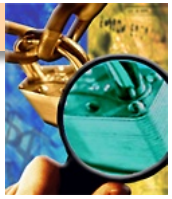
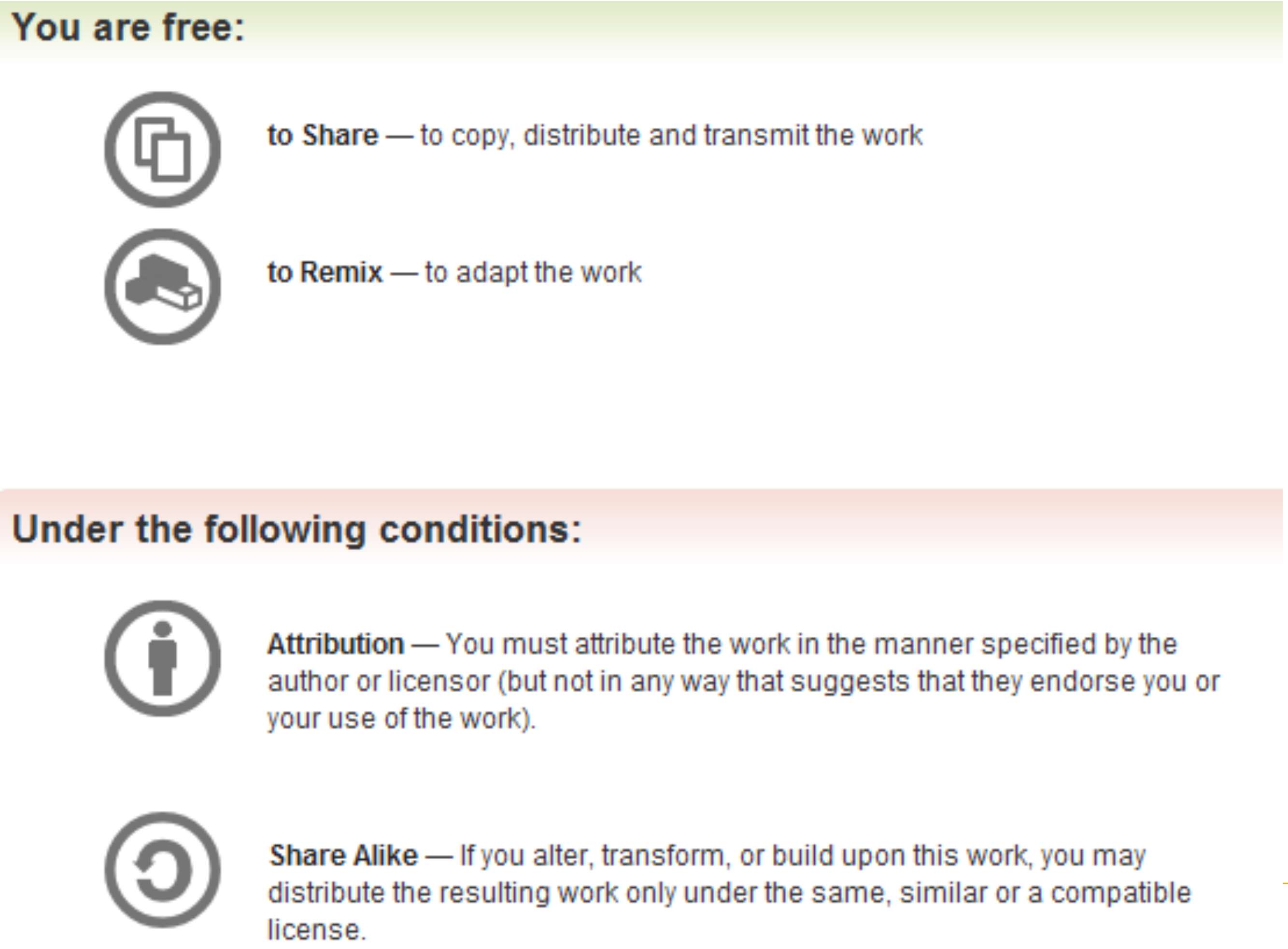
Network Security

Vulnerability Assessment Course

All materials are licensed under a Creative Commons “Share Alike” license.



- http://creativecommons.org/licenses/by-sa/3.0/



You are free:

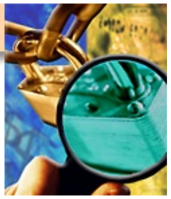
to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

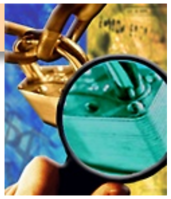
Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.



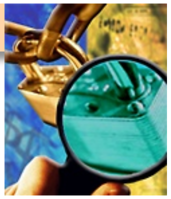
Agenda

- Why Assess
- What’s needed
- Router and Switch Security
- Firewall Security
- IDS Security
- VPN Security
- Network Services



Vulnerability Assessment

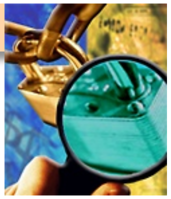
- Provides the opportunity to address weaknesses before an enemy can exploit them
- Implementation: Scanning tools that identify vulnerabilities in computer hardware, software, networks and operating systems
- Common techniques
  - Multiple tools – one tool may not identify all vulnerabilities
  - Ability to identify backdoors security perimeter, e.g., modems, VPNs, etc. – all potential vulnerabilities need to be assessed
  - Correction verification mechanism – ability to check if vulnerability has been eliminated
- Compliance with OMB, DOD, DHS policy
  - Utilize NIST 800-53 and 800-53A
  - DOD 8500 series



What’s Needed

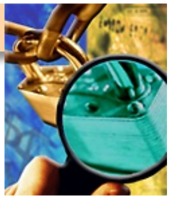
- Networking experience
  - Hands on experience: configuration, managing, building various devices
  - Working knowledge of best practices
- Security Experience
  - Intimate knowledge of how to secure a system
  - Prior experience with CIS Benchmark, DISA STIG/SRR
- Data Collection
  - Network scans from NMAP and Nessus
  - Running device configuration
- Other Skills
  - Need to work with administrators
  - Put vulnerability in their language
  - Be tedious while looking for vulnerabilities
  - Work well in a team

Router and Switch Security



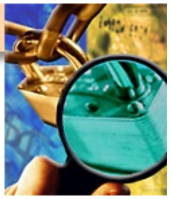
What are Routers and Switches

- Router
  - Determines the next point to forward a packet using distance and cost algorithms
  - Routes can be static or dynamic
  - A router maintains a table of routes (paths to the next hop in the network) and the conditions they are used
- Switch
  - Forwards packets to specific host by MAC address
  - Newer OS’s can route and perform other functions
  - Packets sent to single host via MAC address (unless a broadcast packet)
  - Opposite of a Hub, Individual hosts do not see everyone’s traffic



Threats

- Direct attacks
  - Could exploit vulnerabilities in the IOS
  - Pass through or direct attacks
- Denial of Services attacks
  - Alt routing and upstream provider support
  - Not much can be done to defend against a DDOS
- Compromise from poor configuration
  - Allowing telnet from external
  - Not restricting access to console ports
  - VLAN hopping via poor configuration



Manufactures

- Several vendors and different types of products for network routing and switching
  - Not all products are created equal
  - Differ in command syntax, capabilities, cost

extreme networks

Cisco Systems

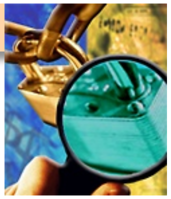
3com

Juniper NETWORKS

Lucent Technologies
Bell Labs Innovations

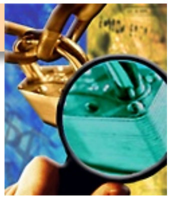
FOUNDRY NETWORKS
The Power of Performance™

NETGEAR



Router Woes

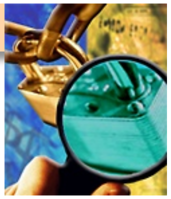
- The bad news
  - All vendors have implemented capabilities differently
  - Syntax and configurations are different
  - Management unique
- The good news
  - At the core the capabilities (forwarding packets) are the same
  - Understand the principles Ethernet and TCP/IP
  - Most vendors documentation available free online



Router Security Practices

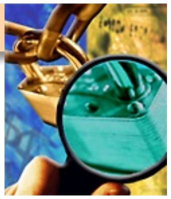
- Configuration
  - Run the most recent IOS (OS) and security patches
  - Disable unneeded services - TFTP, TELNET, HTTP
  - Disable unneeded protocols - BGP, OSPF, RIP
  - Perform EGRESS INGRESS and Anti-Spoofing
  - Encrypt routing updates with strongest algorithm available

- Management
  - Perform secure remote management with SSH or SNMPv3
  - User RADIUS or TACACS+ authentication, authorization, and auditing (AAA)
  - Manage out of band using a direct console connection



Switch Best Practices

- Configuration
  - Run the most recent IOS (OS) system and security patches
  - Disable all unnecessary services
  - Don’t implement VLAN’s across multiple security zones
  - Disable unnecessary services - HTTP, SNMP, TELNET, ROUTING
- Management
  - Perform secure remote management with SSH or SNMPv3
  - User RADIUS or TACACS+ authentication, authorization, and auditing (AAA)
  - Manage out of band using a direct console connection

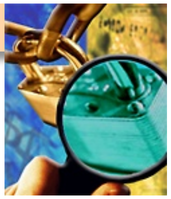


VLAN Security

- Where possible do not use VLAN’s
  - Technology has come a long way since the beginning
  - A misconfiguration or failure could allow data to traverse multiple VLAN’s

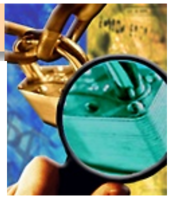
- If you must use VLAN’s ensure:
  - Different security zones do not share the same physical switch
    - Don’t mix external and internal traffic on different vlans within the same switch
  - Ensure all recommendations in CISCO VLAN security guide are followed
  - Consider use of a layer 2 firewall to add additional segmentation and detection capability

MPLS/VRF Security



- Multi Protocol Label Switching (MPLS)
  - Routing packets based on labels versus packet content
  - Layer 2.5 protocol – Can carry IP ATM SONET or Ethernet
  - Creates virtual networks

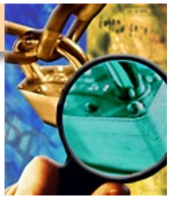
- Virtual Private Network Routing and Forwarding (VRF)
  - Acts like a virtual Router
  - Virtually segments traffic
  - Multiple routing instances coexist in one router



MPLS/VRF Security

- Validate MPLS/VRF Configurations
  - Route leaking through inter VRF Static routes
  - Misconfigurations
  - Firewall challenges

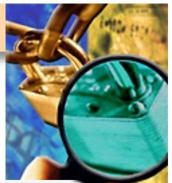
- If you must use them ensure:
  - Architecture is key
  - Do not expose internal routing information to the outside
  - Use IPSec on a hostile network
  - Routing becomes critical
  - Labels should not be set outside of the network
  - External or edge routers should not accept labeled information

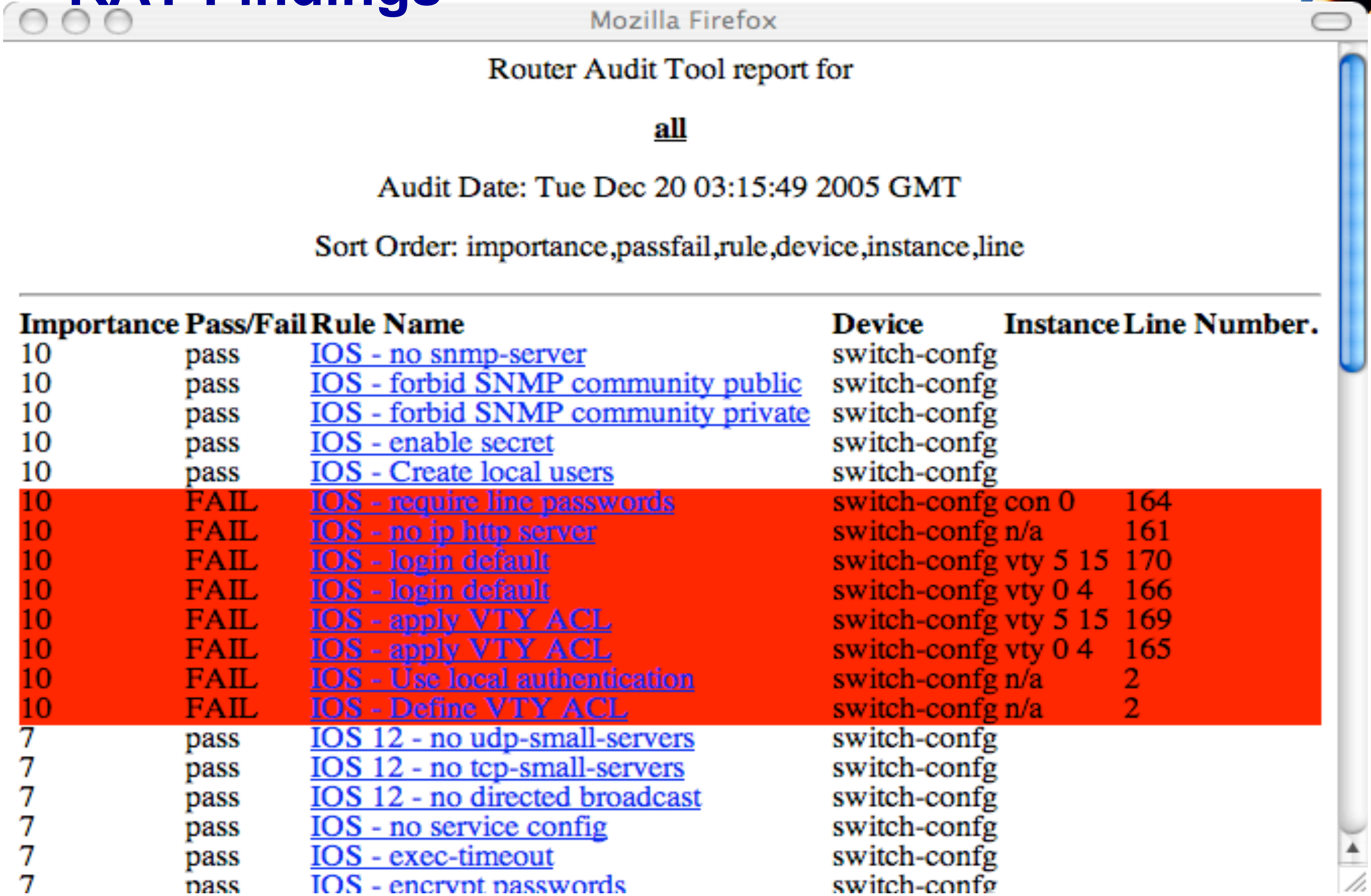


Router Audit Tool (RAT)

- A simple tool that validates the configuration of CISCO routers, switches, and PIX firewalls
  - http://www.cisecurity.org/bench_cisco.html
- Requirements
  - Windows or Unix OS
  - Complete electronic version of configuration file
  - Some CISCO knowledge
- Results
  - Provided in HTML and txt output
  - Includes false positives
  - Does not account for business policy

RAT Findings





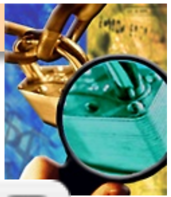
Router Audit Tool report for

all

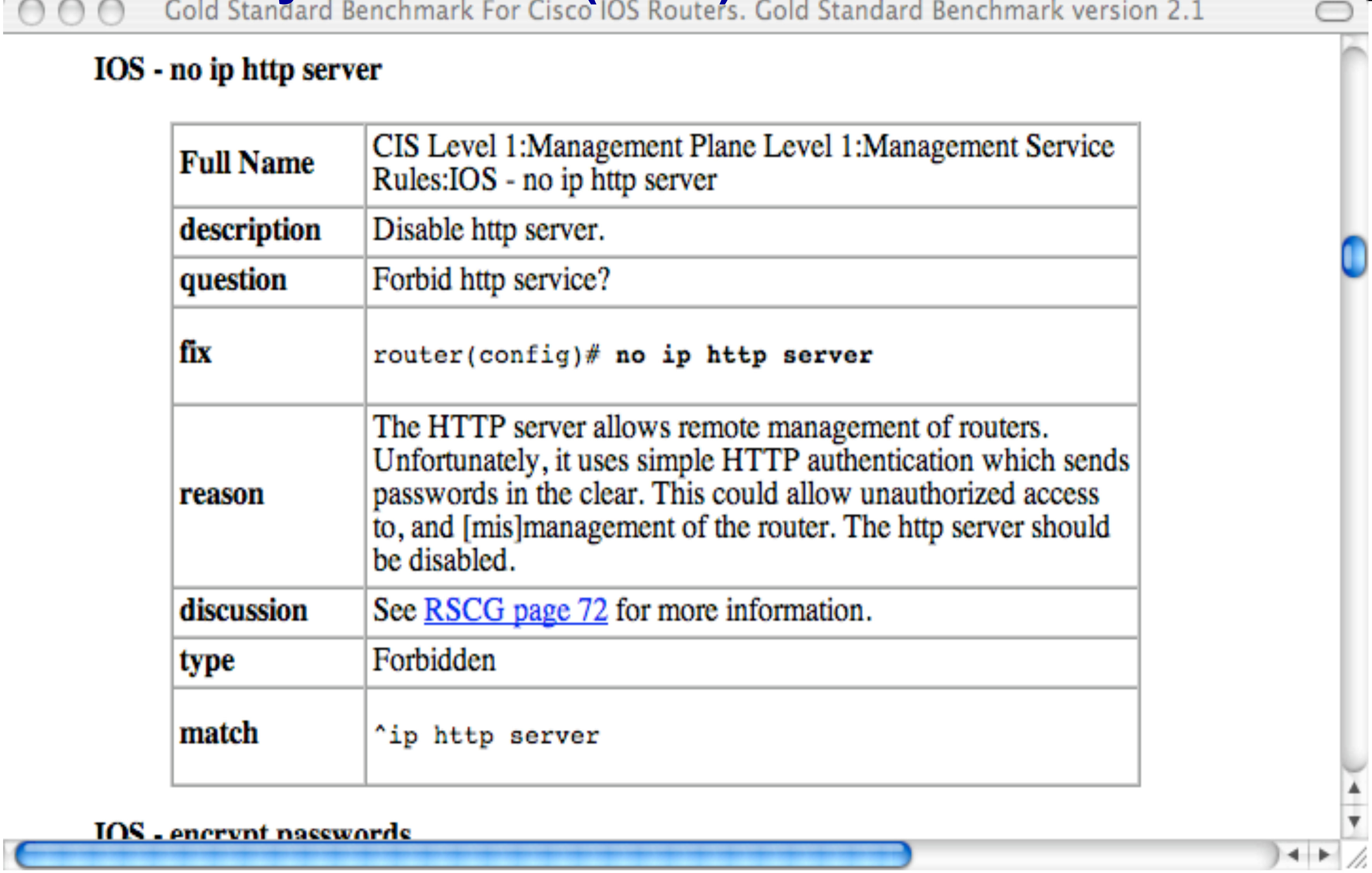
Audit Date: Tue Dec 20 03:15:49 2005 GMT

