



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gsna>

Auditing the Cisco AS5300 Remote Access Router Environment Through The Eyes Of An Independent Auditor

Cliff Ziarno
January 1, 2003
GSNA Assignment version 2.1

Abstract

In a world that cable, DSL and wireless begins to rule the world, there is still the world of the analog line and the remote access server systems. The remote access systems still have their place in the business and social community and continue to be used. Uptime and reliability are crucial to the remote access user functionality and security, just as almost every system, must work hand in hand to provide the services the clients need. This short paper is the audit review of the Cisco AS5300 Network Access Server remote access environment and covers the system, the risks associated with the system, the current state of practice, the audit and it's accompanying report.

© SANS Institute 2003, Author retains full rights

List of Tables and Figures

Figure 1 – Cisco AS2500	Page 6
Figure 2 – Show Version Statement of AS5300	Page 7
Figure 3 – Rear View of AS2500	Page 8
Figure 4 – Client Remote Access Network Setup	Page 9
Figure 5 – Cisco ACS Login Screen	Page 28
Figure 6 – Cisco ACS System Backup Setup	Page 28
Figure 7 - Cisco Failed Login Attempts	Page 30
Figure 8 – Cisco ACS Successful Logins	Page 31
Figure 9 – AS5300 Running Config	Page 31
Figure 10 – Cisco ACS Password Complexity Settings	Page 35
Figure 11 – AS5300 Show Modem in Enable Mode	Page 37
Figure 12 – Remote Access Clients Going to Domain Controllers	Page 38
Figure 13 – Clients Being Blocked From Various Services	Page 38
Figure 14 – Remote Users Having Full Access	Page 38
Figure 15 – Accepted and Blocked Traffic on Firewall	Page 38
Figure 16 – NMap and Nlog Input	Page 40
Figure 17 – Nlog Output from Router	Page 41
Figure 18 – RAT Output of Routing Table	Page 42
Figure 19 – Nessus Output of Router	Page 43

© SANS Institute 2003, Author retains full rights.

List of Abbreviations

AS2500	Access Server 2500
AS5300	Access Server 5300
ACS	Access Control Server
B Channel	Bearer Channel
BIOS	Basic Input/Output System
CIS	Center for Internet Security\
DAA	Designated Approving Authority
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoDCERT	Department of Defense Computer Emergency Response Team
EOS	End of Shelf (Life)
FIPS	Federal Information Processing Standards
FISCAM	Federal Information Systems Controls Audit Manual
FSO	Field Security Operations
IDS	Intrusion Detections System
IOS	Internetwork Operating System
IP	Internet Protocol
IS	Information Systems
LAN	Local Area Network
NCC	Network Control Center
NIACAP	National Information Assurance Certification and Accreditation Process
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
RAT	Router Assessment Tool
RJ-45	Registered Jack-45
SANS	SysAdmin, Audit, Networking and Security
SSAA	System Security Authorization Agreement
SNMP	Simple Network Management Protocol
SP	Special Publication
STIG	Security Technical Implementation Guidance
T-1	T-Carrier System
TACACS	Terminal Access Controller Access Control System
TACACS+	Terminal Access Controller Access Control System+

Table of Contents

Research in Audit, Measurement Practice and Control

1.1 The Audited System	6
1.2 Risk Evaluation	9
1.3 The Current State of Practice	12

The Audit Checklist

2.2.1. Physical Security	15
2.2.2. Contingency Planning	15
2.2.3. Documentation	16
2.2.4. Auditing	16
2.2.5. Authentication	17
2.2.6. Life Cycle Management	18
2.2.7. Remote Access Management	18
2.2.8. Change Control Management	19
2.2.9. Systems Management	20
2.2.10. Incidents and Incident Response Capability	21
2.2.11. Firewall Review	21
2.2.12. Router/Router Table Security	22
2.2.13. ACS Host Server Security	23
2.2.14. ACS Group Settings	23
2.2.15. ACS Network Configuration	24
2.2.16. NTP Configuration	24
2.2.17. ACS System Configuration	25
2.2.18. Administration Control	25
2.2.19. Certification and Accreditation	26
2.2.20. Security and Awareness Training	26

The Audit Evidence

3.1 Conducting the Audit	27
3.2 Residual Risk	45
3.3 Is the System Auditable	45

The Audit Report

4.1 Contingency Planning	46
4.2 Auditing	47
4.3 Authentication	48
4.4 Remote Access Security	48
4.5 Systems Management	49
4.6 Router/Router Table Security	49
4.7 NTP Configuration	50
4.8 Administration Control	51

List of References

52

Research in Audit, Measurement Practice and Control

Section 1 - The Audited System

The system to be audited during this short paper is the Cisco AS5300 Remote Access Server Router environment. The environment pertains to not just the router itself, but also it's accompanying software, Cisco ACS (Cisco Access Control Server) that supports the actions of the access server router through a graphical user interface. The router itself is configured through a standard local interface such as a serial connection, configured through the hyper terminal software of choice and then is configured allowing for minimal connectivity and functionality. When the ACS software is installed on the supported platform of choice, the wizard configures the routing tables through prompts and then implements the choices you make. Since the ACS software is installed on a separate system, the system may also have vulnerabilities of its own.

Figure 1 – 2500 Access Server



The Cisco AS5300 router in the organization being audited is used strictly to support the organization's mission, which is to provide twenty-four hour remote office access via a 800 number anywhere in the world for approximately 200 users. The customer's requirements are that their remote access sessions mimic their personal desktop environment in the local office to the closest degree possible. The AS5300 Access Server currently is configured to handle 48 simultaneous connections. It is not possible for them to connect 48 simultaneous connections due to their T-1 restraint, which only allows for 23 B channels but eventually they will be upgrading their service to handle all 48 modems. The customer does not deploy other services that the router is capable of providing other than analog dial in modem support.

