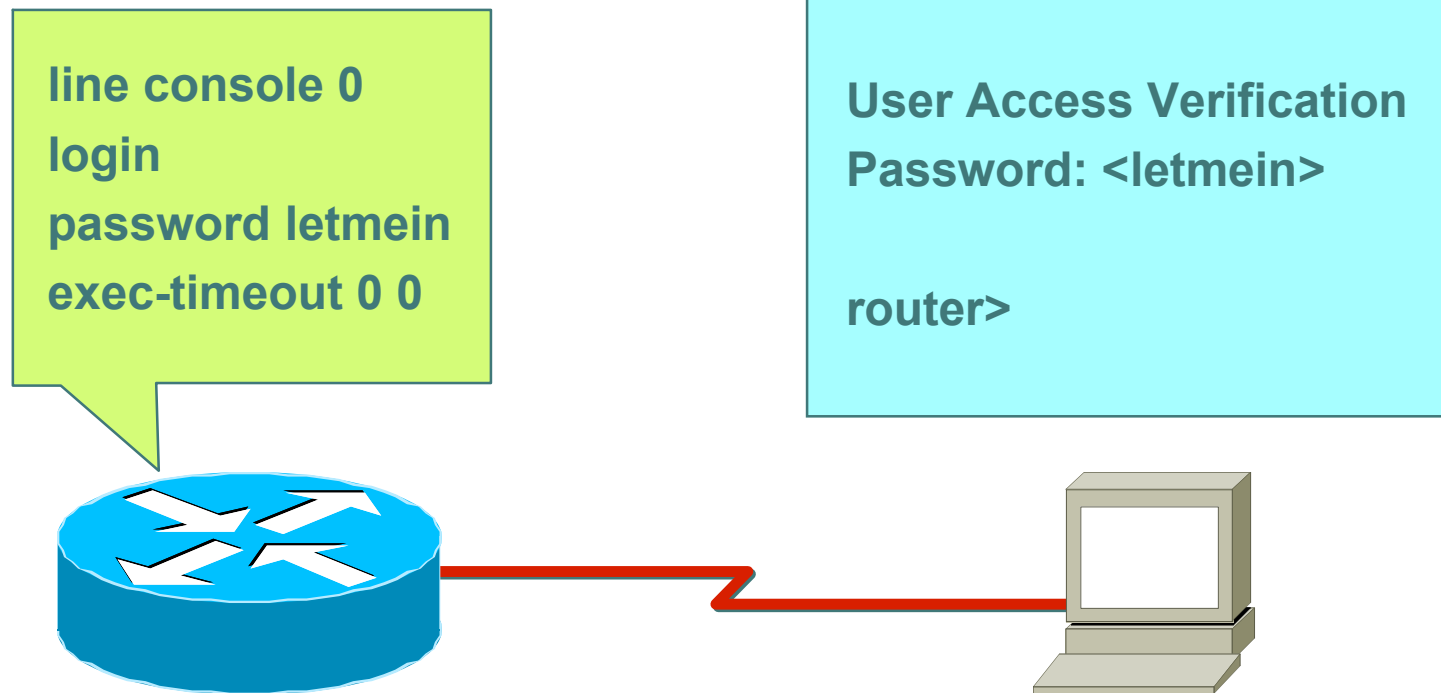
- Miscreants have a far easier time gaining access to devices than you think.
- Ensure that the basic security capabilities have been configured.



# Fundamental Device Protection Security Practices

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through ssh
- Disable device access methods that are not used
- Protect SNMP if used
- Shut down unused interfaces
- Shut down unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners
- Test device integrity on a regular basis