Sort Order: importance,passfail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number.
10	pass	IOS - no snmp-server	switch-confg		
10	pass	IOS - forbid SNMP community public	switch-confg		
10	pass	IOS - forbid SNMP community private	switch-confg		
10	pass	IOS - enable secret	switch-confg		
10	pass	IOS - Create local users	switch-confg		
10	FAIL	IOS - require line passwords	switch-confg	con 0	164
10	FAIL	IOS - no ip http server	switch-confg	n/a	161
10	FAIL	IOS - login default	switch-confg	vty 5 15	170
10	FAIL	IOS - login default	switch-confg	vty 0 4	166
10	FAIL	IOS - apply VTY ACL	switch-confg	vty 5 15	169
10	FAIL	IOS - apply VTY ACL	switch-confg	vty 0 4	165
10	FAIL	IOS - Use local authentication	switch-confg	n/a	2
10	FAIL	IOS - Define VTY ACL	switch-confg	n/a	2
7	pass	IOS 12 - no udp-small-servers	switch-confg		
7	pass	IOS 12 - no tcp-small-servers	switch-confg		
7	pass	IOS 12 - no directed broadcast	switch-confg		
7	pass	IOS - no service config	switch-confg		
7	pass	IOS - exec-timeout	switch-confg		
7	pass	IOS - encrypt passwords	switch-confg		



Security Baseline (RAT)

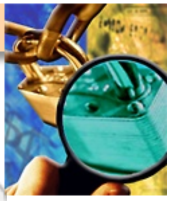


Gold Standard Benchmark For Cisco IOS Routers. Gold Standard Benchmark version 2.1

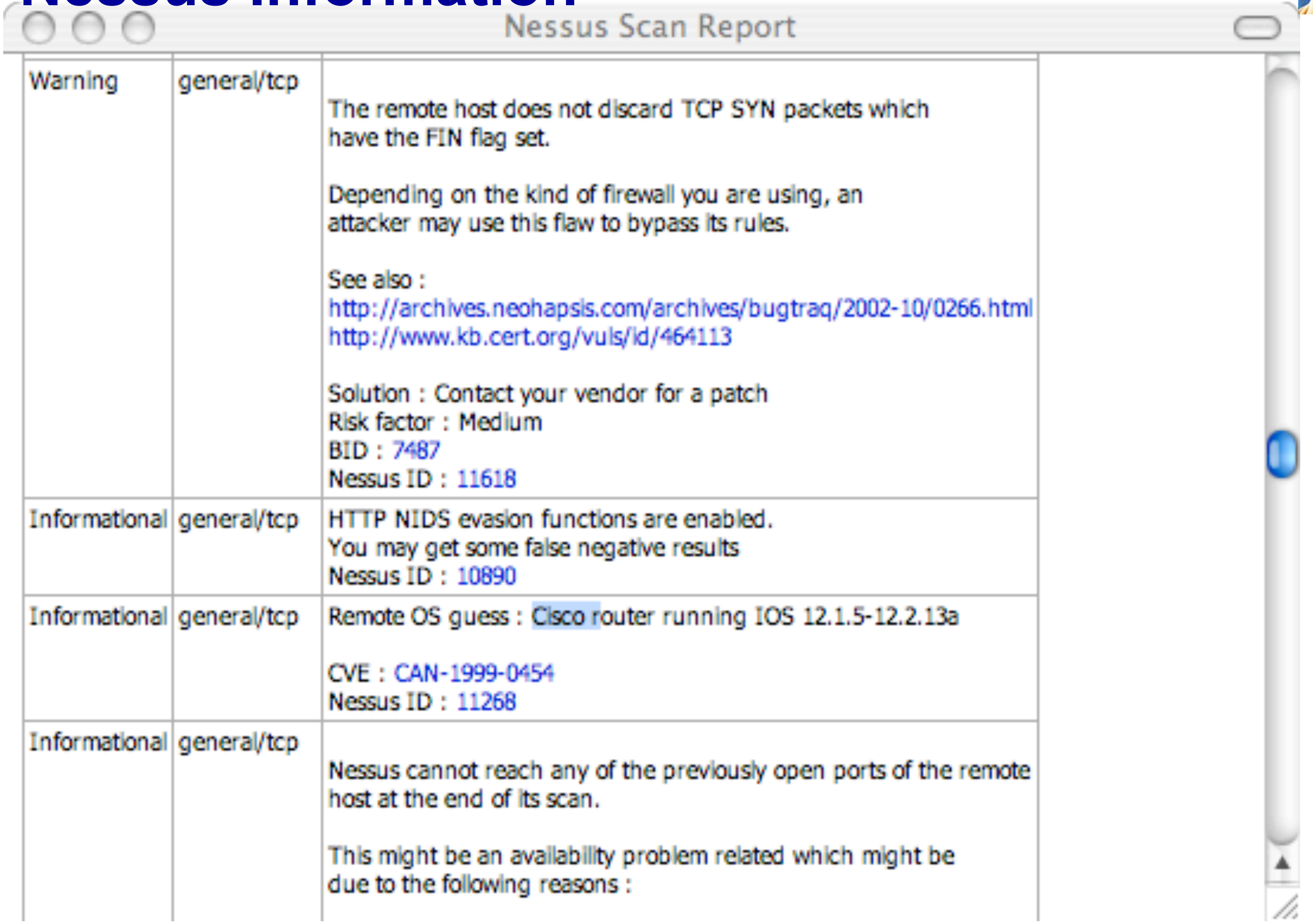
IOS - no ip http server

Full Name	CIS Level 1:Management Plane Level 1:Management Service Rules:IOS - no ip http server
description	Disable http server.
question	Forbid http service?
fix	`router(config)# no ip http server`
reason	The HTTP server allows remote management of routers. Unfortunately, it uses simple HTTP authentication which sends passwords in the clear. This could allow unauthorized access to, and [mis]management of the router. The http server should be disabled.
discussion	See RSCG page 72 for more information.
type	Forbidden
match	`^ip http server`

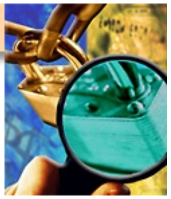
IOS - encrypt passwords



Nessus Information

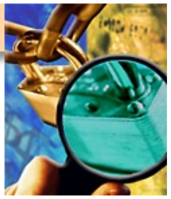


Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890
Informational	general/tcp	Remote OS guess : Cisco router running IOS 12.1.5-12.2.13a CVE : CAN-1999-0454 Nessus ID : 11268
Informational	general/tcp	Nessus cannot reach any of the previously open ports of the remote host at the end of its scan. This might be an availability problem related which might be due to the following reasons :



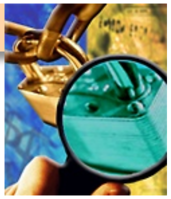
Manual Review

- While RAT does provide a quick look at a device
  - Output may report a missing setting, that exists; just not as expected
  - Does not account for things that are excepted - SNMP use
  - Unique settings, ACL’s or business decisions
- Review the configuration for:
  - Inconsistencies with RAT or Nessus output
  - Authentication methods (AAA, local)
  - Review ACLs
  - Determine how the device is administered
    - How is the administrator authenticated, what commands are they allowed to run
  - Ensure strong md5 passwords are used
  - Check for VLAN implementation (see VLAN security guidance)



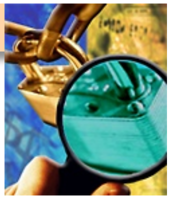
Common Findings

- Poor ACL’s
  - Allow entire subnets or large ranges of unneeded ports is a security risk
  - Depending on the source and destination IP address this could be a high finding
  - Best practice is to have a permit by exception rule base with specific IP to IP and port to port rules
- Lack of Auditing
  - Logging should be done for outbound and inbound network communications
  - This is a Low finding depending on the quality of the ACL’s in place on the device
  - Reviewing firewall log data on a daily basis can aid in detecting malicious external attacks, or potential compromises of internal machines



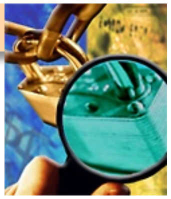
Common Findings

- Poor Configuration
  - The device itself must be securely configured and managed
  - This could be a high finding depending on the severity of the vulnerabilities or configuration errors on the firewall
  - This system should be one of the most secure on the network. It should be well maintained, securely managed, from a secure platform. Unneeded and insecure services should be disabled
    - All passwords on the device must be stored encrypted
    - All routing updates must be encrypted
    - All management traffic must be encrypted
  - Limit access to the device, especially enable mode
  - For administrators, authenticate administrators with TACACS+ and consider using two-factor logins and single-use passwords with SecureID



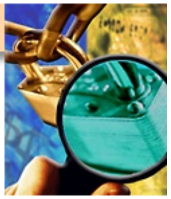
Conclusion

- Each vendor is unique, however the basic principals are still the same
- Routers should be used for only one thing – ROUTING
- Additional functions such as network ACL’s, DHCP, and TFTP should not be done on a router
- Ensure that the device does implement ACL’s to protect itself from attack and unauthorized management
- Be prepared and knowledgeable on specific device configuration and issues.
- Visit the vendor’s web site for security patches (try to test before deploying).



Exercise

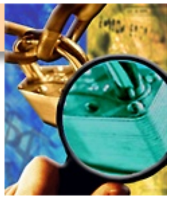
- Review scan of available device and discuss findings
- What services are running?
- What does he actual configuration look like?
- What are the vulnerabilities?



References

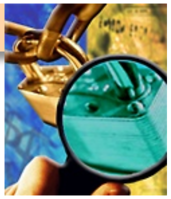
- http://www.cisecurity.org/bench_cisco.html
- NSA Router Security Guidance Activity
- Cisco IOS Security Configuration Guide, Release 12.4
- **http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a85c5.shtml**
- **http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html#wp1018833**

Firewall Security



What is a Firewall

- Software or Hardware
  - Limits network access between one or more networks
  - Provides separation between trusted/untrusted/DMZ
  - Could reside at a network or host level
- Firewalls are one layer of security - They do NOT
  - Typically do not ensure confidentiality, integrity or non repudiation
  - Protect from an insider threat
  - Function as a silver bullet
- Threatened by
  - Direct attacks (unlikely)
  - Denial of Services attacks
  - Information leakage via poor configuration



Vendors

- Several vendors and different types of products for network and host level “firewalls”
  - Not all products are created equal
  - IP Filter, IP Tables

Cisco Systems

Check Point® SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

KERIO

Lucent Technologies Bell Labs Innovations

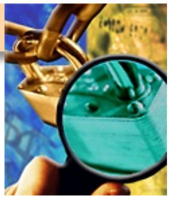
ZONE LABS

NETSCREEN

SIDEWINDER G2 SECURITY APPLIANCE

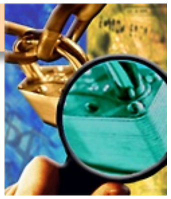
NETGEAR®

Reactivity



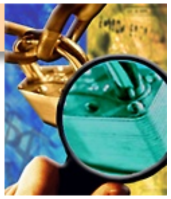
Types of Firewalls

- Packet Filter (Non stateful connections)
  - Similar to router Access Control Lists (ACLs)
  - Requires two rules to make a unidirectional connect work
    - One for the port 80 outbound
    - One for the return traffic to port 80 from a high port
- Stateful packet inspection
  - Determining what connections to allow or deny based off of the packet state.
  - Only one rule is needed to allow a unidirectional session like HTTP
- Application Layer Proxies
  - These are a newer breed of firewalls and perform more detailed packet inspection
  - Validation of protocol standards
  - Actual content inspection



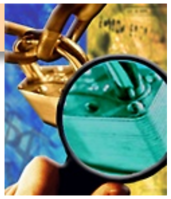
Packet Filter Firewalls

- Also called packet filters
- Usually stateless
- Function by directing packets based on source/destination IP addresses and/or ports
- Fairly cheap to deploy
- Fast and scalable
- Administrator needs to have knowledge of protocols to manage effectively
- Examples: iptables, Older CISCO’s PIX, Router ACL’s



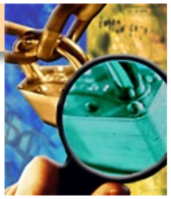
Stateful Inspection Firewalls

- Tries to bridge packet filtering and application-level filtering technologies
- Usually does not proxy connections
- Knows about expected protocol behavior
- Newest firewall model
- Expensive to deploy
- Examples: Checkpoint FW-1, NetScreen firewall, IPFilter



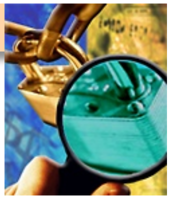
Application Layer Firewalls

- Also called proxy or protocol-based
- Most secure firewall implementation
- More processing intensive
- Not highly scalable
- More expensive to deploy
- Examples: Sidewinder firewall, Teros, Reactivity,



Firewall Woes

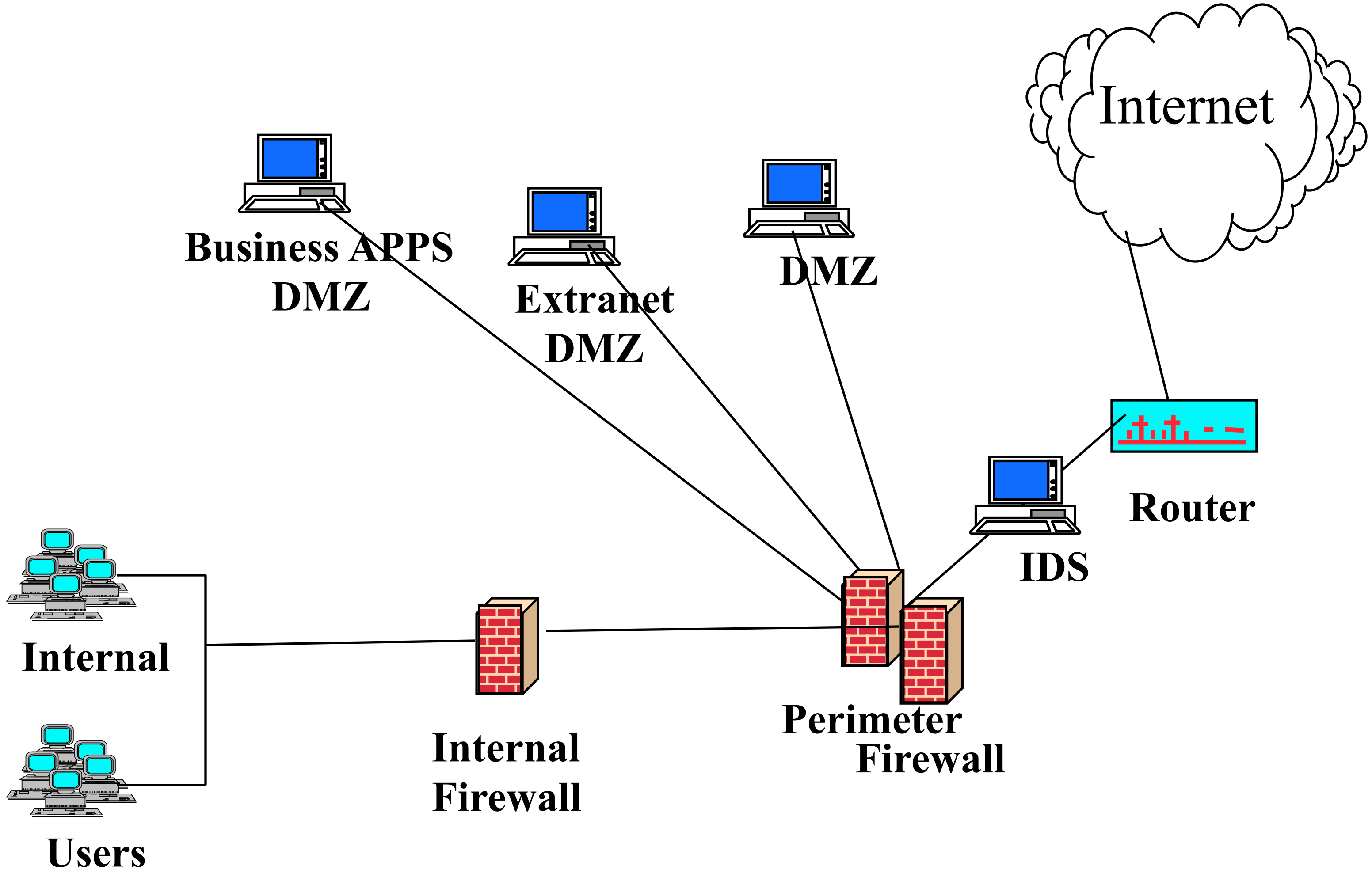
- The bad news
  - All firewall vendors have implemented these capabilities differently
  - Rule structures are different
  - Management unique
- The good news
  - At the core the capabilities (allowing and denying) are the same
  - Understand the principles of firewalls and TCP/IP
  - Most vendors documentation available free online

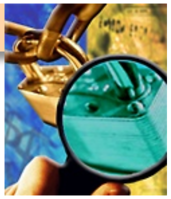


Best Security Practices

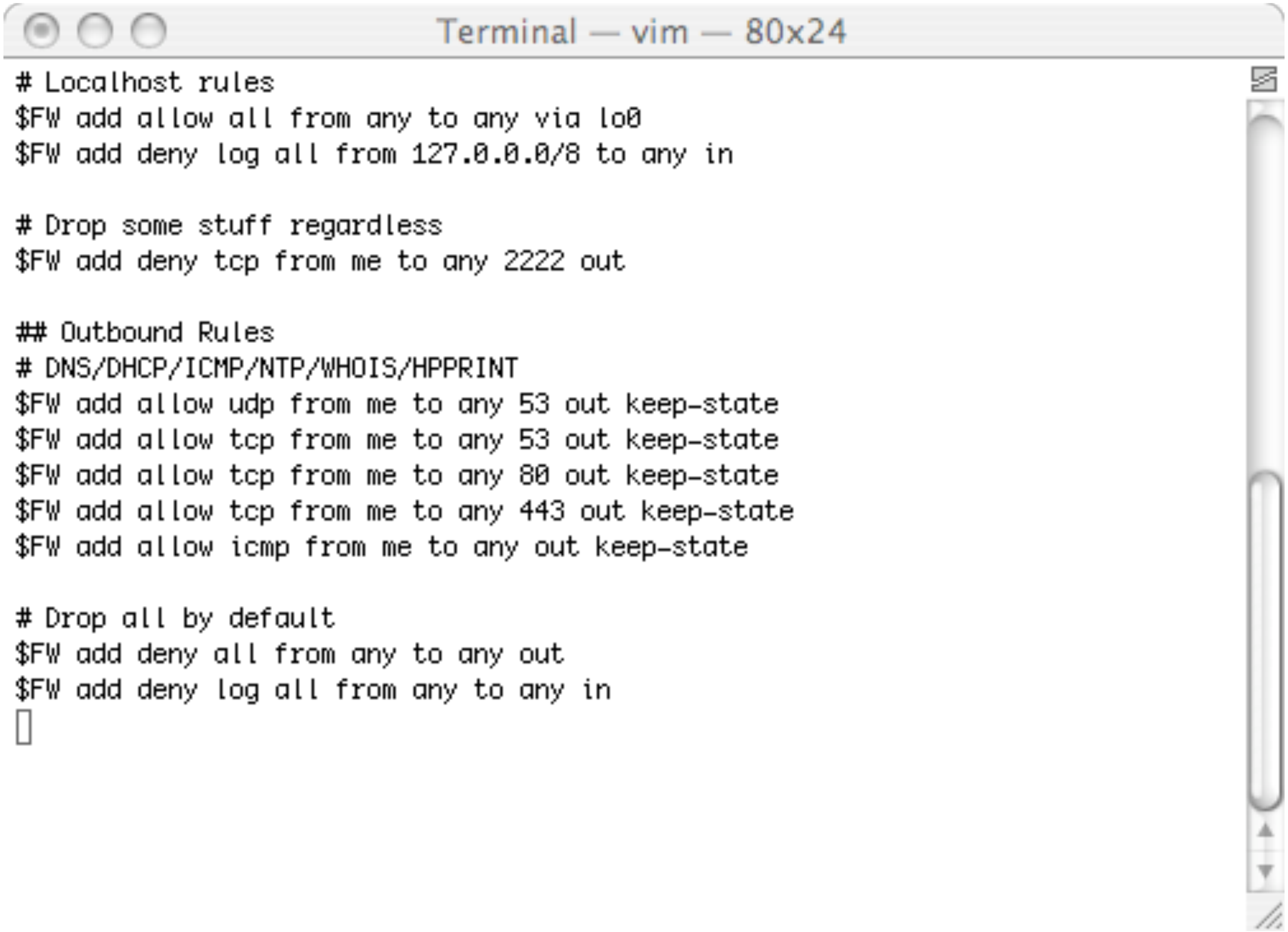
- A firewall that implements a deny-by-default or permit-by-exception rule base
  - This limits communications to what is required
  - Deny all to the firewall directly (except for management)
  - INGRESS EGRESS and Anti-spoofing rules
- Rules should be specific
  - Subnet to subnet rules are not restrictive
  - Port ranges or objects like high ports are not restrictive
  - IP to IP on a specific port or group of ports is preferred
- Management of the firewall should be done out-of-band
  - This allows for centralized logging and management to be done safe and secure isolated from production traffic