The current router **show version** command shown below gives a more detailed description of the contents on the AS5300 router:

Figure 2 – Show Version of AS5300 Router Table (Next Page)

```
AS5300>show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C5300-JS-M), Version 12.0(4)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 18-May-99 12:13 by kpma
Image text-base: 0x600088F8, data-base: 0x60BAE000

ROM: System Bootstrap, Version 11.2(9)XA, RELEASE SOFTWARE (fc2)
BOOTFLASH: 5300 Software (C5300-BOOT-M), Version 11.2(9)XA1, RELEASE SOFTWARE (fc1)

AS5300 uptime is 5 weeks, 2 days, 21 hours, 8 minutes
System restarted by reload
System image file is "flash:c5300-js-mz_120_4_T1.bin"

cisco AS5300 (R4K) processor (revision A32) with 32768K/16384K bytes of memory.
Processor board ID 11818350
R4700 CPU at 150Mhz, Implementation 33, Rev 1.0, 512KB L2 Cache
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.1.
Backplane revision 2
Manufacture Cookie Info:
EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x30,
Board Hardware Version 1.64, Item Number 800-2544-2,
Board Revision B0, Serial Number 11818350,
PLD/ISP Version 0.0, Manufacture Date 4-Jan-1999.
1 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
24 Serial network interface(s)
48 terminal line(s)
4 Channelized T1/PRI port(s)
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
8192K bytes of processor board Boot flash (Read/Write)

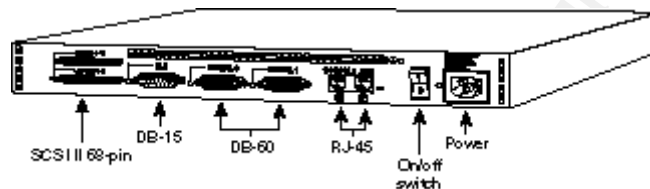
Configuration register is 0x2102
```

As we see from the above **show version** command, the router is running Cisco IOS version 12.0(4). This is an old version of IOS for routers but the AS5300 does not support any higher IOS version's at this time and Cisco does not plan to support any higher IOS versions for this router.

The accompanying Cisco AS5300 ACS server is running on a Compaq Proliant DL360 server running Windows 2000 Server Service Pack 3. The current ACS software revision level is version 2.6 and at the present moment, version 3.1 is the newest version of ACS available. The AS5300 router is already past its end of shelf life (EOS) and is only supported through Cisco maintenance agreements,

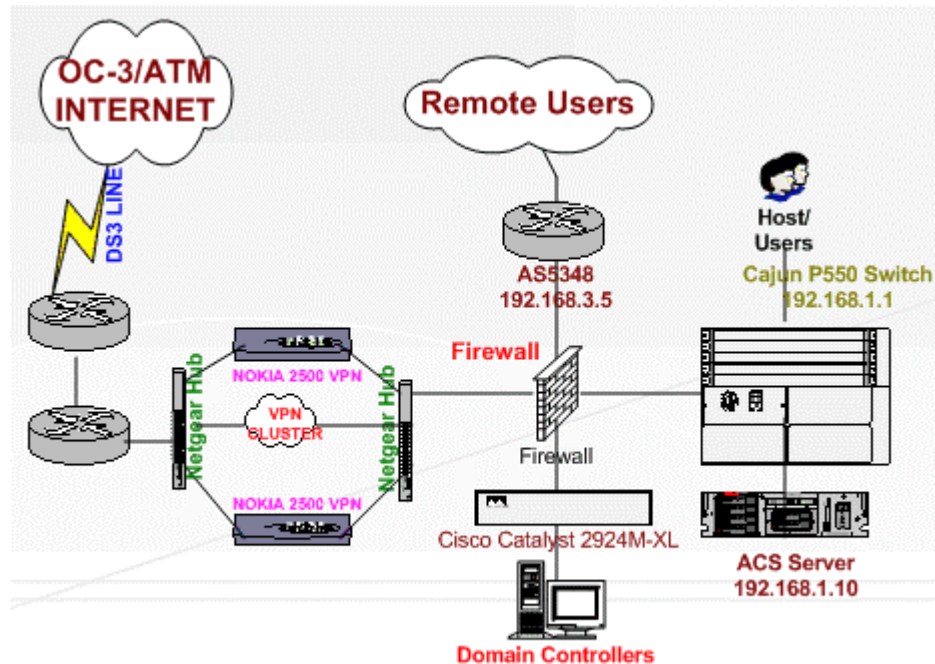
which the client currently purchases yearly along with its other routers at its organization. The Cisco ACS server software is currently configured to use Windows NT/2000 authentication through TACACS+, which is a requirement of the client by preference. They are aware the AS5300 and ACS server system can use RADIUS authentication along with Cisco's CiscoSecure databases but choose to use TACACS+. Below is a picture of a Cisco 2500 remote access router which extremely similar to the AS5300:

Figure 3 – 2500 Access Server (Back)



The Cisco AS5300 router is currently physically located on the client's internal network and contains the private IP address of 192.168.3.5, which is connected to the internal local area network through standard RJ-45 cable (The Network Interface Card can be seen above. It is physically located in the Network Control Center (NCC) at the client's site and is located in a secure, air conditioned cabinet and rack mounted, taking 4 U's of space. The ACS server currently resides on a separate subnet of its own inside the customer's network with the IP address of 192.168.1.10. These two systems that make up the remote access environment are separated and routed through a Checkpoint FW-1 4.0 firewall running on a Windows NT 4.0 server running service pack 6 which tracks and logs all of the activity between the systems. The Checkpoint firewall also routes the ACS software requests between the domain controllers for user authentication through Cisco TACACS+ which allows the client to map drives through scripts automatically and gain access to the Windows 2000 domain resources. These Windows 2000 domain controllers are located in a publicly accessible subnet. The firewall hosts and routes the AS5300 and the ACS server through the same NIC (Network Interface Card) which hosts two separate IP addresses. The publicly accessible subnet the domain controllers are located on is located on another NIC on the same firewall. A diagram of the remote access solution is below:

Figure 4 – Client Remote Access Network (Next Page)



In summary, the client's remote access system being audited is a Cisco AS5300 Access Server router and a Cisco ACS 2.6 server, which authenticates through Windows 2000 Server domain controllers. All traffic between the AS5300 and the ACS server is routed through a Checkpoint FW-1 server along with the Windows traffic, which is required for authentication. With this in mind, we will now continue our audit evaluation. For more information on other Cisco remote access solutions you can check out:

Hardware

<http://www.cisco.com/en/US/products/hw/iad/index.html>

Software

<http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html>

Risk Evaluation

When dealing with this remote access environment in this organization there are some main concerns that we had to understand from a broad overview when trying to realize the risk. Risk is defined specifically by the client, so we as auditors are not involved in the decision making process of which risks are acceptable and which are not. This is the specific task of the organization and the administrator. In the scenario we are evaluating, the client requires 24-hour remote access service allowing for zero downtime. In essence, this means that the systems are always vulnerable and must be fully fault tolerant.

The remote access environment poses risk from the end user and the external environment and the internal users and their environments. The end user when connected by analog phone line is in essence the same as a user that is connected internally except that laptops are much harder to secure than a standard workstation in a local environment. Laptop security must be taken into account and treated as a higher security risk than a standard internal user's workstation.

The end users laptops must be secured just as well as a server on the primary internal network since security is always only as strong as its weakest link. Since the client requires a simulated environment, each part of the remote access environment must be heavily secured and logged. The systems risks are the end users laptops, the remote access router, the server hosting the ACS software, the ACS software and configuration and the rules and logging that are implemented and configured on the firewall. The user's behavior is also one of the major risks that are in this remote access environment because they have full access to the internal LAN just as a local user.

Our security control objectives are to provide a fully functional remote access experience with the highest amount of security applied that doesn't degrade functionality. These security control objectives must be implemented through two types of controls: policies and procedures and technical controls. The policies and procedures are the control objectives that attempt to minimize our risk to systems. For example, if the policies and procedures say we cannot allow AOL Instant Messenger into the network and the user does not follow this course of action, our technical controls even though implemented will not need to be used. Our technical control objectives are the second tier and primary security control objectives. These are the controls that are used to enforce our policies and procedures at the organization to ensure security.

The following is the risk table matrix that addresses ten major risks we will audit for the client's remote access environment:

Risk	Probability	Consequences
Lack of Contingency Planning on the AS5300 and the ACS Server	High	Loss or service to the client due to system downtime causes the remote access clients to be unable to remotely connect causing loss of productivity for the agency.
Lack of sufficient user, vendor password and administrator authentication management.	High	Default vendor passwords or user accounts that belong to user's who are not active, especially fired users, still exist active on the system opening up the organization to possible security holes that could stop remote services or worse, cause

		malcontent and damage on the client's network.
Lack of physical security.	High	Insufficient physical access controls to the system allow non-authorized individuals to accidentally or purposely access the systems possibly causing them to stop functioning properly causing the remote users loss of access and increased trouble tickets for the helpdesk.
Insufficient logging and auditing controls.	High	In the case of a security breach, there are few avenues to track the events. Trying to impose punitive damages on the alleged conspirator could be difficult and costly to the organization. Also, the lack of auditing and logging also increases troubleshooting time for administrators when the systems do not function properly.
Lack of technical controls on laptops.	High	Users and villains cause a network security breach causing downtime, monetary loss and sensitivity problems by inappropriate use of an organization's laptop.
Lack of Systems and Life Cycle Management.	High	In the case of a hardware or software problem, the faults may go undetected causing the organization to support the client in reactive mode. The lack of Life Cycle Management also puts the client in reactive mode, which in turn may end in prolonged downtime for the remote access end user.
Poor configuration and change control management.	High	System configurations change on systems and are poorly tested and not authorized which render the systems non-functional which ends in loss of productivity for the agency and it's remote users.
Lack of policies and procedures for systems and users.	High	Lack of policies and procedures allow for inappropriate controls and inappropriate usage on systems causing overall security problems.
Insufficient management review or re-review of firewall rules that	High	Remote users are granted the same access as local corporate users

control internal and remote access users access.		causing major security problems when remote users systems are breached. Without the regular review of these rules, security breaches may continue unattended causing security violations on the client's network.
Poor systems and modem performance due to the lack of network management and hardware and software maintenance.	High	Users receive high error rates when dialing in due to bad or improperly maintained onboard modems or faulty hardware or software causing productivity loss.

The AS5300 router functions as a router but is not ideally going to be audited nor configured like most routers. When most people think of routers, we think of border routers, which get attacked daily. Even though the AS5300 is a router, it isn't really doing much routing. The risks we are mostly concerned with in this client's network are other matters such as contingency planning, life-cycle management and misconfigured systems from lack of change control management. In short, we are most concerned with the aspects that affect downtime other than just router penetration attacks, even though they are important to secure. The router isn't accessible to the Internet except through analog connections so we must be concerned with the machines accessing it on the outside and what traffic is being passed to the LAN from them. We are also very concerned with the physical risks of the system such as modems running at low performance and the ability or inability to recover after a router or server crash or a power supply failure. These risks are directly involved in the security and performance of the client's objectives unlike most border routers where attackers are trying to bring the system down. A secure configuration for the client's remote access system here is to locally secure the laptop, the AS5300 and the ACS server systems and to secure the flow of the traffic between them in conjunction with solid policies and procedures, not just for administrators but for users and the systems themselves.