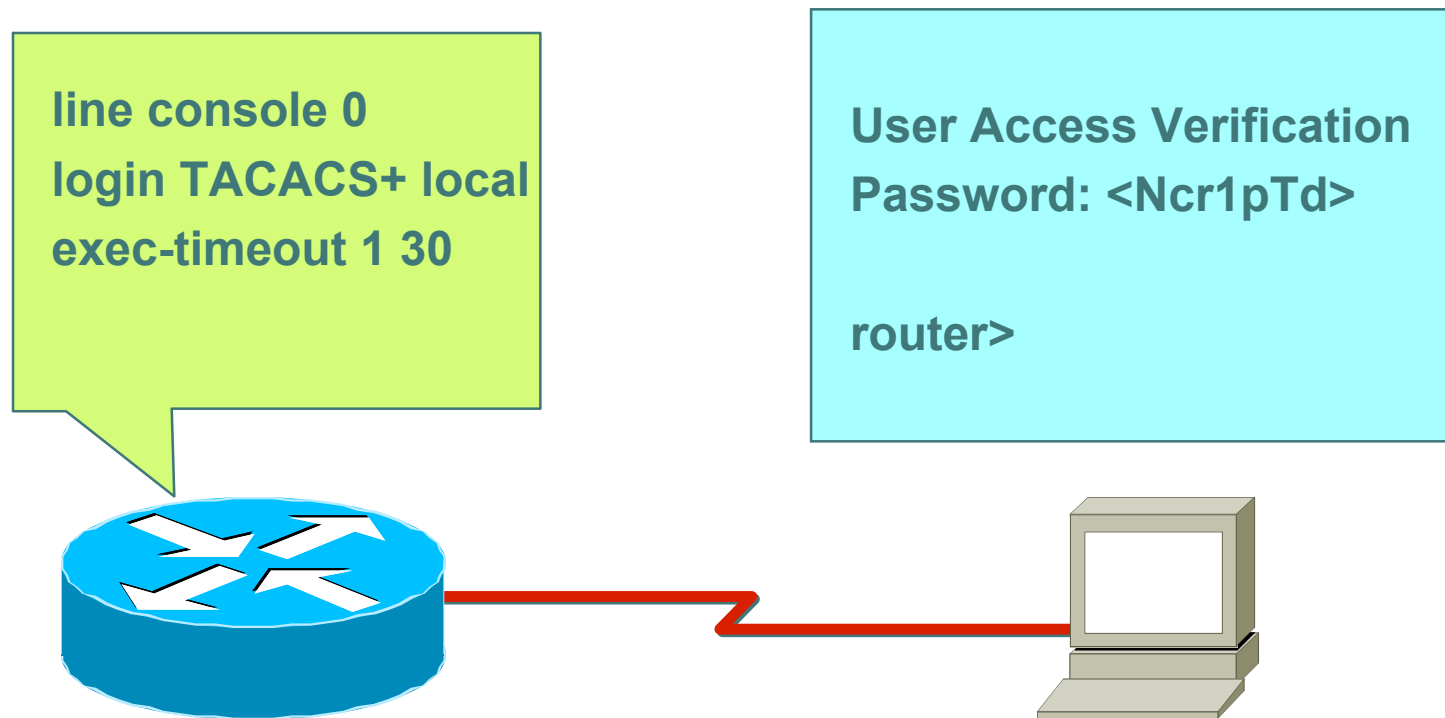
# Secure Access to Routers with Passwords and Timeouts



The native passwords can be viewed by anyone logging in with the enabled password

**NOT SECURE !**

# Secure Access to Routers with Passwords and Timeouts



The native passwords can be **MORE SECURE !**  
logging in with the enabled password



# Never Leave Passwords in Clear-Text

- ***password*** command
  - Will encrypt all passwords on the Cisco IOS with Cisco-defined encryption type “7”
  - Use “*command password 7 <password>*” for cut/paste operations
  - Cisco proprietary encryption method
- ***secret*** command
  - Uses MD5 to produce a one-way hash
  - Cannot be decrypted
  - Use “*command secret 5 <password>*” to cut/paste another “enable secret” password



# Authenticate Individual Users

```
service password-encryption
enable secret 5 $1$mgfc$ISYSLeC6ookRSV7sI1vXR.
enable password 7 075F701C1E0F0C0B
!
username merike secret 5 $6$mffc$ImnGLeC67okLOMps
username staff secret 5 $6$ytjc$IchdLeC6o6klmR7s
```

```
line con 0
exec -timeout 1 30
login local
!
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
```



# Restrict Access To Trusted Hosts

- Use filters to specifically permit hosts to access an infrastructure device
- Example

```
Access-list 103 permit tcp host 192.168.200.7 192.168.1.0 0.0.0.255  
eq 22 log-input
```

```
Access-list 103 permit tcp host 192.168.200.8 192.168.1.0 0.0.0.255  
eq 22 log-input
```

```
Access-list 103 permit tcp host 192.168.100.6 192.168.1.0 0.0.0.255  
eq 23 log-input
```

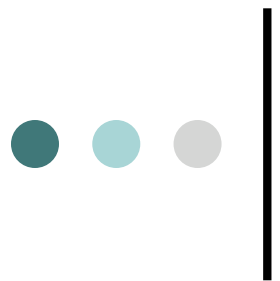
```
Access-list 103 deny ip any any log-input
```

```
!
```

```
Line vty 0 4
```

```
Access-class 103 in
```