Common Architecture



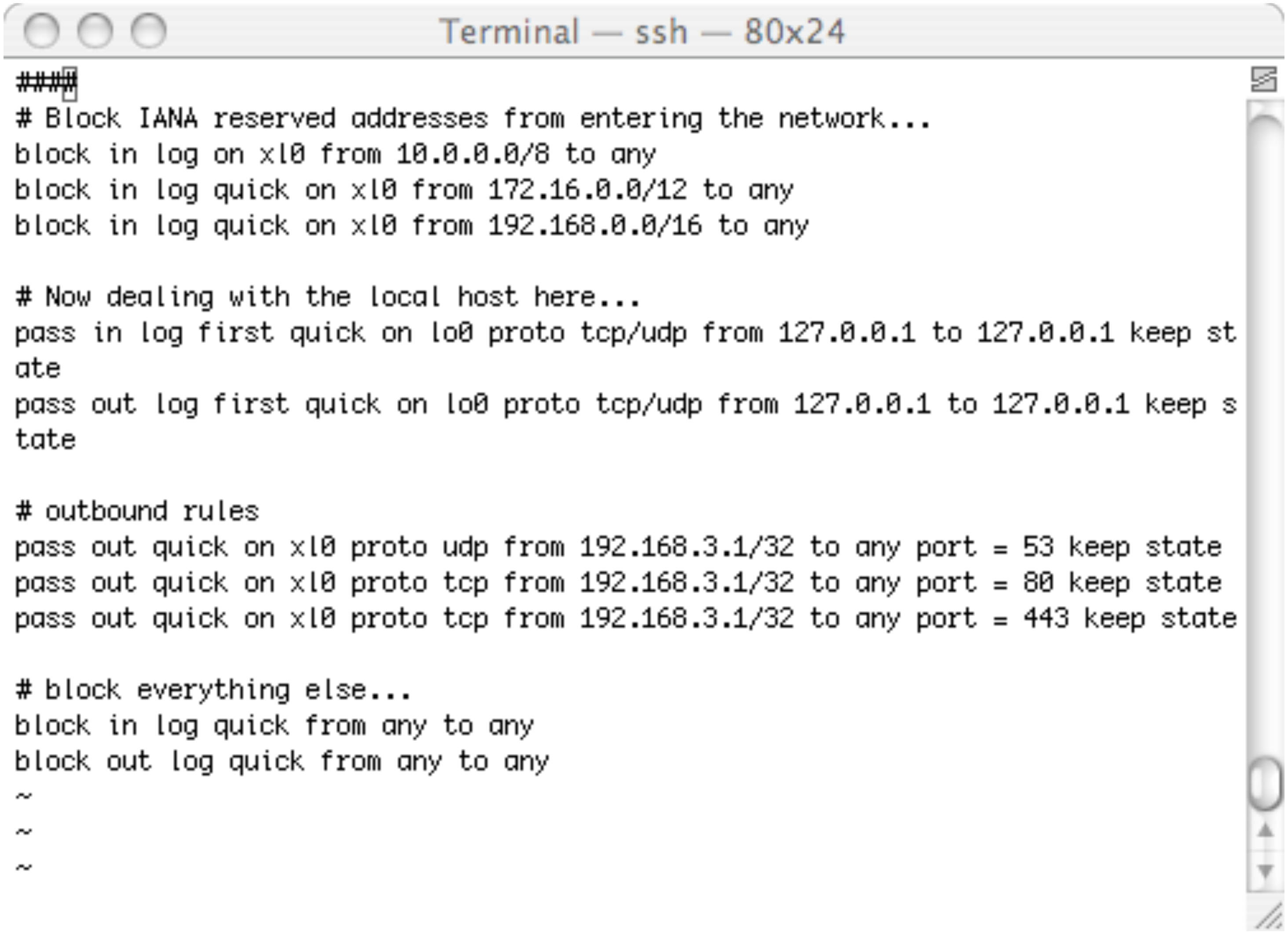


IPFW Rule Syntax



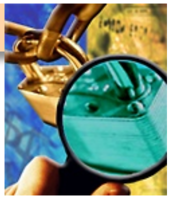
```
# Localhost rules
$FW add allow all from any to any via lo0
$FW add deny log all from 127.0.0.0/8 to any in

# Drop some stuff regardless
$FW add deny tcp from me to any 2222 out

## Outbound Rules
# DNS/DHCP/ICMP/NTP/WHOIS/HPPRINT
$FW add allow udp from me to any 53 out keep-state
$FW add allow tcp from me to any 53 out keep-state
$FW add allow tcp from me to any 80 out keep-state
$FW add allow tcp from me to any 443 out keep-state
$FW add allow icmp from me to any out keep-state

# Drop all by default
$FW add deny all from any to any out
$FW add deny log all from any to any in
```

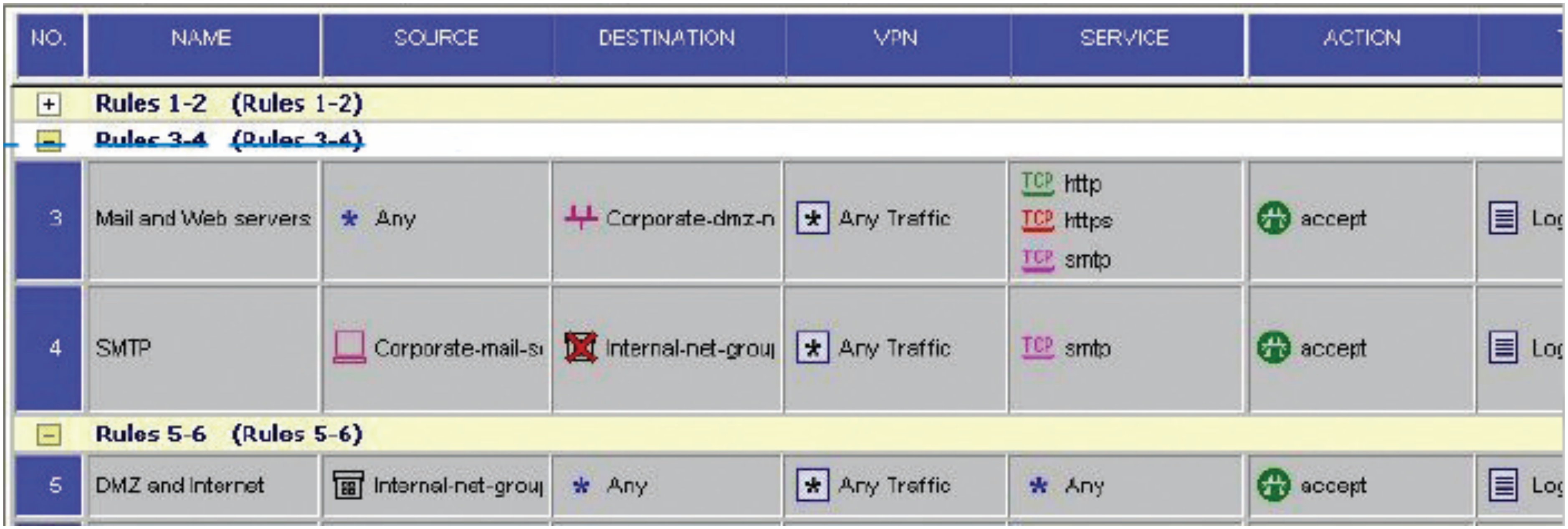
IPFilter Rule Syntax



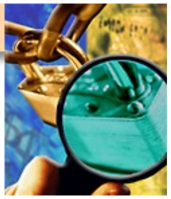
```
####
# Block IANA reserved addresses from entering the network...
block in log on xl0 from 10.0.0.0/8 to any
block in log quick on xl0 from 172.16.0.0/12 to any
block in log quick on xl0 from 192.168.0.0/16 to any

# Now dealing with the local host here...
pass in log first quick on lo0 proto tcp/udp from 127.0.0.1 to 127.0.0.1 keep st
ate
pass out log first quick on lo0 proto tcp/udp from 127.0.0.1 to 127.0.0.1 keep s
tate

# outbound rules
pass out quick on xl0 proto udp from 192.168.3.1/32 to any port = 53 keep state
pass out quick on xl0 proto tcp from 192.168.3.1/32 to any port = 80 keep state
pass out quick on xl0 proto tcp from 192.168.3.1/32 to any port = 443 keep state

# block everything else...
block in log quick from any to any
block out log quick from any to any
~
~
~
```

Checkpoint Rule Syntax



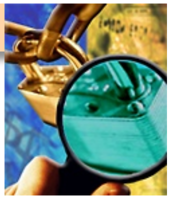


NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	
⊞	**Rules 1-2 (Rules 1-2)**						
⊟	**Rules 3-4 (Rules 3-4)**						
3	Mail and Web servers	* Any	Corporate-dmz-n	☒ Any Traffic	TCP http TCP https TCP smtp	accept	Lo
4	SMTP	Corporate-mail-s	Internal-net-grou	☒ Any Traffic	TCP smtp	accept	Lo
⊟	**Rules 5-6 (Rules 5-6)**						
5	DMZ and Internet	Internal-net-grou	* Any	☒ Any Traffic	* Any	accept	Lo



Manual Review

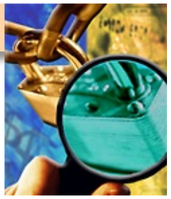
- There are no automated tools that evaluate the business case of a rule set
  - Network access may not be provided during assessment
  - There are some tools to audit the configuration of the firewall (RAT for PIX)
  - Most configurations are manually reviewed
  - Each vendor is unique in their options and syntax
  - Nmap and Nessus scans are not very valuable
- A quick look for bad stuff
  - Insecure communications
  - Any communications
  - Entire subnet communications
  - Large ranges or groups of ports
  - Duplicate entries



Manual Review

- Firewall rule base review are generally done by hand
  - It is important to have a network diagram, a list of all objects and groups and a lot of time

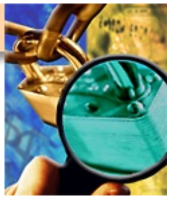
- Once the easy stuff is done
  - Begin checking from the top down
  - Looking for rules that do not make sense
  - Allow excessive access to devices
  - Bridged network segments without ACL’s
  - Ensure that the firewall is dedicated to being a firewall



Firewall Testing Tools

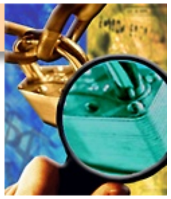
- Some tools can be used to audit a firewall if:
  - You have network access to the firewall
  - You are allowed to assess the firewall in real-time
  - You are performing a penetration test

- hping
  - http://hping.org
  - Sends custom packets to test firewall filters
    - Supports ICMP, UDP, TCP, RAW-IP
- fragroute
  - http://monkey.org/~dugsong/fragroute
  - Intercepts, modifies, and rewrites egress traffic
    - Use to test against stateful inspection firewalls



Firewall Testing Tools

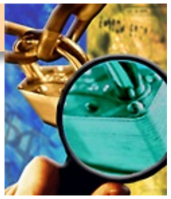
- Firewalk
  - http://packetfactory.net/firewalk
  - Tries to determine filter rules on gateway devices and map the network
  - Old tool which uses older libraries
- IRPAS (taken off line because of DE laws)
  - http://phenoelit.de/irpas
  - Internet Routing Protocol Attack Suite
  - Manipulates routes on gateway devices to bypass filters
    - Takes advantage of unauthenticated communications between routing devices
    - Protocols supported include CDP, IGRP, HSRP, RIP, OSPF



Common Findings

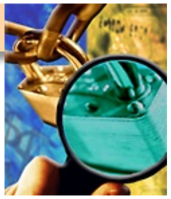
- Poor ACL’s
  - Allow entire subnets or large ranges of unneeded ports is a security risk
  - Depending on the source and destination IP address this could be a high finding
  - Best practice is to have a permit by exception rule base with specific IP to IP and port to port rules

- Lack of Auditing
  - Logging should be done for outbound and inbound network communications
  - This is a Low finding depending on the quality of the ACL’s in place on the firewall
  - Reviewing firewall log data on a daily basis can aid in detecting malicious external attacks, or potential compromises of internal machines



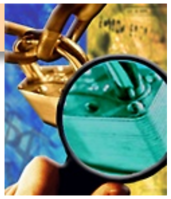
Common Findings

- Poor Configuration
  - The firewall itself must be securely configured and managed securely
  - This could be a high finding depending on the severity of the vulnerabilities or configuration errors on the firewall
  - This system should be one of the most secure on the network. It should be well maintained, securely managed, from a secure platform.



Conclusion

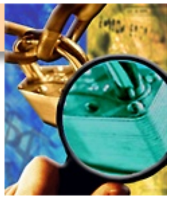
- Each vendor is unique, however the basic principles are still the same (restricting communications)
- Firewalls should be used to segment different levels of trust (internal from external, servers, from users, DMZ, from internal)
- Firewalls must be securely configured
- ACL’s or Rule base must be a permit by exception with granular access control



Firewall Exercise

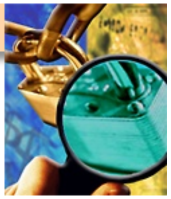
- Will demonstrate the effectiveness of firewall rules via tcpdmp and nmap

- Your Solaris 10 VM can be used
  - IPFilter is configured
  - Rulebase /etc/ipf/ipf.conf
  - Active rulebase ipfstat –hio
  - Reload rulebase ipf –Fa –f /etc/ipf/ipf.conf



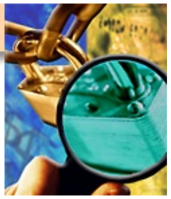
References

- http://www.faqs.org/rfcs/rfc2267.html
- http://www.sans.org/y2k/egress.htm



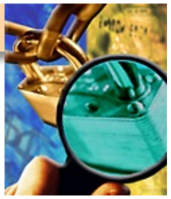
Observations

- Firewalls work well
  - The entire network security is dependent on the weakest link
  - Not all assets are behind the firewall
- Operational requirements always dictate some “holes” in the firewall security policy
- Intrusion detection must be used to monitor “holes”
  - If a VPN is used IDS cannot be done at the network perimeter
- Firewalls must be supplemented with host level scanning



Questions

Vuln-Assessment: IDS, IPS, etc.



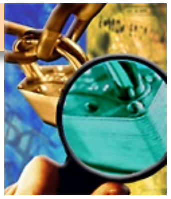
IDS – Approach and Purpose

- We’re technically on the other side of the fence here
  - Intrusion-Detection Systems are a defensive measures
  - Intrusion-Detection Systems *catch* people like us

- Advise/review IDS installations
- You will run into plenty of IDS systems in your vuln-audits

- A wide variety of intrusion-detection capabilities now exist
  - The challenge is making good use of these capabilities
  - Surprisingly difficult… our syste owners could use help here

- Your vuln-assessments should incorporate IDS systems
- Know which questions to ask, which answers are “good”



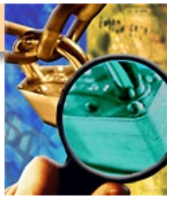
IDS – Agenda

- Refining our scope

- Alphabet Soup – NIDS, NIPS, HIDS, HIPS, SIM, SEM
- File integrity checkers, signatures, anomalies, flows… etc.

- Common IDS design/deployment patterns
  - Placement
  - Technology versus threat match

- What to examine on a VA
  - Proper use of IDS
  - Proper care and feeding of IDS

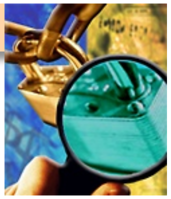


Old School IDS, In Brief

- IDS detects unwanted host/network activity in real-time
  - Host IDS (HIDS) = a software agent running on a desktop/server
  - Network IDS (NIDS) = a free-standing passive listener (“sniffer”)
  - Report to – and managed by – a central console

- Network-based IDS (NIDS)
  - Commonly deployed at perimeter or along DMZ
  - Sometimes deployed internally

- Host-based IDS (HIDS)
  - Generally used selectively (high-value targets, laptops)
  - Very handy if host-to-host communications are encrypted

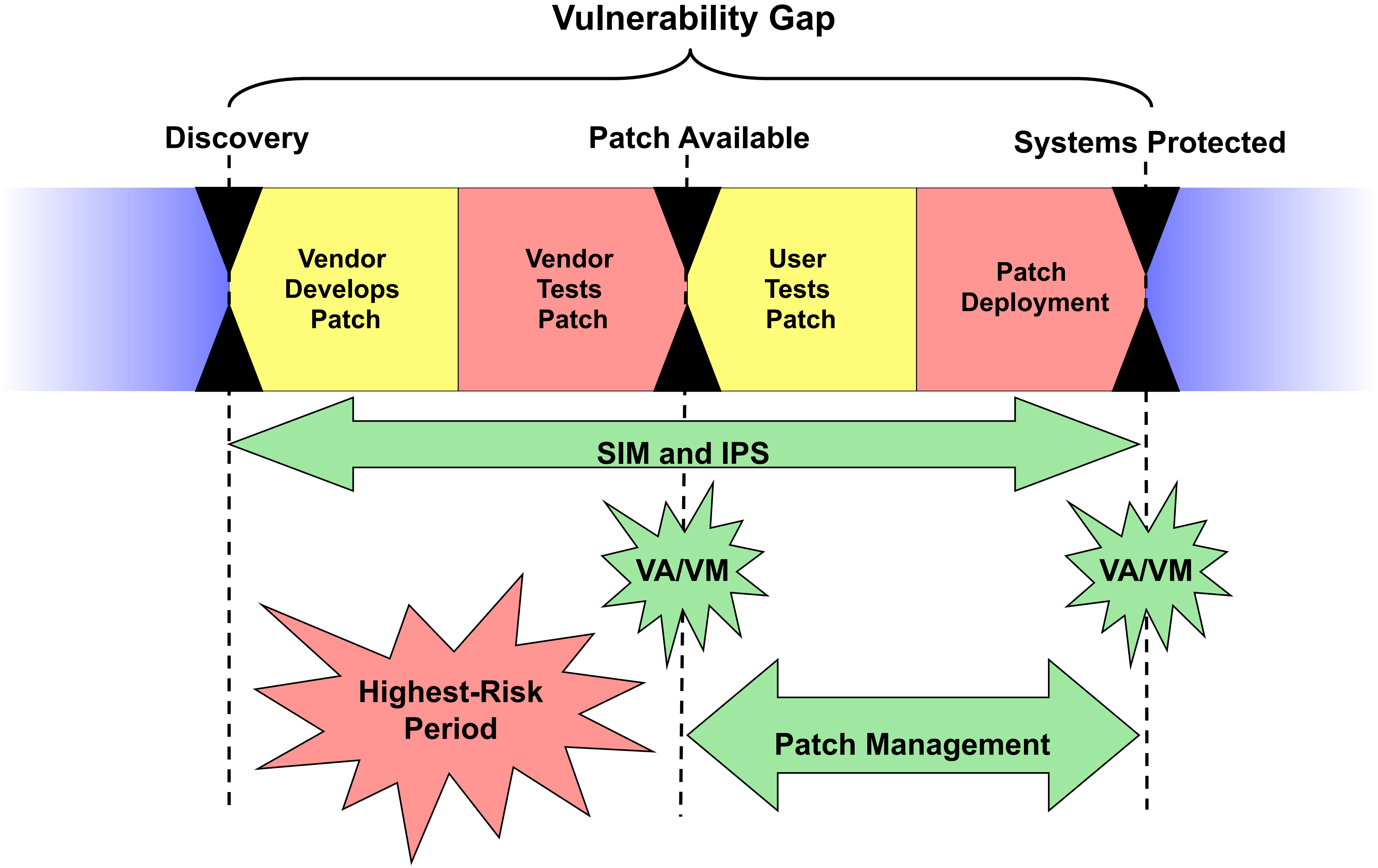


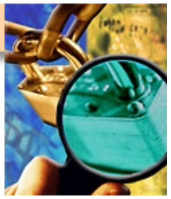
Intrusion Prevention Systems

- IPS is essentially IDS technology, on crack
  - Can fight back… drop packets or stop programs from running
  - NIPS typically run on customized hardware, inline on network
  - HIPS run close to OS kernel, insight into program, sys behavior
  - IPS is the next step in IDS technology
  - IDS has been criticized for high false-alarm rates and poor ROI
  - IPS can be even *worse*, counterattacking your own network !!!
  - Tuning the system to block ‘bad’ and allow ‘good’ is nontrivial