The Current State of Practice

When doing research on the systems, the best practice is to attack the audit from two angles. The first side is more of the business side that revolves around the policies and procedures of the systems. These are the steps that keep the systems approved and configured correctly, planning for contingencies and the impact of the system being down. It is more of a business perspective and a management side. The NIST government publications are absolutely invaluable for policy and procedure assessments of systems. The NIST publications come with hearths of information about conducting audits along with follow along templates. The client that was audited for this paper was DoD so the DITSCAP documentation was heavily used. The DITSCAP (DoD Information Technology Security Certification and Accreditation Process) is the accreditation system that

is specific to the military systems and very similar to the NIST government documentation. It covers many similar subjects just as the NIST manuals such as Life Cycle Management and Contingency Planning. The NIACAP (Information Assurance Certification and Accreditation Process) is the government's equivalent of the DITSCAP. Both the government and DoD must follow these specific guidelines before a system can be accredited to officially run on the agency's network by acquiring it's SSAA or System Security Authorization Agreement. The formal definition of the SSAA is:

The SSAA is a formal agreement among the DAA(s), certifier, user representative, and program manager. The SSAA is used throughout the entire NIACAP process to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security.¹

The whole purpose of these documents is to guide a system from the beginning of its birth to the end of its life, being accredited the whole way through. It's a way of managing systems to keep them secure and also keeping the agency in a proactive stance instead of a reactive stance. These publications can be found here along with some other very helpful links:

DITSCAP and NIACAP

<http://iase.disa.mil/ditscap/ditsdocuments.html>

Federal Information Processing Standards (FIPS)

<http://csrc.nist.gov/publications/fips/index.html>

NIST Special Publications

<http://csrc.nist.gov/publications/nistpubs/index.html>

Department of Commerce

<http://www.osec.doc.gov/osy/SECURITYMANUAL/manualecuritypolicies.htm>

Federal Computer Incident Response Center

<http://www.fedcirc.gov/>

Office of Management and Budget Documentation

<http://www.omb.gov>

Open Source Security Testing Methodology Manual

<http://www.isecom.org/>

Conducting technical research on the systems was of a different matter. The NIST publications site has many semi-technical articles and checklists but to get the extremely detailed information pertaining to checklist, it was better find this

¹ National Information Assurance Certification and Accreditation Process, Page 2

information at technical security websites as the ones below:

Center for Internet Security – NSA Router Configuration Guide, Router Assessment Tool (RAT), Windows 2000/NT Benchmarks)

<http://www.cisecurity.org/>

NMap Stealth Port Scanner Tool

<http://www.insecure.org>

Cisco Systems – Router Security

<http://www.cisco.com>

SANS Reading Room – Security White Papers

<http://www.sans.org>

Various Tools and Reading

<http://www.security-focus.com>

Nessus Security Scanner

<http://www.nessus.org>

NLog Tool

<http://www.secureaustin.com>

Microsoft Security

<http://www.microsoft.com/security>

These sites not only offer information but invaluable tools that assist with the audit of these systems. Most of the information that was found when the paper was started was by just using standard search engines such as:

<http://www.google.com>

<http://www.lycos.com>

<http://www.yahoo.com>

Since the remote access environment here was Cisco based (www.cisco.com), research was also one extensively at the vendor site. There were many documents that addressed locking down routers such as the AS5300, but there was little or no documentation on the Cisco ACS server software. Most the checklist coming in the next part of this paper was done through the collation of the many documents, testing and hands on experience. One of the best sources of knowledge that was found was through news group postings, which had user specific issues addressed. One of the main documents used during this process was the DISA Field Security Operations checklist, which I believe is not accessible to the public but may be able to be ordered.

Section 2 - The Audit Checklist

1. Physical Security	
Reference	DISA Network STIG, NIST SP-800-26, FIPS 31, DITSCAP
Control Objective	Provide physical security for systems in a controlled area and account for only certain individuals who have access to these systems. Also and try to eliminate unauthorized entry and access to these systems.
Risk	The systems can be mishandled, stolen and/or compromised causing monetary loss for the organization and system downtime contributing to productivity loss from theft or destruction.
Compliance	The systems should be in a controlled area in which only authorized have individuals too. The physical security officer should possess the official documentation that shows the policies and procedures of access and who has it.
Testing	The controlled area should have an official document outside the entrance with the authorization information that includes a list of who is allowed access and who to contact if any questions exist. The systems should also be physically secured in the controlled room, preferably mounted and in a locked cabinet.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

2. Contingency planning	
Reference	NIST SP 800-26, FISCAM, DITSCAP
Control Objective	Provide contingency planning support for the systems including the ability to restore critical files in the case of natural disaster or normal administrator error.
Risk	The systems can be compromised or suffer hardware or software errors resulting in downtime and productivity loss.
Compliance	The critical configuration files should be backed up and protected in a fireproof safe offsite. If required, there may be a spare AS5300 and a spare ACS server ready for fault tolerance but this is may not be a requirement.

Testing	Provide proof of files being backed up to tape and taken offsite for storage. If there are spare units available, take one offline and confirm the fault tolerance. All log files should be backed up also. For restore testing, delete a configuration file and restore it and assure working order. The ACS configuration can be found in the System Configuration tab under ACS Backup and ACS Restore.
Objective/Subjective	Objective/Subjective – The actual process of providing proof of the contingency plan process is objective but the concept of needing true fault tolerance or not is subjective by the client.