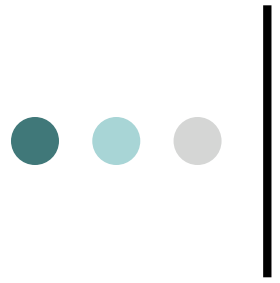
```
Transport input ssh telnet
```



# Telnet is Insecure

- Avoid using Telnet if possible
- Telnet sends username and password information across the wire in plain text format.
- Do not use telnet to gain access to any of your boxes (router-to-router could be exception for troubleshooting, but limit access in these instances)





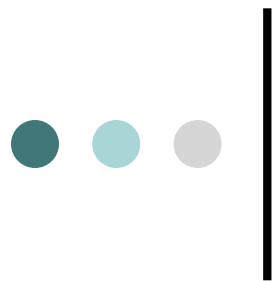
# Secure Shell (SSH)

- Username/password information is encrypted
- Flexible authentication methods
  - One-time password
  - Kerberos
  - Public key
- Allows Secure Tunneling
  - TCP port forwarding
  - Forward remote ports to local ones
- Uses TCP port 22



# SSH Support

- Two flavors of ssh, ssh1 and ssh2
- Use ssh2 if possible
- In general the client connecting to your ssh server will either "speak" ssh1 or ssh2
- OpenSSH for UNIX
  - [www.openssh.org](http://www.openssh.org)
  - Supports both ssh1 and ssh2
- Putty client for Windows
  - [www.chiark.greenend.org.uk/~sgtatham/putty/](http://www.chiark.greenend.org.uk/~sgtatham/putty/)



# Secure SNMP Access

- SNMP is primary source of intelligence on a target network!
- Block SNMP from the outside
  - access-list 101 deny udp any any eq snmp
- If the router has SNMP, protect it!
  - snmp-server community fO0bAr RO 1
  - access-list 1 permit 127.1.3.5
- Explicitly direct SNMP traffic to an authorized management station.
  - snmp-server host fO0bAr 127.1.3.5



# Secure Logging Infrastructure

- Log enough information to be useful but not overwhelming.
- Create backup plan for keeping track of logging information should the syslog server be unavailable
- Remove private information from logs
- How accurate are your timestamps?

# Timestamp Issues

```
unix% tail cisco.log
```

```
Feb 18 21:48:26 [10.1.1.101.9.132] 31: *Mar  2 11:51:55 CST:  
  %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.1.2)
```

```
unix% date
```

```
Tue Feb 18 21:49:53 CST 2005
```

```
unix%
```

```
version 12.2
```

```
service timestamps log datetime localtime show-timezone
```

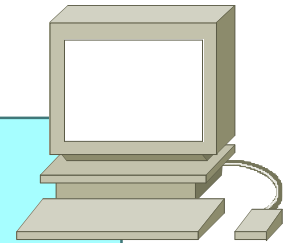
```
!
```

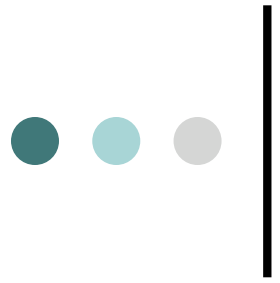
```
logging 10.1.1.2
```

```
Router>sho clock
```

```
*11:53:44.764 CST Tue Mar 2 1993
```

```
Router>
```





# Banner....what's wrong?

banner login ^C  
Martini

2.5 ounces vodka  
1/5 ounce dry vermouth

Fill mixing glass with ice, add vermouth and vodka, and stir to chill. Strain into a Martini glass and garnish with an olive or lemon twist.

RELAX....INDULGE.....Get Off My Router!!  
^C

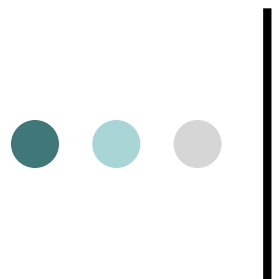


# Better Device Banner

**!!!! WARNING !!!!**

You have accessed a restricted device.

All access is being logged and any  
unauthorized access will be prosecuted  
to the full extent of the law.



# System Image and Configuration File Security

- Careful of sending configurations where people can snoop the wire
  - CRC or MD5 validation
  - Sanitize configuration files
- SCP should be used to copy files
  - TFTP and FTP should be avoided
- Use tools like 'rancid' to periodically check against modified config files





# Bare Minimum Device Security

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through ssh
- Disable device access methods that are not used
- Shut down unused interfaces
- Shut down unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners
- Test device integrity on a regular basis



- Router Device Security
- SSH on LINUX