- IPS’s key value propositions:
  - Block “bad” traffic and/or host activity w/o human intervention
  - Provide defense against attacks during the “vulnerability gap”

Managing The Vulnerability Gap





Other IDS-type Technologies

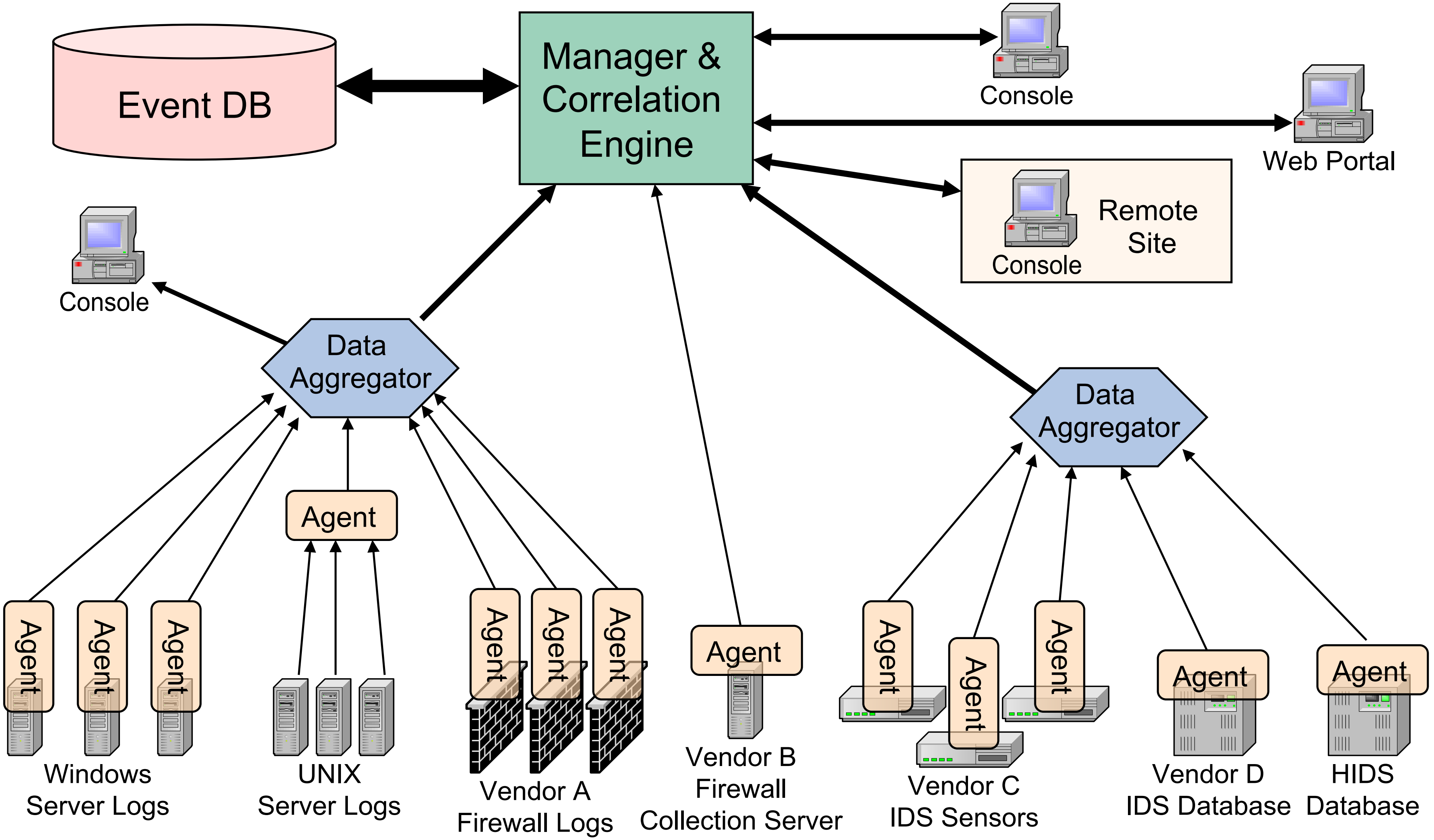
- File integrity checkers (e.g. Tripwire)
  - Monitor changes to key system configuration files

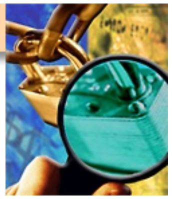
- Flow-based IDS (NetFlow)
  - Tracks network connections
  - Establishes patterns of normal traffi
  - Alert when unusual services/patterns/protocols/behaviors seen
  - Can give a good overall situational view on large network(s)

- Exotic detection capabilities
  - Augment or replace signature-based detection
  - Usually anomaly/behavior-based (pseudo-artificial intelligence)
  - Often require “training” periods to establish a baseline

- Note: IDS/IPS/SIM/NetFlow distinctions are blurring…

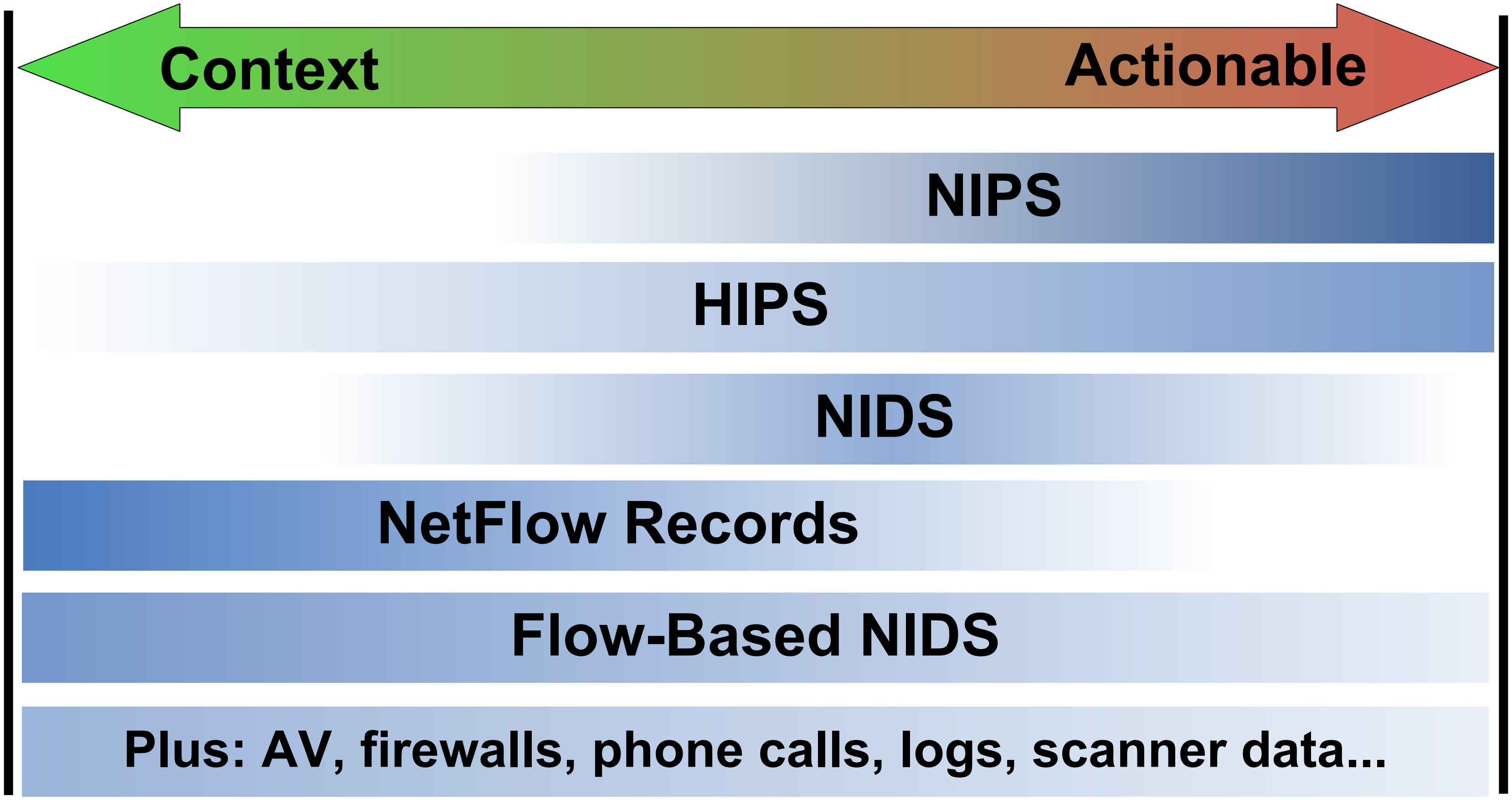
Typical SIM Architecture





Near-Realtime Intrusion Detection: Not a One-Device Job Any More…

Coherent Intrusion Detection/Response requires complete coverage:



Context

Actionable

NIPS

HIPS

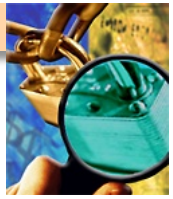
NIDS

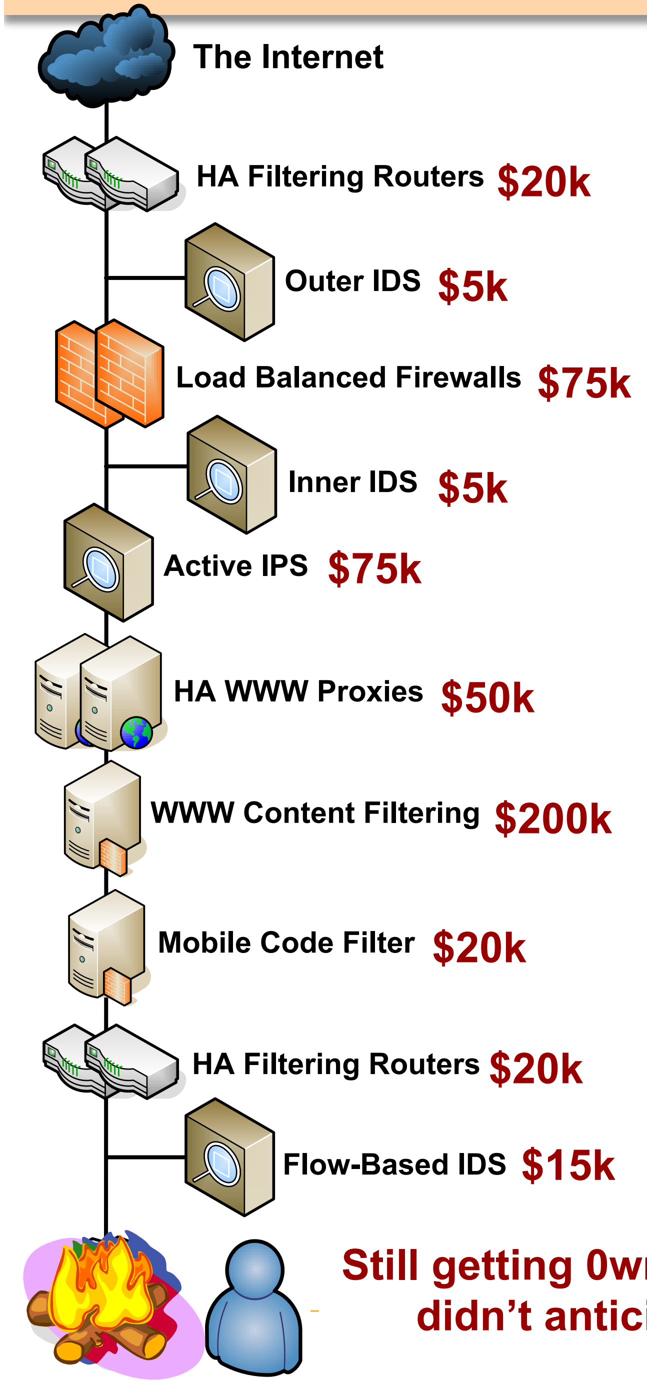
NetFlow Records

Flow-Based NIDS

Plus: AV, firewalls, phone calls, logs, scanner data...

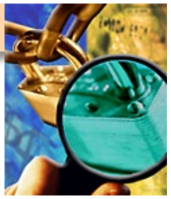
Seen This Picture Before?





- InfoSec best-practice = Defense-In-Depth
  - How many hops from user to the Internet?
- NIDS + NIPS are not the same (diff foci)
  - Ex: very different attack-views and auditing
- They are not designed to be the same
  - Can't just ignore NIPS technology
  - High capital cost, lower ops + maintenance
  - Can they afford $50k+ per NIDS appliance?
  - Can they pay that and still keep their IDS?
- Cost efficacy, not just cool technology
  - How to assemble this mis-mash?
  - Balance capital investment and O&M

Still getting 0wn3d by 7 year-old exploits because your OS vendor didn't anticipate every corner case in the RFCs… priceless.



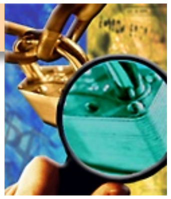
Deploying the Right IDS…

- There are a variety of IDS technologies currently available
  - You will run into them during Vas

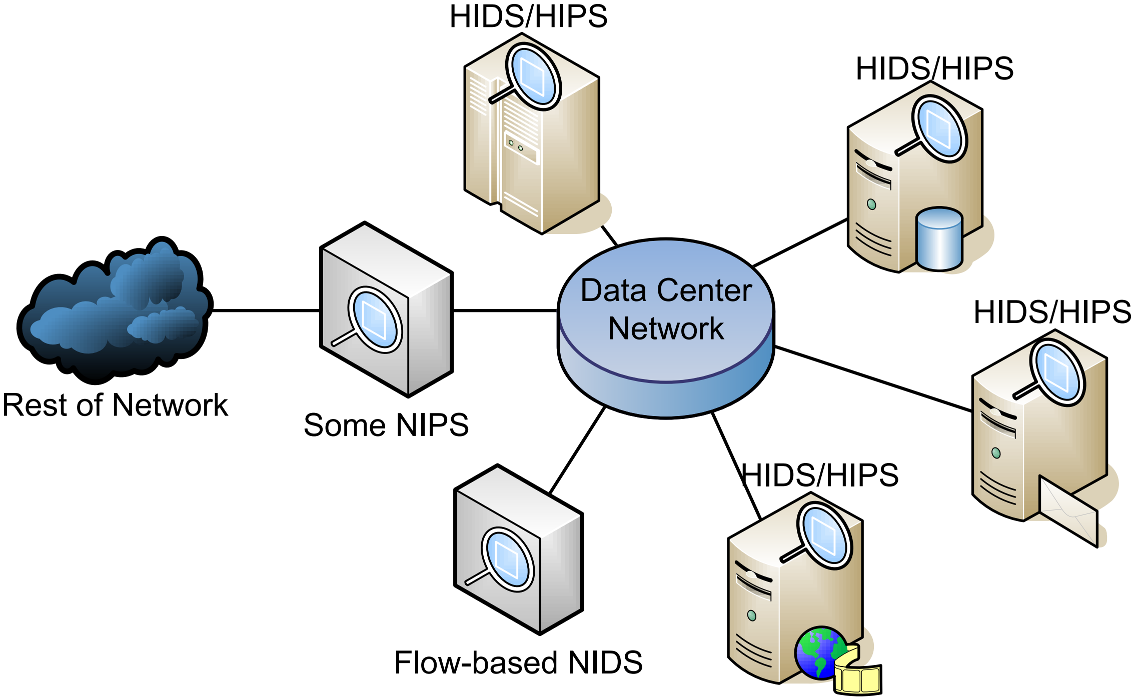
- Consider how IDS are placed, if/how they are layered, etc…
  - Correctly positioned in the architecture

    [very similar to the inside-fw vs. outside-fw vuln assessment views]
  - Appropriate choice of detection technology
  - Be careful not to recommend “IDS overkill” to your customer

- Let’s discuss a few IDS examples across the enterprise…

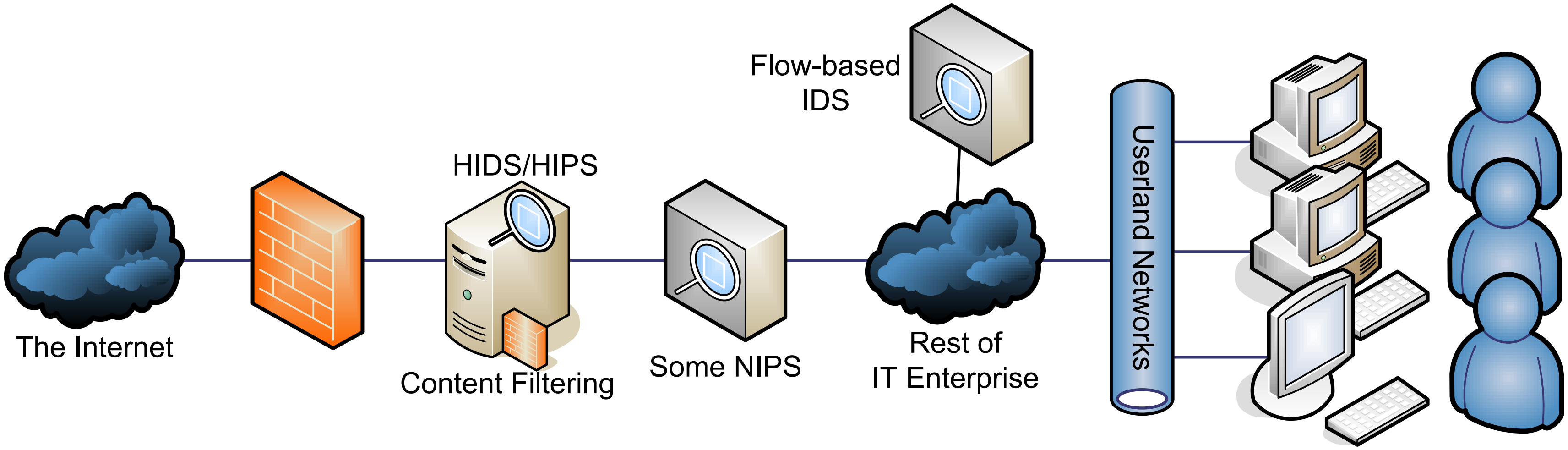


Good Uses of IDS: In The Data Center



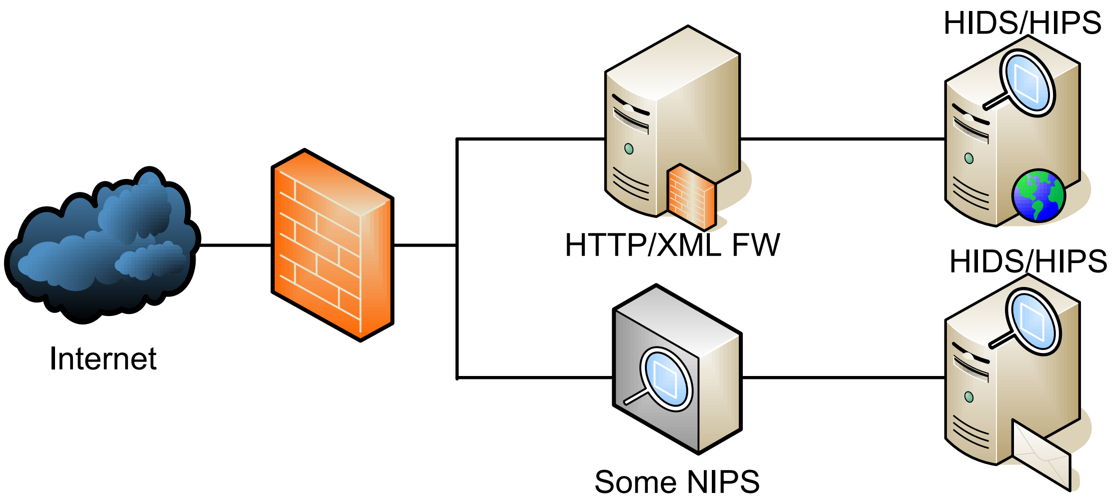
- **Use of Host-based IDS/IPS is paramount on high-val targets**
  - **Every production Windows/*NIX server should have it**
  - **Some mainframes might not support modern IDS; Tripwire or judicious system logging might be best**
- **Enclave-based NIPS is a good idea**
- **Enclave deployments of passive IDS is a bonus**