3. Documentation	
Reference	NIST SP 800-26, FISCAM, DITSCAP
Control Objective	Provide documentation that supplies the vendor contact numbers, part numbers and other configuration parameters of the systems. Also provide the SSAA (System Security Authorization Agreement) approval to operate on the network.
Risk	With the lack of documentation, getting a machine up from a compromised position will require excessive time to track down vendors during a recovery. From a configuration management standpoint, documentation is valuable and without it you lose man-hours doing excessive legwork that would be easily achieved with up to date documentation.
Compliance	Confirm the systems have official documentation and that it covers vendor information, SSAA agreements and configuration information.
Testing	Affirm that the documentation exists, is up to date and is in a safe place such as a fireproof safe.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

4. Auditing	
Reference	DISA Network STIG, NIST SP-800-26, DITSCAP
Control Objective	Provide the ability to produce audit logs for administrative and security uses. Audit logs allow administrators and security professionals to review actions amongst the systems such as performance problems and a trail to follow during a security

	breach.
Risk	Systems and users can incur functionality problems that administrators will not be able to see without a functioning audit log causing wasted and inefficient use of time. The audit log also allows you to follow audit trails for security auditing. Without these, the administrator will have little ammo to push punitive damages.
Compliance	The systems should have appropriate auditing turned on and configured on the ACS server, the Firewall and the Cisco AS5300.
Testing	Assure that auditing is functioning correctly by dialing into the AS5300, attempting an activity such as browsing the web, then logging off. Also, test logging in with incorrect passwords. Service logging should be turned on in the ACS configuration menu under System Configuration/Service Control and System Configuration/Logging. To assure logging is working, check the appropriate log path and make sure they are there. Also check under System Configuration, ACS Service Management to confirm logging is set.
Objective/Subjective	Objective/Subjective – This item is primarily objective but is partly subjective because the client has to understand certain parts of it's risk. To audit every action on a system could take excessive space and processing power and may render the system useless.

5. Authentication

Reference	DISA Network STIG, NIST SP-800-26, DITSCAP
Control Objective	Provide logical access controls security to the corporate network through authentication.
Risk	The corporate system could allow unauthorized users entering it remotely due to bad password policies or procedures.
Compliance	The organization should have policies and procedures that address how clients will authenticate to the network. They should use at least two-factor authentication in the case that a perpetrator discovers one of the authentication pieces.
Testing	Provide policies and procedures that address the authentication scheme of the systems. Also, physically prove that the authentication works by

	logging in remotely. Try bypassing passwords by cracking and/or locating them on the laptop somewhere. Make sure that the two-factor authentication works properly by trying to use only one factor authentication and testing results. Also confirm that the individual ACS and AS5300 login passwords are of complexity. To check passwords complexity on the AS5300, check the System Configuration/Password Validation option and confirm complexity. If the users are authenticating through TACACS+ (Network Configuration/Access Server Setup), confirm the Windows domain policy enforces complexity.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

6. Life Cycle Management

Reference	NIST SP-800-26, DITSCAP
Control Objective	Provides a program or process that allows the system be accounted for within its life-cycle allowing for full support at all times and allows for future budgeting of new equipment and software.
Risk	The systems will become outdated and non-supported. When in the need for new systems, the budget may not be in place to upgrade a new system from the legacy system causing monetary problems for procurement. The systems in turn may not function at 100 percent reducing remote access productivity.
Compliance	The systems should possess life cycle management policies and procedures that address the specific systems along with its accompanying documentation.
Testing	Provide the necessary policy and procedures documentation that shows the end of life cycle dates of the systems and the planned budget that is forecasted for it. All dates of purchase, support and dates must be documented.
Objective/Subjective	Objective/Subjective – The end of life cycle documentation is fully objective but the concept of when the hardware is “end of life” is mainly subjective and the client may continue to use it at this stage.

7. Remote Access Security

Reference	NIST SP 800-46, DITSCAP
Control Objective	Provide policies and procedures that address remote access use for the organization that will mitigate risk to the organization's network.
Risk	Flagrant remote access use by users and administrators could cause a security breach on the organizations network.
Compliance	The organization should possess written and documented policies and procedures for remote users and remote administration. The policies should be extremely detailed, precise and understood. The laptop systems should be secured and protected in the case of sabotage or theft.
Testing	The laptop should be locked down with anti-theft devices such as locks and logically secured through the use of two-factor authentication. Firewalls should be installed on the systems and configured. Anti-virus software must be installed and configured to update definitions and prove that it actually updates. File integrity checkers should be installed on all the laptops. Encryption should be in use in the case of theft or unauthorized use. Web browsers should be configured to limit ActiveX, Java and JavaScript and plug-ins should be disabled. The laptops should have non-descriptive carrying cases, BIOS passwords set and Spyware tools installed.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

8. Change Control Management

Reference	DISA Network STIG, NIST SP-800-26, DITSCAP
Control Objective	Provide change control management for the systems. By providing this, the systems will remain in states that are understood by management along with administration. This saves time and money due to troubleshooting time when systems are down.
Risk	Without change control, the systems may be configured or modified without knowledge of it putting the systems in an insecure state or non-functioning state.
Compliance	Change control management will primary be upheld by policies and procedures. In essence, most systems allows administrators full control of systems

	so changes are inevitable but there should be processes that adhere to testing before going production after these changes. You can also institute separation of duties with peer review on systems so change control risk is lowered.
Testing	Provide the systems policies and procedures that adhere to the system change control policies. Attempt to make changes to a system that should have separation of duties instilled onto it.
Objective/Subjective	Objective/Subjective – Providing the documentation on policies and procedures of the change control management is objective but the decision to employ separation of duties on the systems is highly subjective.

9. Systems Management	
Reference	DISA Network STIG, NIST SP-800-26, DITSCAP
Control Objective	Provide systems management that addresses hardware and software performance. The goal in this control objective is to allow the systems to perform at peak performance and find problems that arise in a proactive arena versus reactive. The control's goal is to provide 100 percent uptime for the client by monitoring the systems hardware and software.
Risk	The systems may be performing under an acceptable performance level causing downtime and possibly downtime.
Compliance	Confirm that the systems have policies and procedures drafted that address the implementation of systems network management and that the policies and procedures are actually implemented.
Testing	Confirm that the use of tools such as HP Openview and CiscoWorks are being used for monitoring. Also, make sure the logging is turned on the router and that modem performance is monitored daily. Confirm that the ACS server and its services are being monitored through some type of monitoring or log server. SNMP will need to be activated on the router for management so confirm that only private SNMP community strings are used and documented. Preferably only allow out of band management on the router also by physically checking the cables attached to the system.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

	are not applicable to any subjective ideas.
--	---

10. Incidents and Incident Response Capability	
Reference	DISA Network STIG, NIST SP-800-26
Control Objective	Provides the administrator the procedures to effectively and efficiently handle security breach issues against the system.
Risk	Individuals wishing to do harm against the organization may succeed in breaking into the environment through the remote access system. Without these policies and procedures, the administrator will not know what to do when this happens, if he/she even knows "what" is. Without the accompanying IDS, they may not be able to track the activity.
Compliance	The systems should have policies and procedures that are in place to implement the control objective when the system is breached are attempted to be breached. Also, the organization should implement an IDS that works in conjunction with the remote access network.
Testing	Provide the documentation that shows the steps to take when a breach has occurred on the system and then implement them. This documentation should contain actual steps and contacts you will need such as the DoDCERT. Also, confirm that the organization is utilizing an accompanying Intrusion Detection Systems (IDS) that is working correctly by scanning a dummy machine from a remotely logged in laptop using a penetration utility such as Nessus and watch the IDS logs for the scanning activity and confirm the IDS can see the activity.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

11. Firewall Review	
Reference	DISA Network STIG, NIST SP-800-26
Control Objective	Assure that the firewall rules or router filters function correctly and are secure. These rules are to fulfill client's functionality along with containing activity that is not approved on the agency's network.
Risk	The remote access system may bypass the normal internal network and may allow security breaches to occur purposely or non-purposely. The rule may

	also stop the client from receiving full functionality that they should receive when using the remote access network.
Compliance	Assure that the firewall rules or the router tables function correctly and isolate the remote access network from the internal local area network. The activity should be logged and monitored and confirmed.
Testing	Access the network remotely and test the functionality of the remote user by making sure they can use the services that are guaranteed to them. Also, try to bypass controls on the firewall by trying to use services that are not approved. This can be done by analyzing the firewall rules and firewall logs.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

12. Router/Router Table Security	
Reference	DISA Network STIG, NIST SP-800-26, CIS Benchmark v1.1
Control Objective	Provide logical security for the router from internal and external threats. Also, reducing services and increasing security to increase performance.
Risk	The unsecured router may allow for internal and external persons to attack and take down or negatively affect the router and its performance. Also, the router may not run at peak performance due to extraneous unneeded services running on it.
Compliance	The router should have all extraneous services removed and secured while providing full functionality in its mission. The unit should not be “over secured”.
Testing	Examine the routing table. Whole books are written on how to secure a routing table. A quick way to do this is through use of tools. Run Nmap against the router to find out what services are open and are unneeded. Run RAT from http://www.cisecurity.org against the routing table to see the flaws of the routing table. Run Nessus using the Cisco plug-ins to assess the routers penetration weaknesses. For the AS5300, be sure that ACL's are used for access to the router, services such as finger are disabled, small servers are disabled, http server is disabled and enable secret is set.

Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.
----------------------	--

13. ACS Host Server Security	
Reference	DISA Network STIG, NIST SP-800-26, http://www.cisecurity.org , http://www.microsoft.com , http://www.sans.org
Control Objective	Secure the host operating system that the ACS server resides in from internal or external persons wishing to do malcontent.
Risk	The host system running the ACS service could be compromised rendering the remote dial-in system useless due to the lack of the functioning ACS counterpart.
Compliance	Assure that the system hosting the ACS services is secured as well as possible.
Testing	Using the checklists provided by Microsoft, Cisecurity and SANS, audit the host operating system and note the problem areas. Run Microsoft's Minimum Security Baseline tool against the operating system to check for vulnerabilities and non-patches holes. Securing an operating system is an extremely long process but basic concepts such as minimizing services and using ACL's still apply. It is imperative to cover the "big fish" before getting too granular. Check to see if the host is in a Windows domain. The Cisco ACS services do not require the host operating system be a Domain Controller but the host must reside on a Domain.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

14. ACS Group Settings	
Reference	Hands on Security Knowledge
Control Objective	To control users by using groups instead of configuring individual users and controlling the security through them and reducing administrative overhead.
Risk	By configuring the remote access network to use individual users, administration becomes extremely tedious and hard to manage, never less time consuming. Due to the high administrative overhead, user configurations could be mishandled allowing for a security breach.