Good Uses of IDS: In Userland

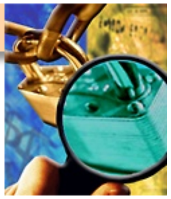


- Be careful recommending/using IDS on the desktop
  - HUGE volume of alerts, security analysts are drowning already
- Good idea to put a NIPS betw. users and the Internet
  - Keep the job of content monitoring to purpose-built devices
- Flow-based IDS at the core is a good idea
- Be cautious of all-in-one firewall + IPS + content filtering
  - Immature technology, may not scale to large enterprises
  - Putting all the eggs in one basket (if it fails or doesn’t detect…)

Good Uses of IDS: On the DMZ

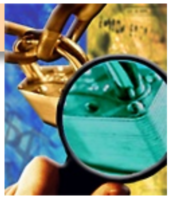


- Host-based HIDS/HIPS should be on all servers
- Use service-specific IDS/firewall products where possible
  - And NIPS where you can't



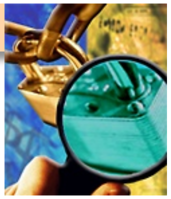
Questions

VPN Security



What is a Virtual Private Network (VPN)

- Software or Hardware
  - Provides a protected communications path
  - Could reside at a network or host level
  - SSL VPNs versus IPSec
- VPNs are one layer of security - They do NOT
  - Ensure authorization or protection from malicious logic
  - Protect from an insider threat
  - Function as a silver bullet
- Threatened by
  - Direct attacks (unlikely)
  - Denial of Services attacks
  - Information leakage via poor configuration



Vendors

- **Several vendors and different types of products for network and host level VPNs**
  - **Not all products are created equal**

Cisco Systems

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

netopia

equant

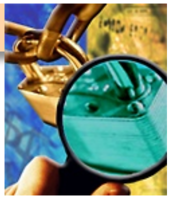
SONICWALL

Juniper
NETWORKS

NETGEAR

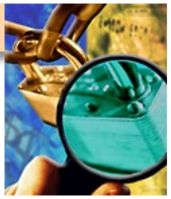
Global Crossing

NETSCREEN



Types of VPNs

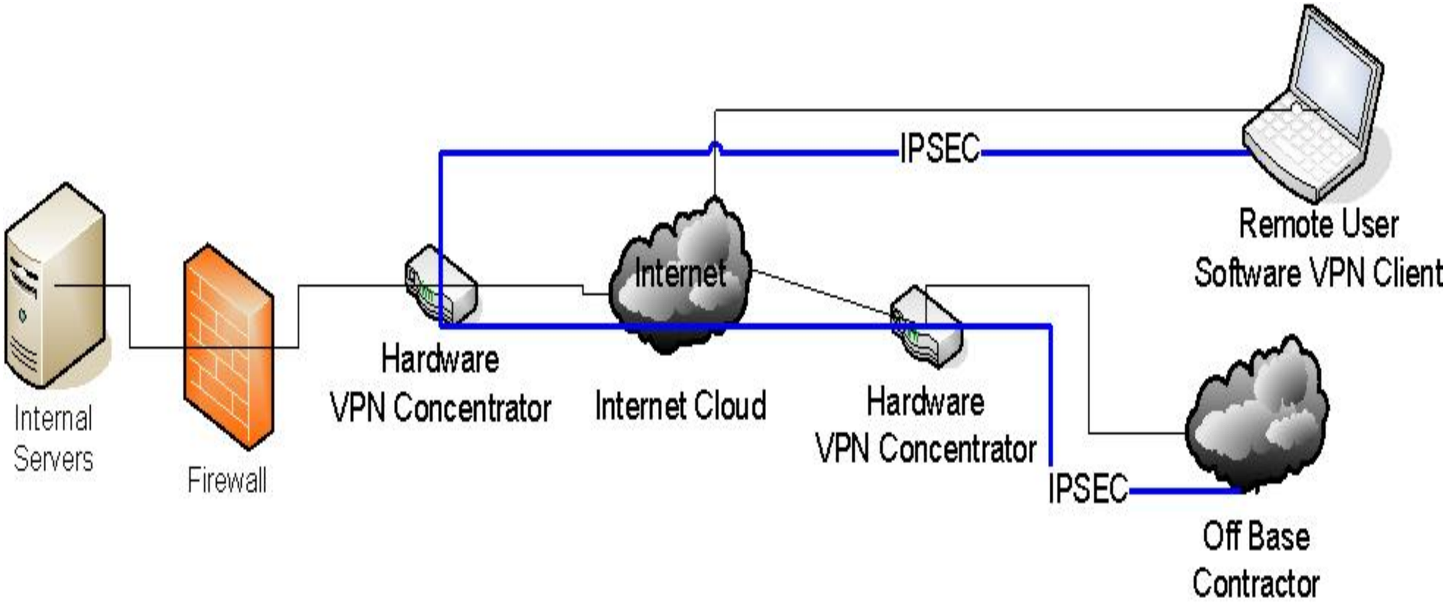
- Site to Site
  - Generally done in hardware to extend campus networks
  - Lowers security to lowest common denominator
  - Mainly for providing confidentiality
  - Network architecture critical to ensuring security
- User to Site
  - Software on local client connecting to VPN server
  - Can provide confidentiality, integrity and access control
  - Network architecture critical to ensuring security
- SSL VPNs
  - These are a newer breed of VPN and do not require client
  - Based on SSL standard
  - Wide support and capability
  - Provides confidentiality

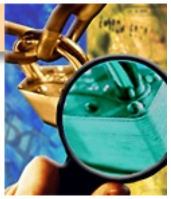


Best Security Practices

- A VPN that implements a deny-by-default or permit-by-exception rule base
  - Limits access to authorized users only!
  - Limits communications to what is required for external business
- Authentication
  - Two factor authentication
  - User groups
  - Certificates for mutual key exchange
- Architecture
  - Restricts access or terminates in a DMZ where further security inspection can be accomplished
  - Enforce Client configuration where possible (split tunneling, host based firewall rules, software versions, AntiVrius config, etc.)

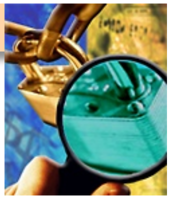
Common Architecture





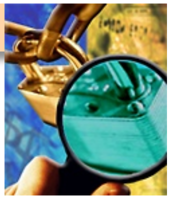
Common Findings

- Poor Configuration
  - Weak ciphers or encryption algorithms
  - Single factor authentication
  - NO client configuration enforcement
  - NO auditing
  - Improper network architecture
  - Shared VPN servers



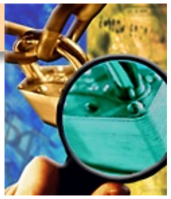
Other Topics

- Load Balancers (F5, ACE)
  - Used to load balance across multiple devices
  - Critical that they are secure
  - Equally critical how they distribute information
- Proxy servers (Websense, Squid, Webwasher)
  - Content filtering
  - Malware detection/removal
  - Signatures/polices
- All in one devices (ASA)
  - Firewall, VPN, SSL VPN, IDS
- Home Grown
  - Look out, you’ll see some crazy stuff



Common Findings

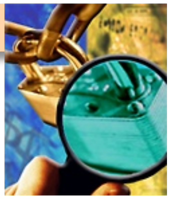
- Poor Configuration
  - Capabilities not understood
  - Logging not implemented
  - Updates not performed
  - Insecure authentication



Questions

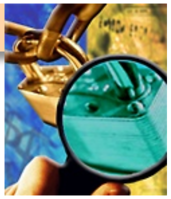
Network Services

Agenda



- What’s needed
- DNS Security
- DHCP Security
- SSH Security
- NTP Security
- Conclusion

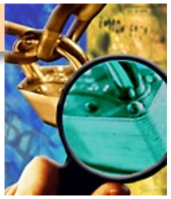
76



What’s Needed

- Networking experience
  - Hands on experience: configuration, managing, building various devices
  - Working knowledge of best practices
- Security Experience
  - Intimate knowledge of how to secure a system
  - Prior experience with CIS Benchmark, DISA STIG/SRR
- Data Collection
  - Network scans from NMAP and Nessus
  - Running device configuration
- Other Skills
  - Need to work with administrators
  - Put vulnerability in their language
  - Be tedious while looking for vulnerabilities
  - Work well in a team

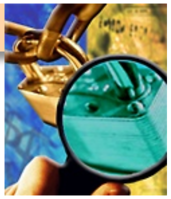
DNS Security



What is DNS

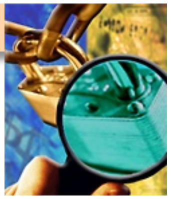
- Software that:
  - Is a hierarchal distributed database
  - Maps host names to IP addresses - forward
  - Translates IP address to names - reverse
  - Supplies mail routing information and other domain data

- Threatened by
  - Direct attacks via vulnerabilities
  - Denial of Services attacks
  - Spoofing information
  - Information leakage via poor configuration



BIND

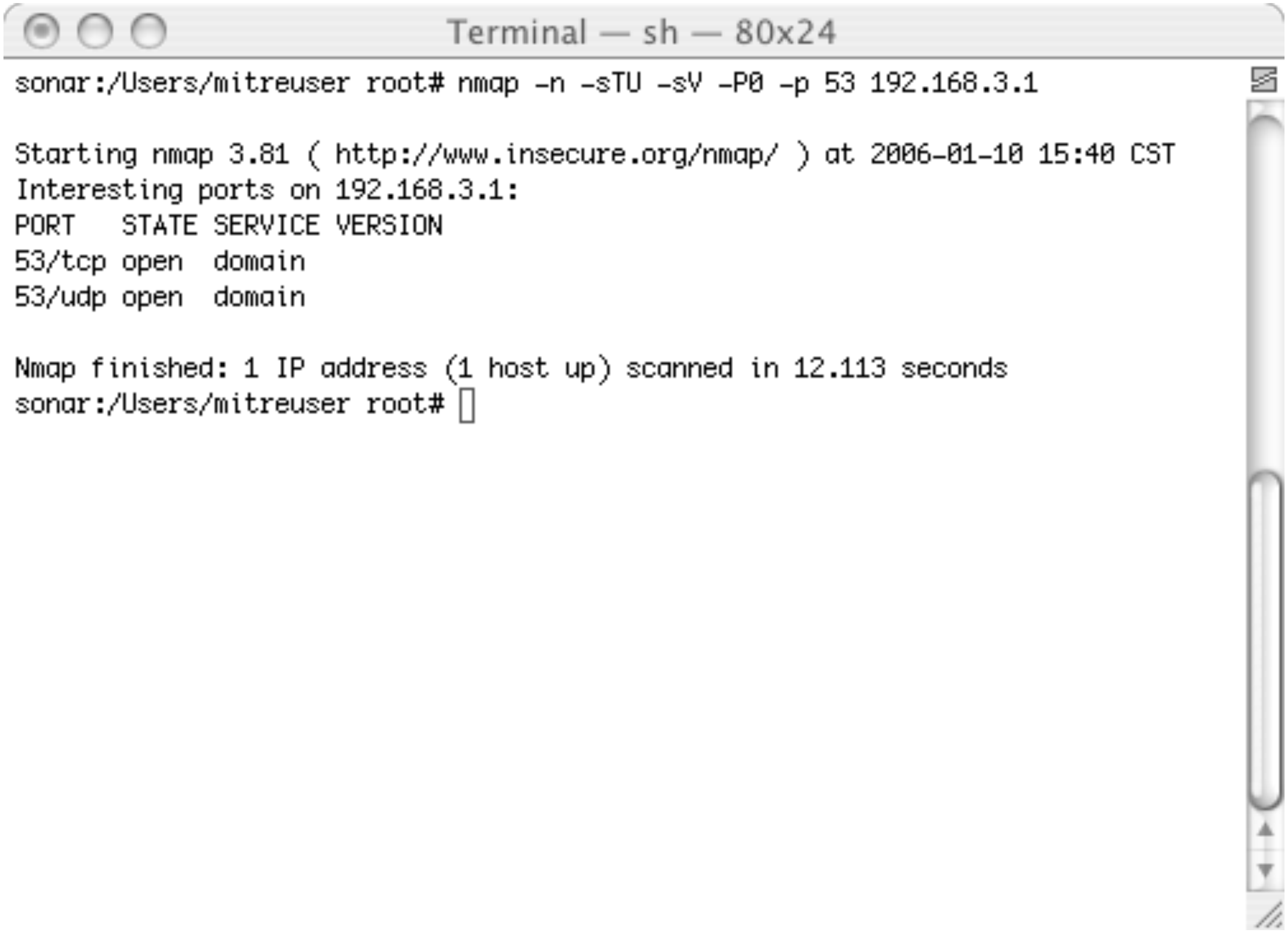
- Berkeley Internet Name Domain (BIND)
- Opensource DNS server maintained by the Internet Software Consortium (ISC)
- Current Version 9.7.3 release 02/15/2011
- Widest availability and support



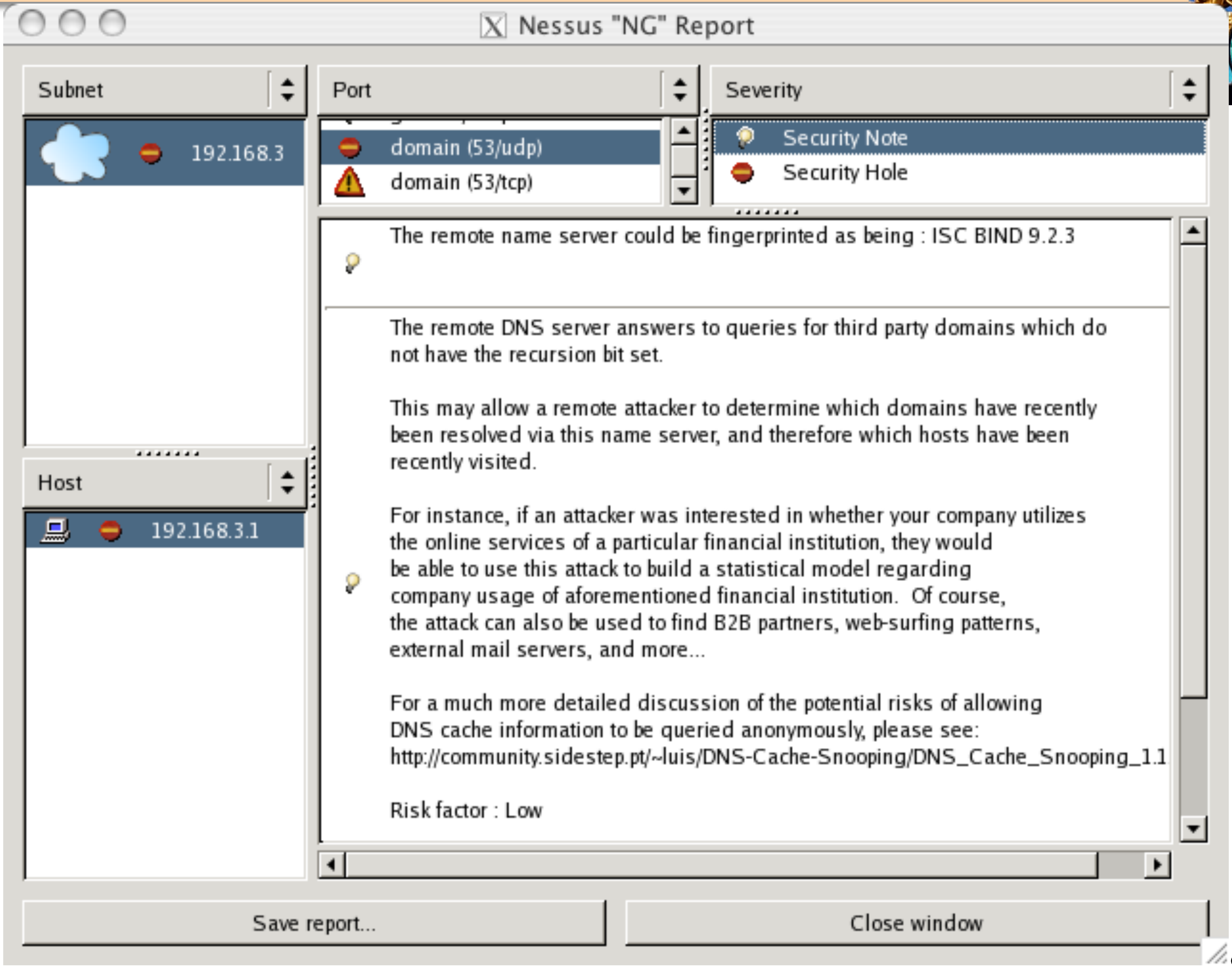
Named Config

- acl - to restrict access to the server
  - internal (192.168.1.0/24; };
  - xfer (172.16.1.53/32; };
- options - global server settings
  - version “None of your Business”;
  - listen-on { 192.168.1.53; 127.0.0.1; };
  - allow-query { internal; };
  - blackhole { };
  - allow-transfer { }; -global and per zone
  - recursion { }; - define per zone

Nmap Information



```
sonar:/Users/mitreuser root# nmap -n -sTU -sV -P0 -p 53 192.168.3.1

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-01-10 15:40 CST
Interesting ports on 192.168.3.1:
PORT   STATE SERVICE VERSION
53/tcp open  domain
53/udp open  domain

Nmap finished: 1 IP address (1 host up) scanned in 12.113 seconds
sonar:/Users/mitreuser root# 
```