Compliance	The ACS Group Settings should be configured to only allow 1 individual session per user. Enabling call back and using static IP address is preferred and DHCP should be maintained through a separate system, not the AS5300 router. Users should be setup in groups according to their function or organizational group if access is different where applicable.
Testing	Check the configuration the ACS server and confirm that only 1 session per user is set. Also, note the DHCP server being used if static IP addresses are not using and also note the call back settings. Make sure that users are in separate groups that divide them by their functions or roles that they play in the organization. Be sure to check several user accounts in the User Setup tab to ensure they are set use Group Authentication.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

15. ACS Network Configuration

Reference	Hands on Security Knowledge
Control Objective	Assure that the AS5300 only allows inbound connections.
Risk	Allowing users to dial out through it and possibly bypassing internal security controls may exploit the agency's LAN by users dialing out through the system and adopting Trojans, viruses and other malicious damage since there are no controls in place to combat it.
Compliance	Assure that the system has only inbound configured in the ACS menu.
Testing	Go into the ACS Network Configuration tab and choose the AAA servers tab and confirm that the machine is set for inbound only.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective areas.

16. NTP Configuration

Reference	Hands on Security Knowledge, http://www.cisecurity.org
Control Objective	Assure that the AS5300 and ACS server are synched by running the NTP (Network Time Protocol) service.

Risk	Systems that do not possess the correct time will give you incorrect information when you try to troubleshoot problems on them or attempt to audit them, especially when a security breach has occurred and time is of utmost importance.
Compliance	Assure the AS5300 and the ACS server hosts are updating their system times through a functioning and approved NTP server. In the case that there are more than one approved time servers, be sure to set them to pull from the same time server.
Testing	Check the host ACS is running on inspect it to see if it is updating and from where. Also check the routing table on the AS5300 and confirm that a NTP server is configured and updating from the same NTP server as the ACS server host. Change both system times and monitor to make sure the time is corrected at the time of update.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

17. ACS System Configuration

Reference	Hands on Security Knowledge
Control Objective	Assure that a production CiscoSecure database is being replicated to an approved server over a secure channel.
Risk	If a CiscoSecure database is being replicated, especially over the Internet, persons wanting to do harm can intercept the replication.
Compliance	Assure that the system the CiscoSecure database is being replicated to is an approved server with a valid SSAA and is being encrypted if the data is going over the Internet.
Testing	Check the ACS configuration in the System Configuration/CiscoSecure Database Replication tab and check for replication servers. If there any, check firewall rules that assess its ability to replicate and if they are replicating over a public network, that they replicate over encrypted channels.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

18. Administration Control

Reference	DISA Network STIG, Hands on Security Knowledge
Control Objective	Assure that there are at least two or three administration accounts on the ACS server.

	administration accounts on the ACS server.
Risk	User's accounts and configurations may need to be changed immediately and only the one administrator with access may be unavailable causing downtime and disruption of service for the user. In addition, using a single administrator account that every administrator uses does not give valid audit results.
Compliance	The ACS administration should have at least two administrators that associated with a specific administrator or person.
Testing	In the Administration Control tab, the Access Policy tab should be set to specific IP addresses and to only a specific port. Under the Session Policy tab, the ACS should be configured to a short timeout value, Automatic Login should be disabled, Respond to Invalid IP address connection checked and failed login attempts should be tracked.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

19. Certification and Accreditation	
Reference	NIST SP 800-26, DITSCAP
Control Objective	Assure that the organization's parent authorizes the AS5300 and ACS system and it's management to operate on the organization's network.
Risk	The possibility that the systems are not approved to operate on the agency's network. This prior testing is done to make sure there are no security problems before they are put into the production network. Fixing problems down the road causes extreme amounts of manpower and downtime to fix them and even may result in a total loss of monies that were required to purchase the system in the case it is never approved.
Compliance	The systems should have official documentation that authorizes the systems to reside on the organization's network.
Testing	Review the appropriate C&A (Certification and Accreditation) authorization documentation.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

20. Security and Awareness Training	
Reference	NIST SP 800-26, OSSTMM v20

Control Objective	Assure users have appropriate end user training for Security and Awareness.
Risk	Inappropriate remote access use by untrained people can open many security problems to internal network they are connected to such as virus and Trojans.
Compliance	Provide proof (official documentation) that remote access users have attended annual or bi-annual SATE training.
Testing	Look for official training of remote access users. Also, attempt to social engineer remote access users through the use of phone calls and e-mails asking for things such as their passwords and other personal information.
Objective/Subjective	Objective – The conditions are either met or not and are not applicable to any subjective ideas.

Section 3 - Audit Evidence

1. Contingency Planning	
Procedures Taken	The ACS Configuration was checked for system configuration backups through System Configuration/ACS Backup Scheduling. Logging was checked in the System Configuration/Logging tab to confirm logging was turned on and the log files were existent to be backed up. The router image files were checked for the existence of backups along with the host operating system supporting the ACS server. The backup tapes were checked to assure they were in a locked, fireproof safe.
Conclusion	ACS logging was functioning correctly but no ACS service backups were being run. Dialing in and checking logs updated confirmed logging was functioning. Also, there were no router image file backups or network backups being run on the host operating system that supported the ACS service.
Compliance/Rating	Failure