The remote name server could be fingerprinted as being : ISC BIND 9.2.3

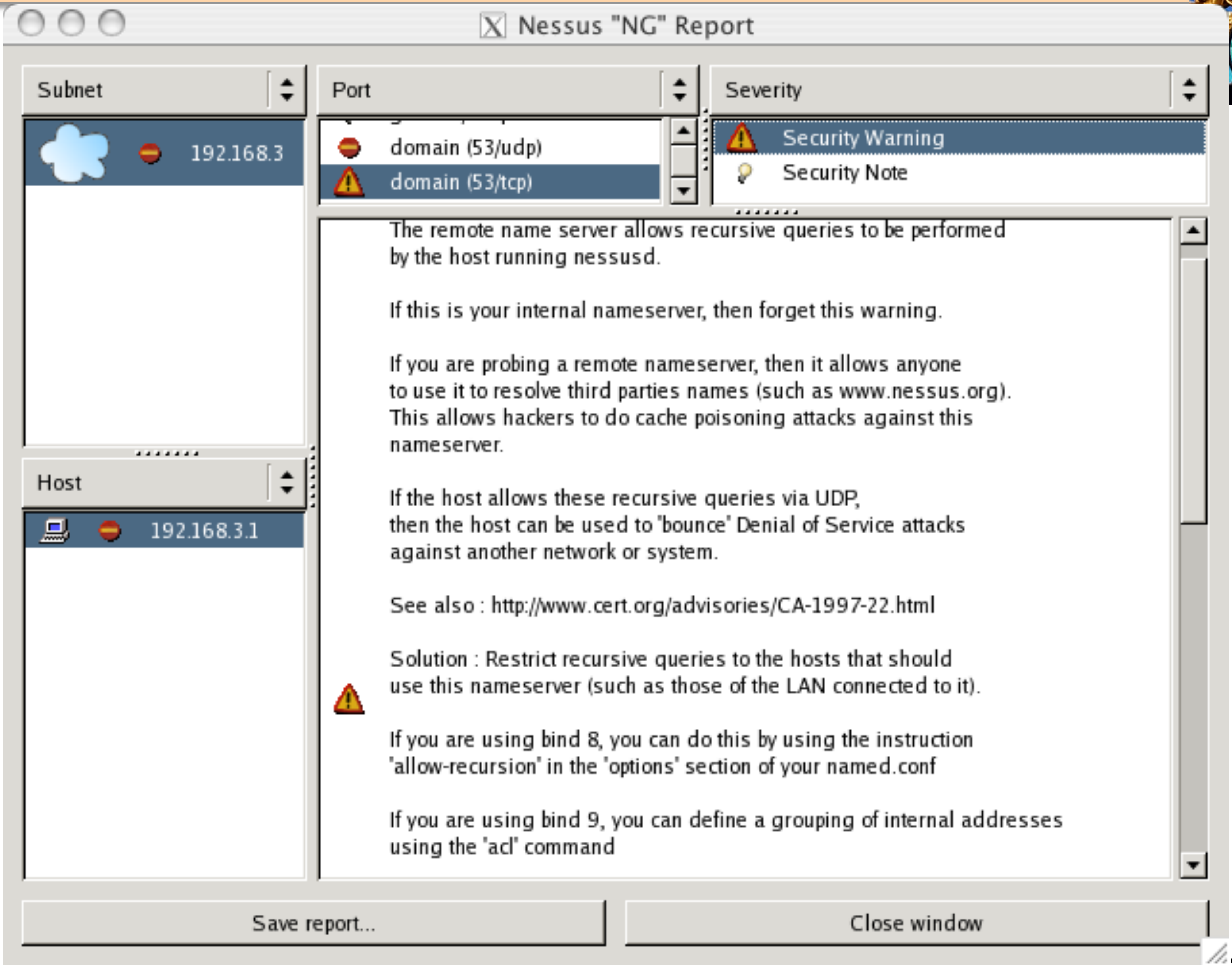
The remote DNS server answers to queries for third party domains which do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of aforementioned financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more...

For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see:
http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1

Risk factor : Low



The remote name server allows recursive queries to be performed by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

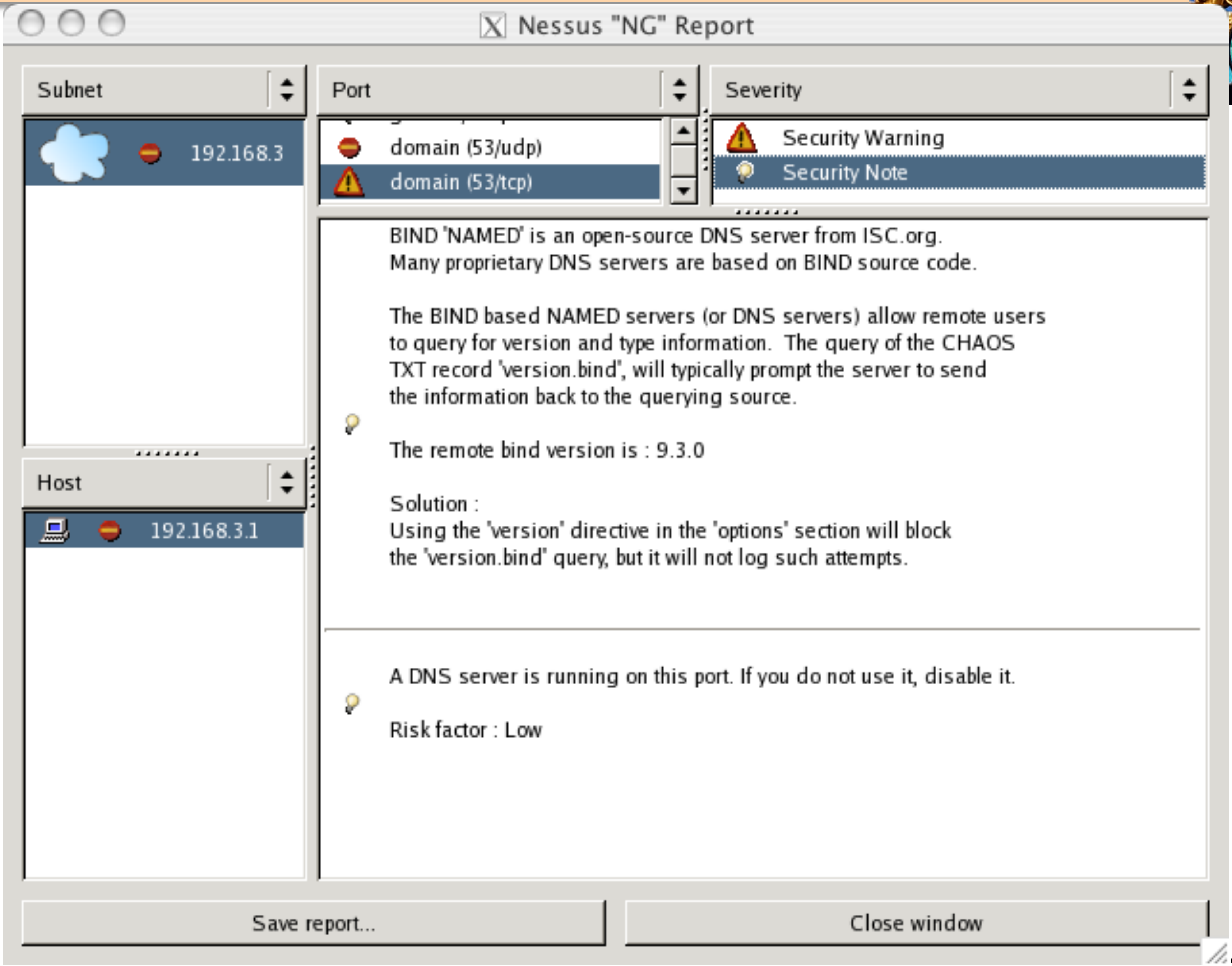
If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

See also : http://www.cert.org/advisories/CA-1997-22.html

Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).

If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf

If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command



BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.

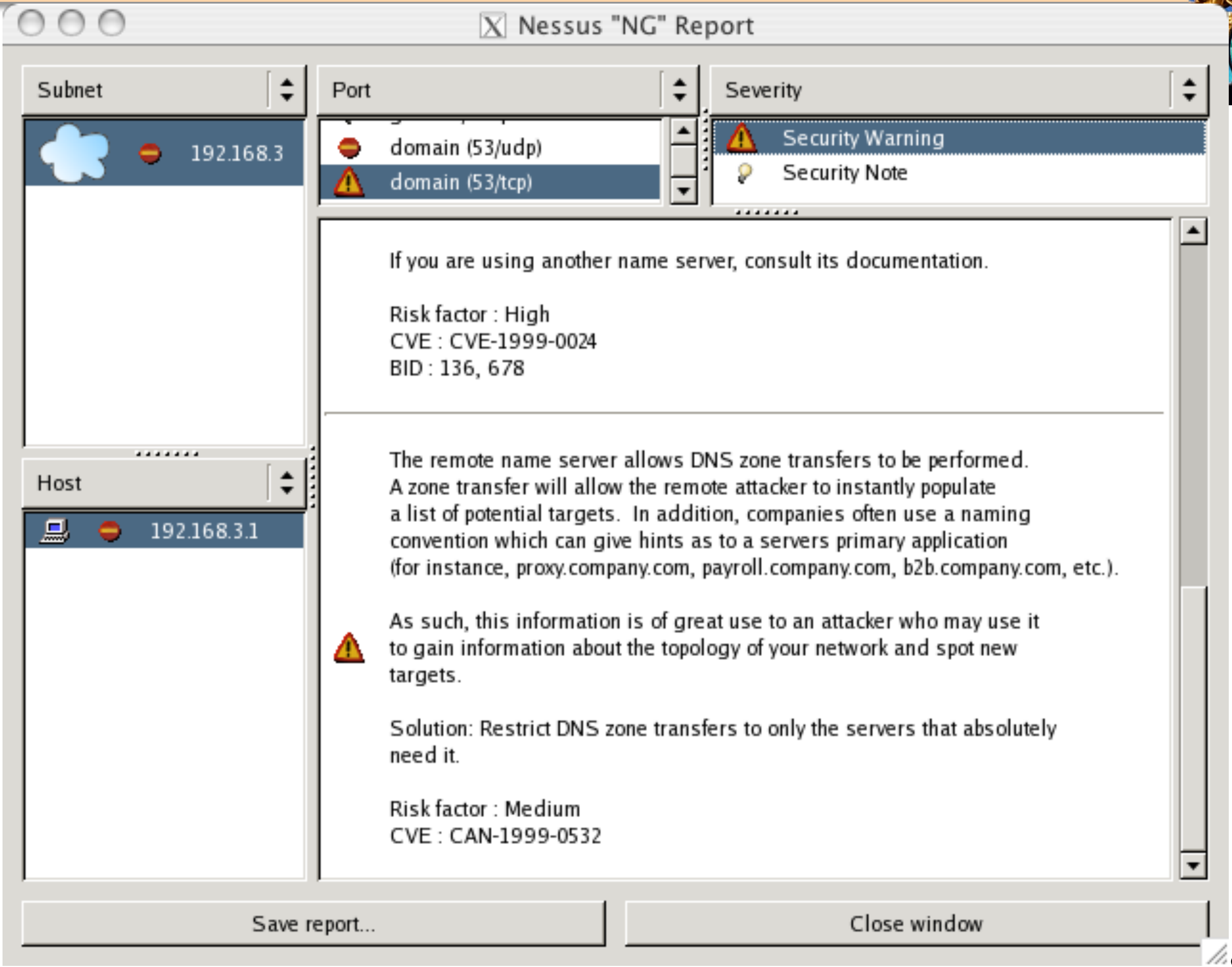
The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information. The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.

The remote bind version is : 9.3.0

Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low



If you are using another name server, consult its documentation.

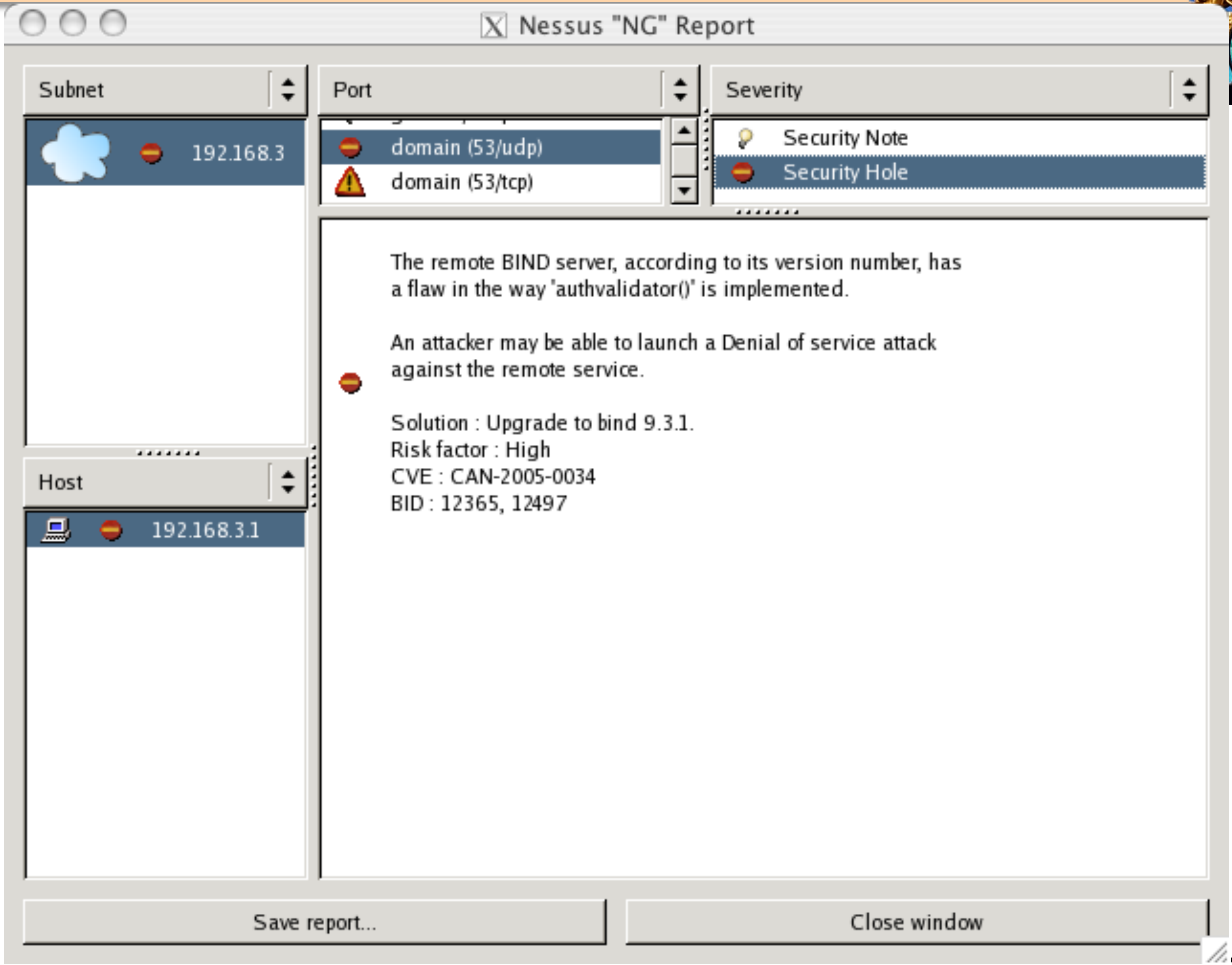
Risk factor : High
CVE : CVE-1999-0024
BID : 136, 678

The remote name server allows DNS zone transfers to be performed.
A zone transfer will allow the remote attacker to instantly populate
a list of potential targets. In addition, companies often use a naming
convention which can give hints as to a servers primary application
(for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).

As such, this information is of great use to an attacker who may use it
to gain information about the topology of your network and spot new
targets.

Solution: Restrict DNS zone transfers to only the servers that absolutely
need it.

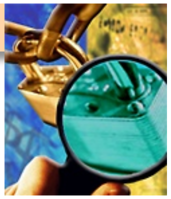
Risk factor : Medium
CVE : CAN-1999-0532



The remote BIND server, according to its version number, has a flaw in the way 'authvalidator()' is implemented.

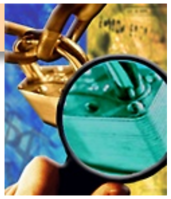
An attacker may be able to launch a Denial of service attack against the remote service.

Solution : Upgrade to bind 9.3.1.
Risk factor : High
CVE : CAN-2005-0034
BID : 12365, 12497

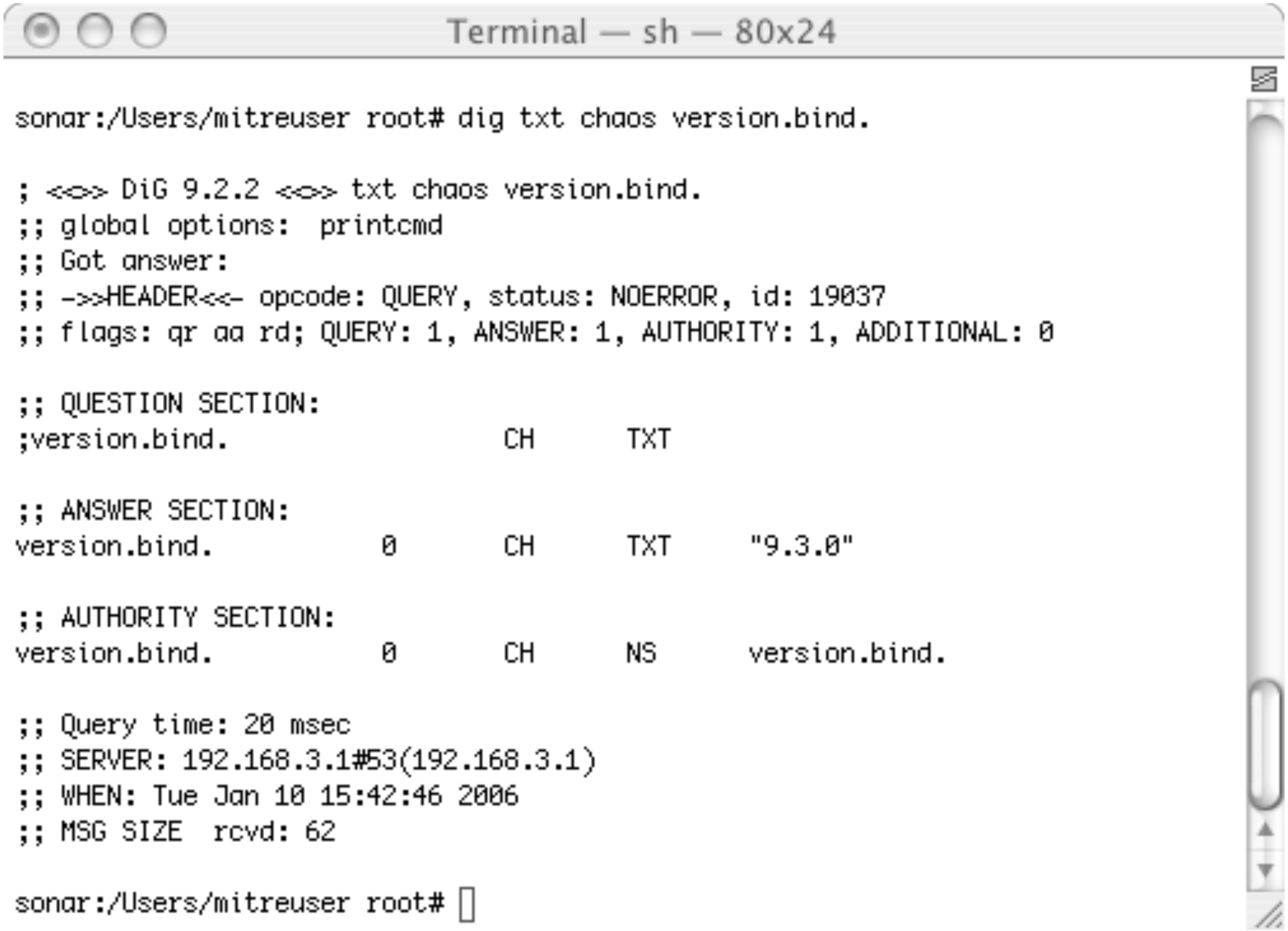


Manual Review

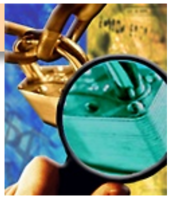
- dig - Domain Information Groper
  - Allows more control than nslookup
  - Specify domain
  - Query type (mx, axfr, ns, soa, txt,……)
  - Server @myserver.mydomain.net
  - Query for mail exchange records in a domain
    - Dig mydomain.net mx
- dnswalk - DNS database debugger
  - Perl Script that Analyzes zone transfer data
  - Requires Zone transfers to be enabled (not a good thing)
  - Reports configuration warnings and errors
  - Requires Perl module Net::DNS



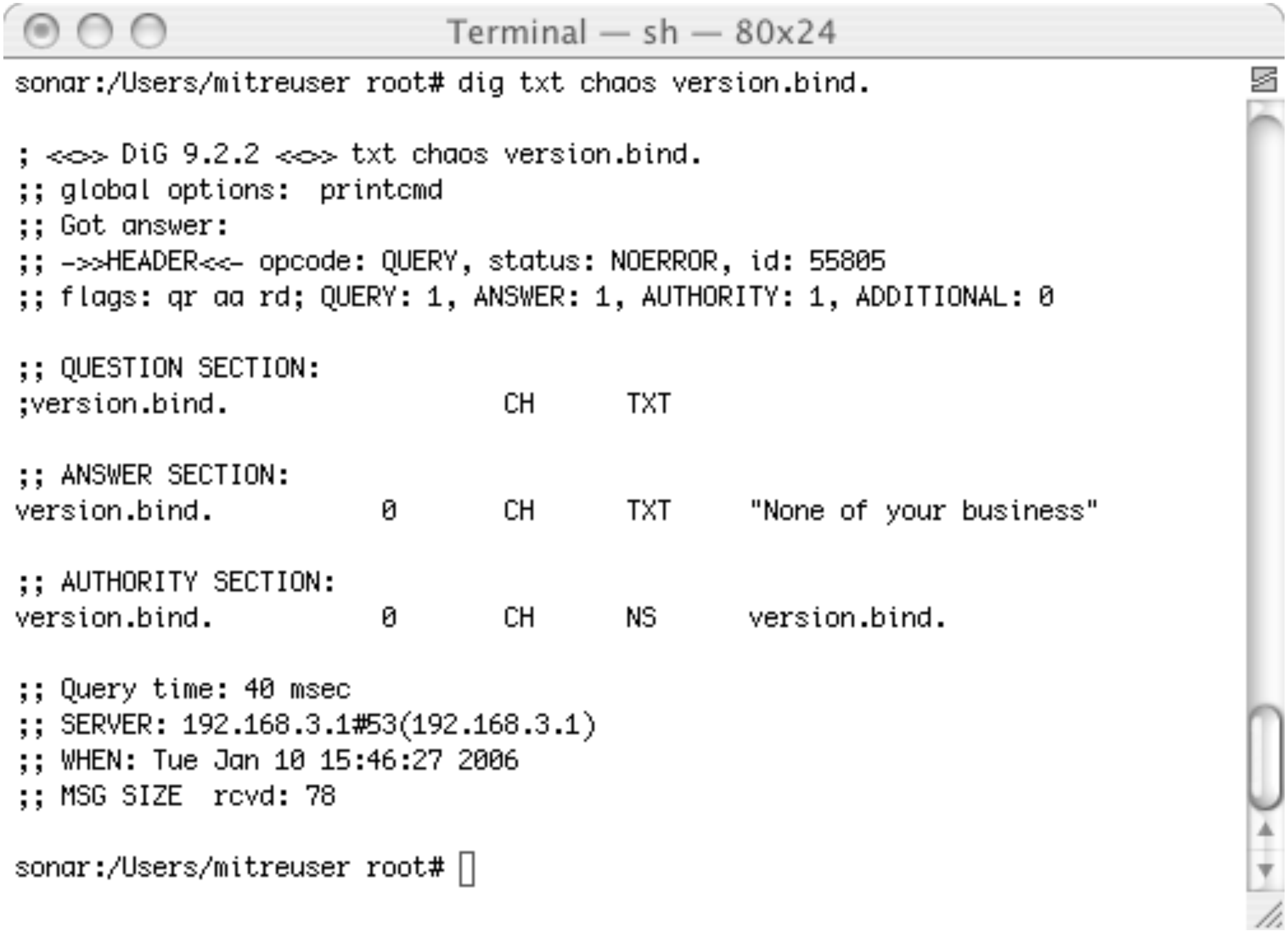
Dig Version Info



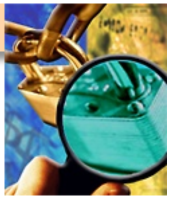
```
sonar:/Users/mitreuser root# dig txt chaos version.bind.

; <<>> DiG 9.2.2 <<>> txt chaos version.bind.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19037
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.3.0"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 20 msec
;; SERVER: 192.168.3.1#53(192.168.3.1)
;; WHEN: Tue Jan 10 15:42:46 2006
;; MSG SIZE  rcvd: 62

sonar:/Users/mitreuser root# ▯
```



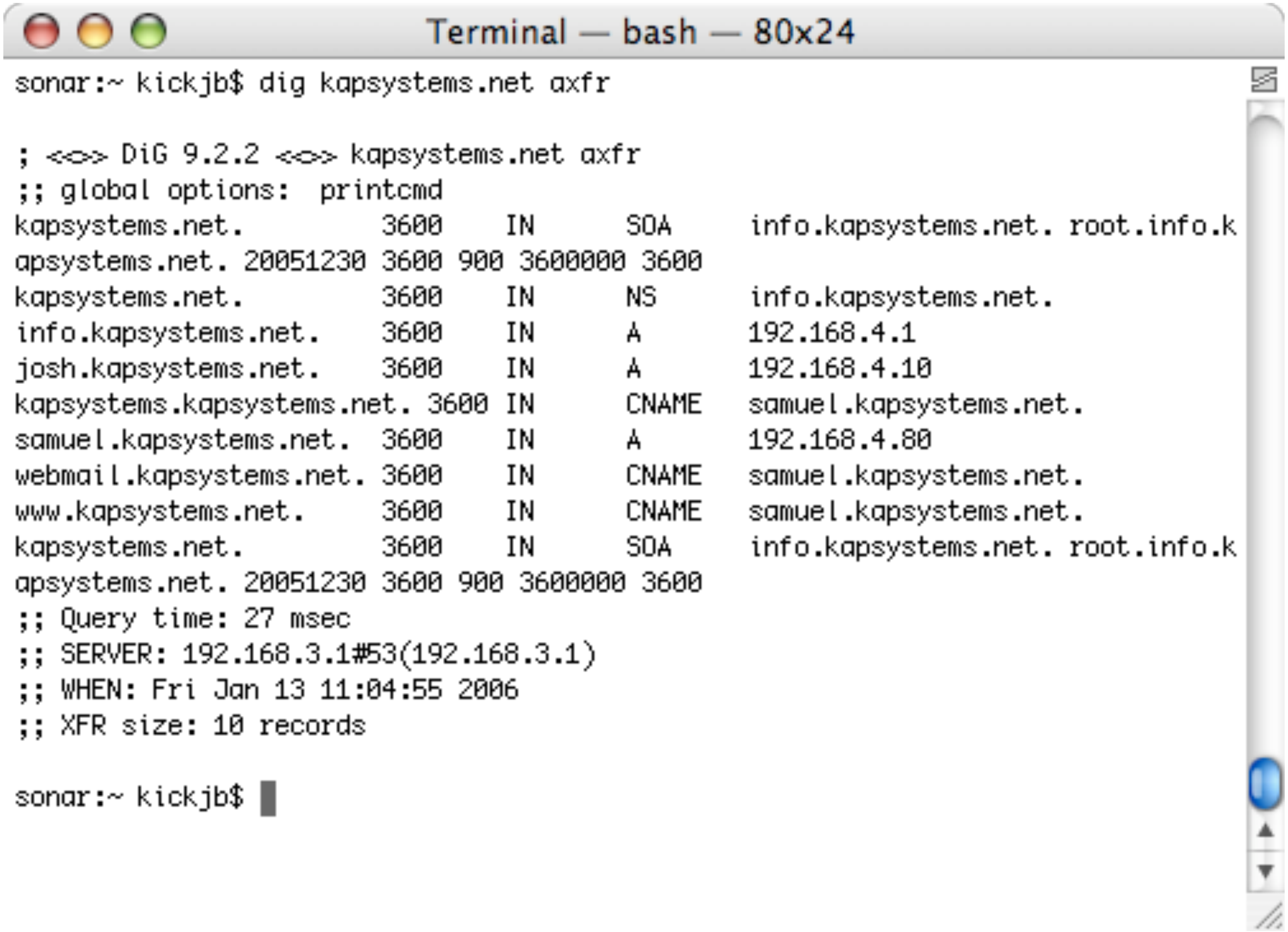
Dig Without Version



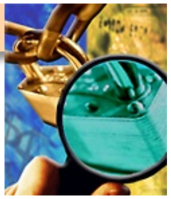
```
sonar:/Users/mitreuser root# dig txt chaos version.bind.

; <<>> DiG 9.2.2 <<>> txt chaos version.bind.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55805
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "None of your business"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 40 msec
;; SERVER: 192.168.3.1#53(192.168.3.1)
;; WHEN: Tue Jan 10 15:46:27 2006
;; MSG SIZE  rcvd: 78

sonar:/Users/mitreuser root# 
```



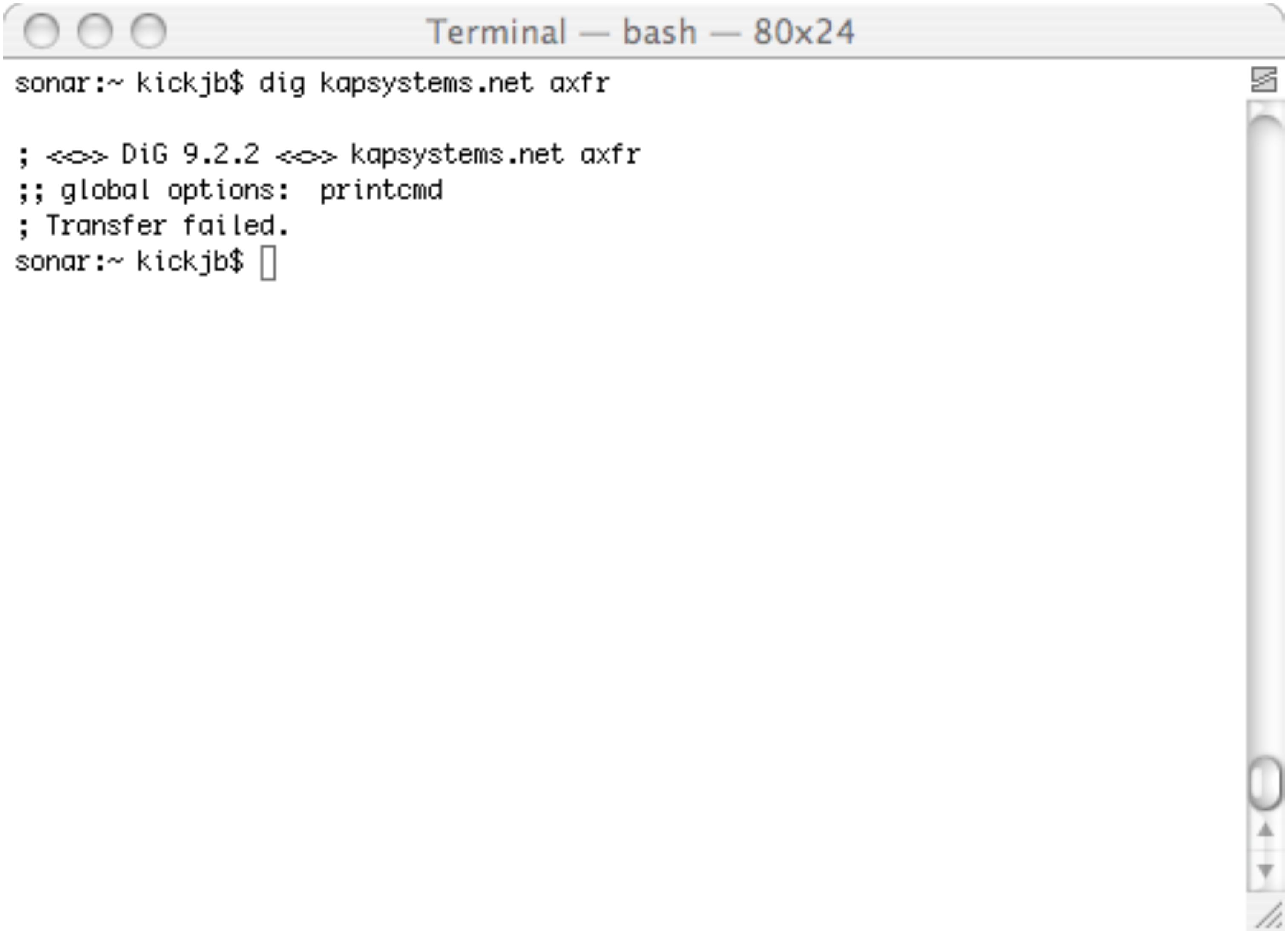
Dig - Zone Transfer



```
sonar:~ kickjb$ dig kapsystems.net axfr

; <<>> DiG 9.2.2 <<>> kapsystems.net axfr
;; global options:  printcmd
kapsystems.net.         3600    IN      SOA     info.kapsystems.net. root.info.k
apsystems.net. 20051230 3600 900 3600000 3600
kapsystems.net.         3600    IN      NS      info.kapsystems.net.
info.kapsystems.net.    3600    IN      A       192.168.4.1
josh.kapsystems.net.    3600    IN      A       192.168.4.10
kapsystems.kapsystems.net. 3600 IN      CNAME   samuel.kapsystems.net.
samuel.kapsystems.net.  3600    IN      A       192.168.4.80
webmail.kapsystems.net. 3600    IN      CNAME   samuel.kapsystems.net.
www.kapsystems.net.     3600    IN      CNAME   samuel.kapsystems.net.
kapsystems.net.         3600    IN      SOA     info.kapsystems.net. root.info.k
apsystems.net. 20051230 3600 900 3600000 3600
;; Query time: 27 msec
;; SERVER: 192.168.3.1#53(192.168.3.1)
;; WHEN: Fri Jan 13 11:04:55 2006
;; XFR size: 10 records

sonar:~ kickjb$ █
```

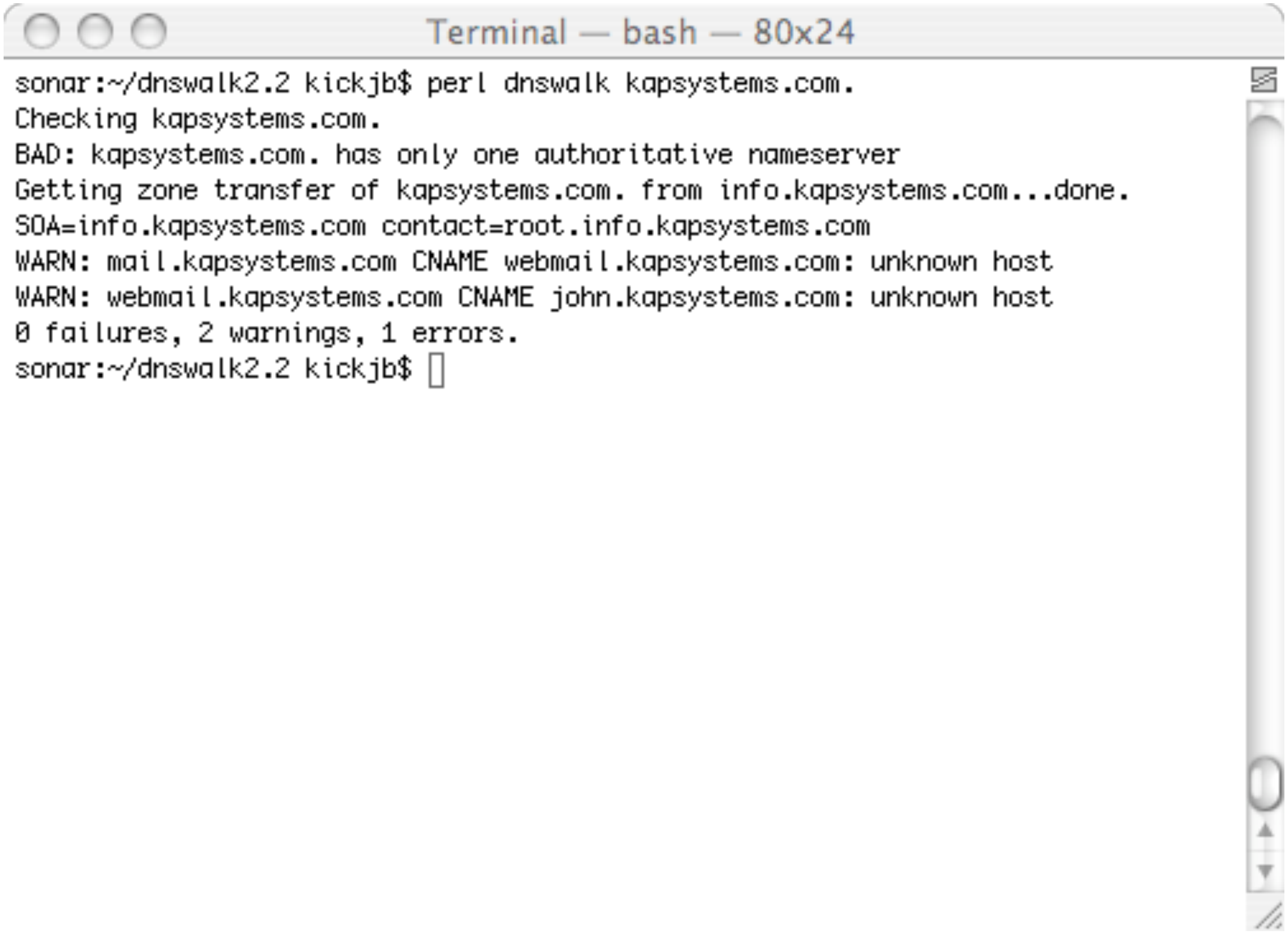


Dig - Zone Failure

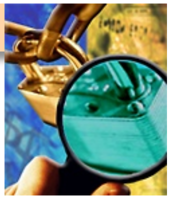


```
sonar:~ kickjb$ dig kapsystems.net axfr

; <<>> DiG 9.2.2 <<>> kapsystems.net axfr
;; global options:  printcmd
; Transfer failed.
sonar:~ kickjb$ 
```

dnswalk Output



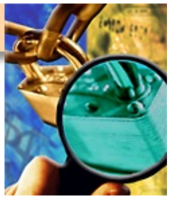
```
sonar:~/dnswalk2.2 kickjb$ perl dnswalk kapsystems.com.
Checking kapsystems.com.
BAD: kapsystems.com. has only one authoritative nameserver
Getting zone transfer of kapsystems.com. from info.kapsystems.com...done.
SOA=info.kapsystems.com contact=root.info.kapsystems.com
WARN: mail.kapsystems.com CNAME webmail.kapsystems.com: unknown host
WARN: webmail.kapsystems.com CNAME john.kapsystems.com: unknown host
0 failures, 2 warnings, 1 errors.
sonar:~/dnswalk2.2 kickjb$ 
```



Common Findings

- Jail not implemented
  - Failure to run BIND in a controlled environment exposes the entire system to compromised instead of just the BIND server
  - This is a high finding, especially if bind has vulnerabilities
  - Using the -t flag only chroots the name server process not the entire application and libraries
  - http://www.cymru.com/Documents/secure-bind-template.html

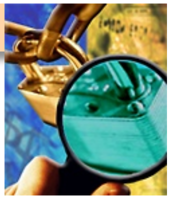
- BIND version displayed
  - Advertising the version of any software provides attackers unneeded information and should not be done
  - This is a medium finding, High if vulnerabilities are present
  - Add the the version option with a value other than the BIND version (e.g. version “Not Advertising”;)



Common Findings

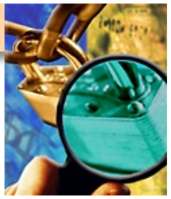
- Zone transfers not configured correctly
  - A zone transfer could allow all information for a zone to be taken or updated by an attacker
  - This could be a high finding if transfer is external
  - Ensure that zone transfers are implemented correctly using ACL’s

- ACL’s not implemented or incorrect
  - ACL’s are incorrectly configured
  - This could be a high medium or low depending on where the server is within the infrastructure
  - If the ACL’s allow unauthorized address to query then use high
  - External users should not be able to use the DNS server to resolve addresses other then domains for which the server is authoritative



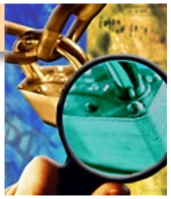
Common Findings

- External recursion allowed
  - Allowing recursion from outside will allow anyone to use your DNS server to perform lookups (cache poisoning)
  - High finding
  - It is a best practice to split DNS function between an internal external server
    - Internal for all clients; does not respond to external queries
    - External for external entities to resolve authoritative answers for your domain
- Inadequate logging
  - Logging on the most communicated with device besides a mail gateway is critical
  - Medium finding
  - Logging is a critical aspect of detecting malicious use of a DNS server



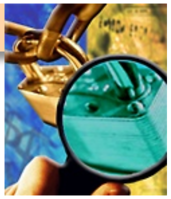
Common Findings

- Incorrect records
  - Having correct DNS records is essential to the success and purpose of a DNS server
  - This could be a low finding provided the system is not compromised
  - Ensure that the records are accurate



Conclusion

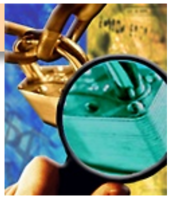
- DNS is a necessary evil in today's world
  - IPv4 addresses are easy to remember, but what about IPv6
  - What's the IP address of www.google.org??
- There are critical security implications of improper DNS configuration
- Thorough evaluation of DNS must be completed
  - Automated tools provide a network view of the service (nessus, nmap, dig, dnswalk)
  - Automated tools will not tell you additional information such as improper ACL's, logging config, transfer hosts and other details
  - Manual review of named.conf or equivalent
- Evaluator should have DNS references on hand during review if not familiar with DNS configuration settings



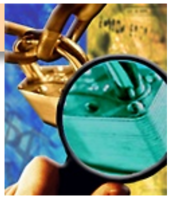
DNS Exercise

- Determine what mail servers exist in the testlab domain
- What possible security errors/vulnerabilities exist in the configuration of the testlab domain server

References

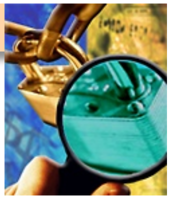


- http://www.oreilly.com/catalog/dns4/chapter/ch11.html
- CERT CC "Securing an Internet Name Server" August 2002
- Secure BIND Template By Rob Thomas http://www.cymru.com/Documents/secure-bind-template.html
- Chroot-BIND HOWTO By Scott Wunsch http://www.linuxsecurity.com/docs/LDP/Chroot-BIND-HOWTO.html



Questions

DHCP Security

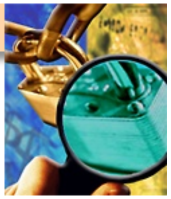


What is Dynamic Host Configuration Protocol (DHCP)

- Software that
  - Passes dynamic host configuration data in a TCP/IP network
  - Implemented as a client server model
  - Can perform dynamic DNS updates
  - Provides client information like IP, netmask, DG, hostname
  - Sets network server information such as NTP, DNS, LOG

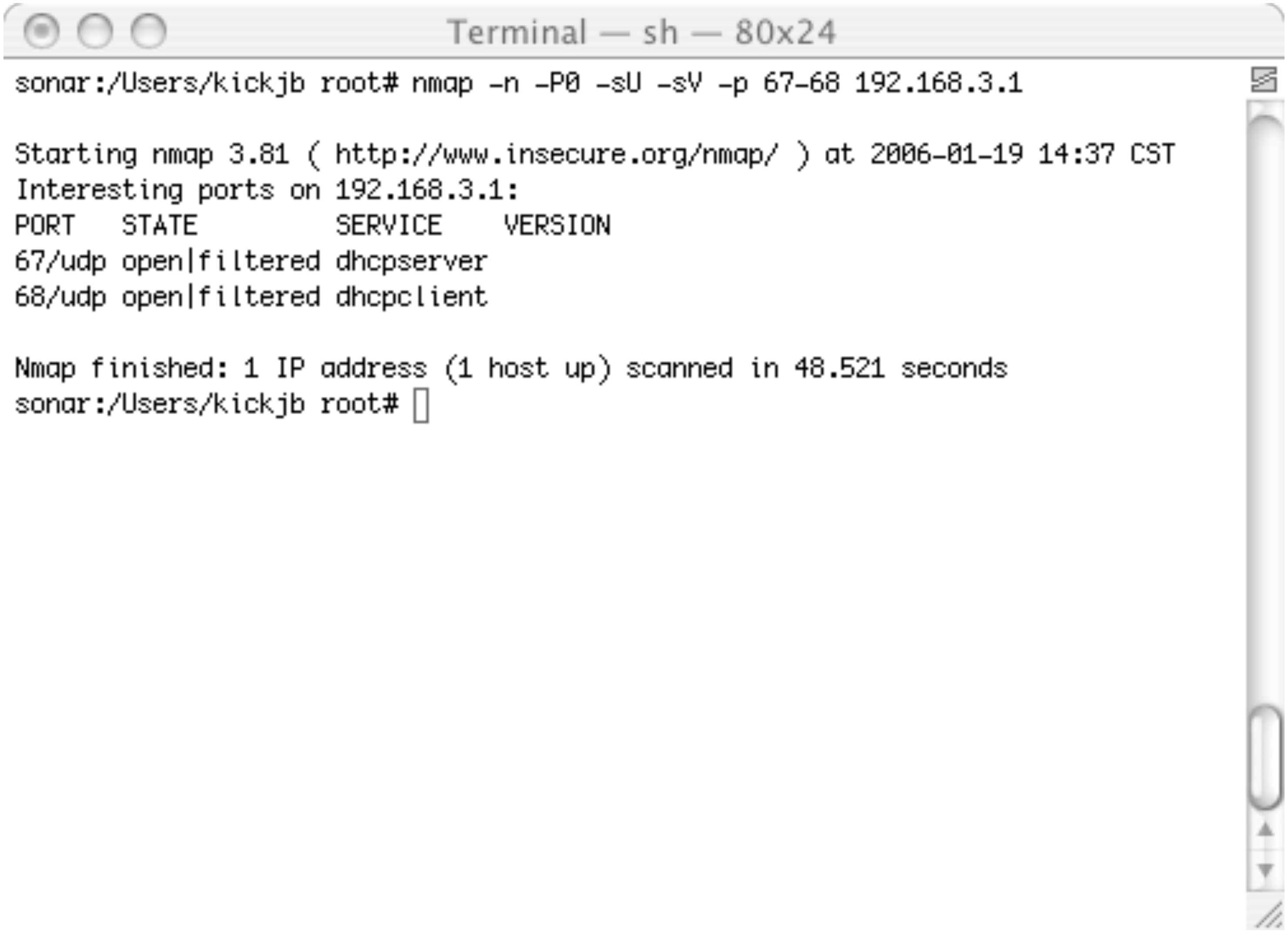
- Threatened by
  - Poor configuration
  - Denial of Services attacks
  - Spoofing attacks

ISC Dynamic Host Configuration Protocol (DHCP)

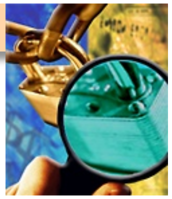


- Opensource DHCP server/client maintained by the Internet Software Consortium (ISC)
- Current Version 4.2.0p2 release 12/10/2010
- Widest availability and support
- Built from RFC2131 and RFC1533

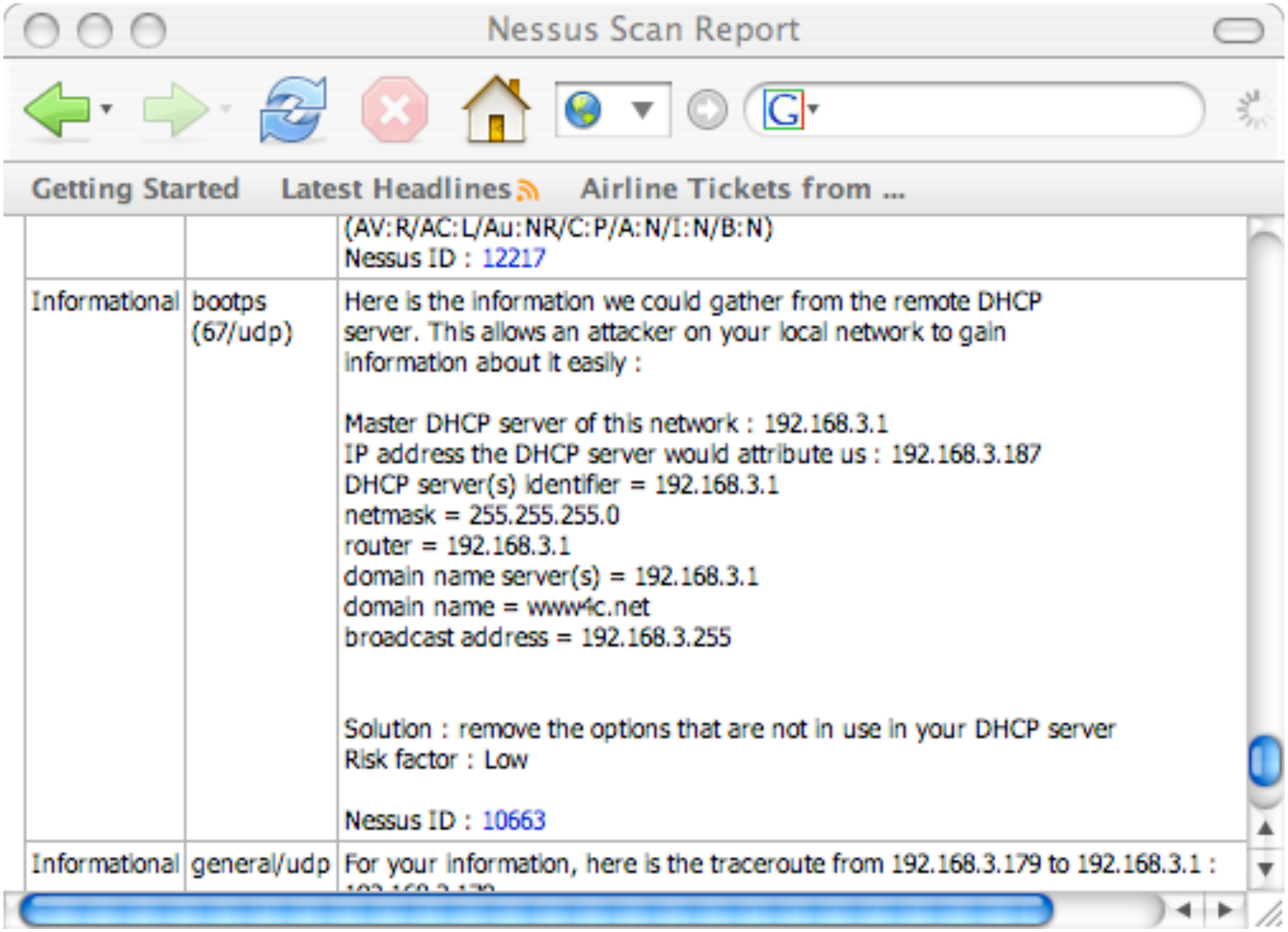
Nmap Information



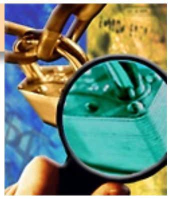
```
sonar:/Users/kickjb root# nmap -n -P0 -sU -sV -p 67-68 192.168.3.1

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-01-19 14:37 CST
Interesting ports on 192.168.3.1:
PORT   STATE         SERVICE    VERSION
67/udp open|filtered dhcpserver
68/udp open|filtered dhcpclient

Nmap finished: 1 IP address (1 host up) scanned in 48.521 seconds
sonar:/Users/kickjb root# 
```



Nessus Information



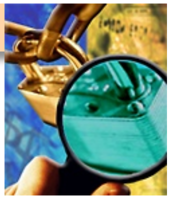
		(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N) Nessus ID : 12217
Informational	bootps (67/udp)	Here is the information we could gather from the remote DHCP server. This allows an attacker on your local network to gain information about it easily : Master DHCP server of this network : 192.168.3.1 IP address the DHCP server would attribute us : 192.168.3.187 DHCP server(s) identifier = 192.168.3.1 netmask = 255.255.255.0 router = 192.168.3.1 domain name server(s) = 192.168.3.1 domain name = www4c.net broadcast address = 192.168.3.255 Solution : remove the options that are not in use in your DHCP server Risk factor : Low Nessus ID : 10663
Informational	general/udp	For your information, here is the traceroute from 192.168.3.179 to 192.168.3.1 :



Common Findings

- Jail not implemented
  - Failure to run dhcpd in a controlled environment exposes the entire system to compromised instead of just the DHCP server
  - This is a low/medium finding
  - Need to ensure that the entire process and libraries are isolated versus just the proces
  - Similar to BIND or Apache jailing

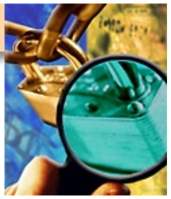
- Unauthorized access to server
  - Allowing access to the DCHP server from external or unauthorized devices could expose the server to compromise
  - Depends on the situation, generally low
  - DHCP services should only be available internally



Common Findings

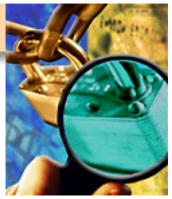
- Failure to check for rogue DHCP server
  - A rouge DHCP server on a network could assign the wrong IP addresses, or other network information to clients denying them access or providing a means to spoof valid servers and to capture/manipulate traffic.
  - Depends on situation and clients low or medium
  - Scan network looking for dhcp server or monitor dhcp requests/responses

- Inadequate logging
  - Logging is essential to detecting malicious user and misconfigurations
  - Medium finding
  - Ensure that proper diligence is performed on logging



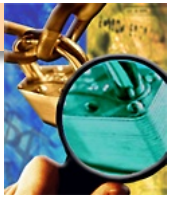
Common Findings

- Improper configuration
  - This should be a low finding but could be higher
  - Allowing clients to modify their own records could create conflicts or other issues on the network
  - Ensure that ignore client-updates is set



Conclusion

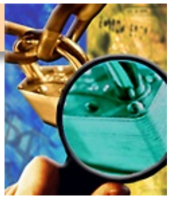
- DHCP is a useful service in a client environment
  - Dynamic address assignment, various options and DNS update functions
- DHCP has limited security impacts
  - Can be used to spoof systems and possibly disclose information
- A review of DHCP server should be completed
  - Automated tool is sufficient (nessus, nmap)
  - Manual review of dhcpd.conf or equivalent just as easy
- Evaluator should have DHCP references on hand during review if not familiar with DHCP configuration settings



References

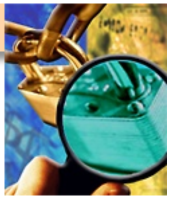
- https://www.isc.org - DHCP
- http://www.faq.org/rfcs/rfc2131.html - DHCP Protocol
- http://www.faq.org/rfcs/rfc1533.html - DHCP Options

Secure Shell



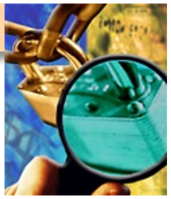
What’s SSH

- SSH (Secure Shell) is a protocol
  - Uses a variety of crypto algorithms
  - Version 1 outdated and weak
  - Version 2 best option
- Many implementations
  - F-Secure
  - Data Fellows Secure CRT
  - OpenSSH (Unix OS, Cygwin)
- Noticeable differences between implementations (key formats, syntax files)



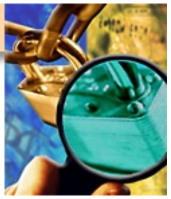
Why Use SSH

- It provides cryptographic transmission security (not clear text like Telnet/FTP)
- Replaces telnet, FTP, RSH type activities
- Commonly accepted in industry/DoD
- Adds many capabilities
  - Port forwarding
  - Key-based authentication
  - Key-based host authentication (shosts)



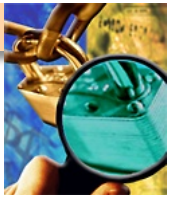
sshd_config

- Important options
  - AllowPortForwarding ?
  - Protocol 2
  - LogFacility ?
  - AllowRootLogin no
  - PamEnabled ?
  - HostBasedAuthentication ?
  - AllowFrom 192.168.3.1 johndoe ?



Key Based Authentication

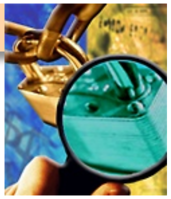
- Stronger form of authentication
  - Requires access to private key for authentication
  - Protected with a pass phrase
  - Pre-distributed public key
  - Can not be guessed/brute forced like a password
- Higher confidence of user identity
- Works great with ssh-agents for authentication



Two key formats

- F-Secure/Secure CRT format (SSH Commercial)
  - Convert from SSH-Compatible to Openssh
  - Ssh-keygen –X –f my_fsecure_key.pub
- Openssh format
  - Convert Openssh to SSH2-Compatible
  - Ssh-keygen –x –f id_dsa

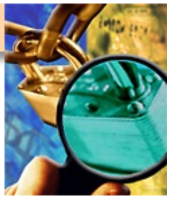
Questions



SSH Detection

- Determine where SSH is running
  - nmap
- Determine what versions of the SSH protocol are use
  - ssh-keyscan

NTP

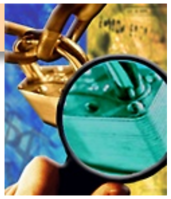


What is Network Time Protocol (NTP)

- Software that
  - Designed to synchronize clocks on a network
  - Master/Slave model

- Implementations
  - Appliances, hosts, servers, GPS time servers
  - Required for proper auditing and analysis
  - Accurate and reliable
  - Has some security features

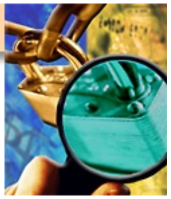
- Threatened by
  - Poor configuration
  - Denial of Services attacks
  - Spoofing attacks



Common Findings

- Not implementing a time synchronization process
  - Creates challenges in auditing events and analysis log system logs
- Allow every client to contact external NTP servers
  - There should be at least two primary NTP servers within an enclave for use by all clients
- Not standardizing on a time zone or offset for systems across multiple geographic regions
  - Complicates log event correlation and analysis

SMTP

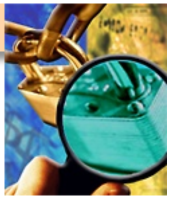


Simple Mail Transfer Protocol (SMTP)

- Software that
  - Designed to relay mail messages between systems

- Implementations
  - Appliances, hosts, servers, GPS time servers
  - Required for proper auditing and analysis
  - Accurate and reliable
  - Has some security features, not widely used

- Threatened by
  - Poor configuration
  - Denial of Services attacks
  - Spoofing attacks



Common Findings

- Not disabling unneeded features
  - EXPN and VRFY
  - Relaying
  - IMAP/POP

- Missing security
  - Spam detection
  - Malware checking
  - SPF records

- Outdated/vulnerable versions

Questions