Figure 5 - ACS Login Screen

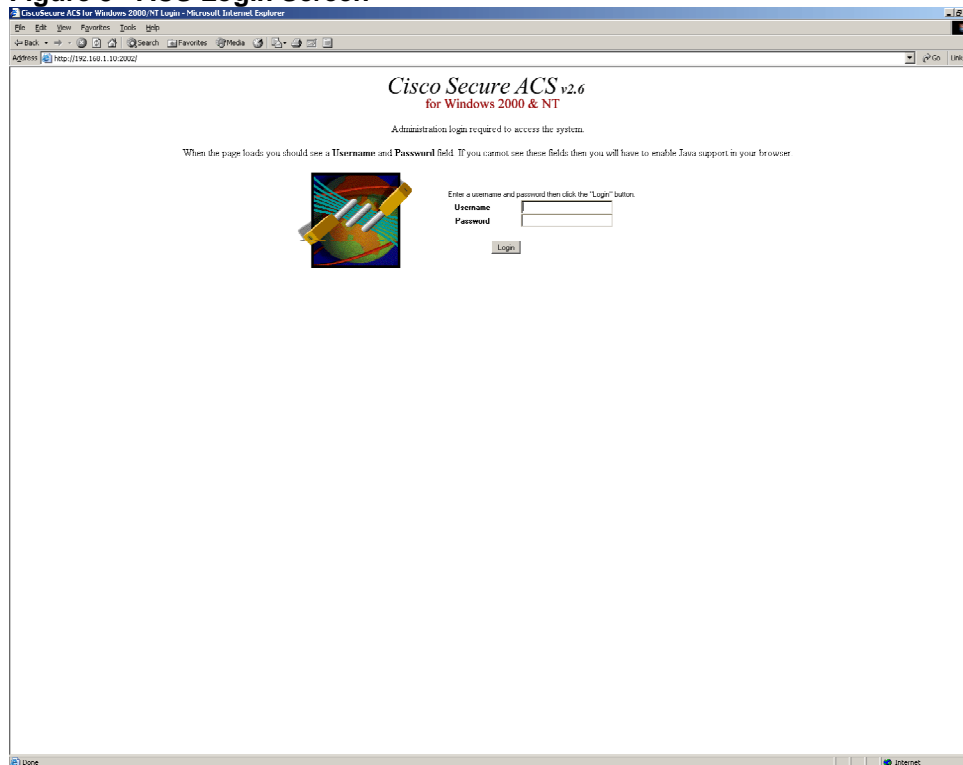
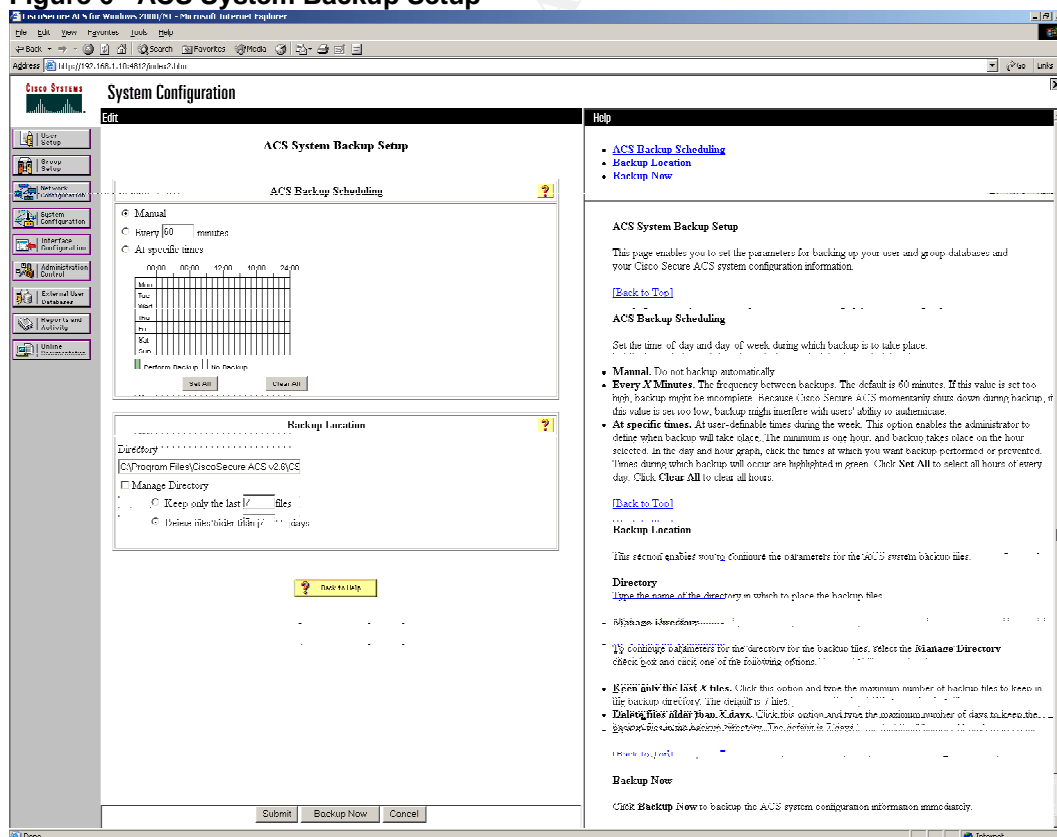


Figure 6 - ACS System Backup Setup



2. Auditing	
Procedures Taken	A laptop was used to dial into the AS5300 and ACS remote access system and confirm that logging was taking place in the correct path that was specified under System Configuration/Logging. Incorrect passwords were entered to ensure that failure logging was working correctly also. The router table was checked to see if logging was enabled on the AS5300 by logging into the router and running the "show running-config" command and assuring that the statement was in the active running-config and startup-config files. The CSTACACS service was stopped on the Windows 2000 host to ensure correct NT auditing was working correctly when the service went into a stopped state.
Conclusion	The ACS server was logging failed attempts and correct logins efficiently and correctly. Logging was enabled on the AS5300 when the "show running-config" command was issued but was configured incorrectly because the server that was specified was not an active log server (192.168.1.15). The CSTACACS service was stopped and the Windows 2000 host correctly logged the event in the event viewer.
Compliance/Rating	Failure

© SANS Institute

Figure 7 - Failed Attempts

Figure 7 displays a screenshot of the CiscoSecure ACS for Windows 2000/NT interface, specifically the "Reports and Activity" section. The browser window shows the URL <http://192.168.1.104/ACS/index.htm>.

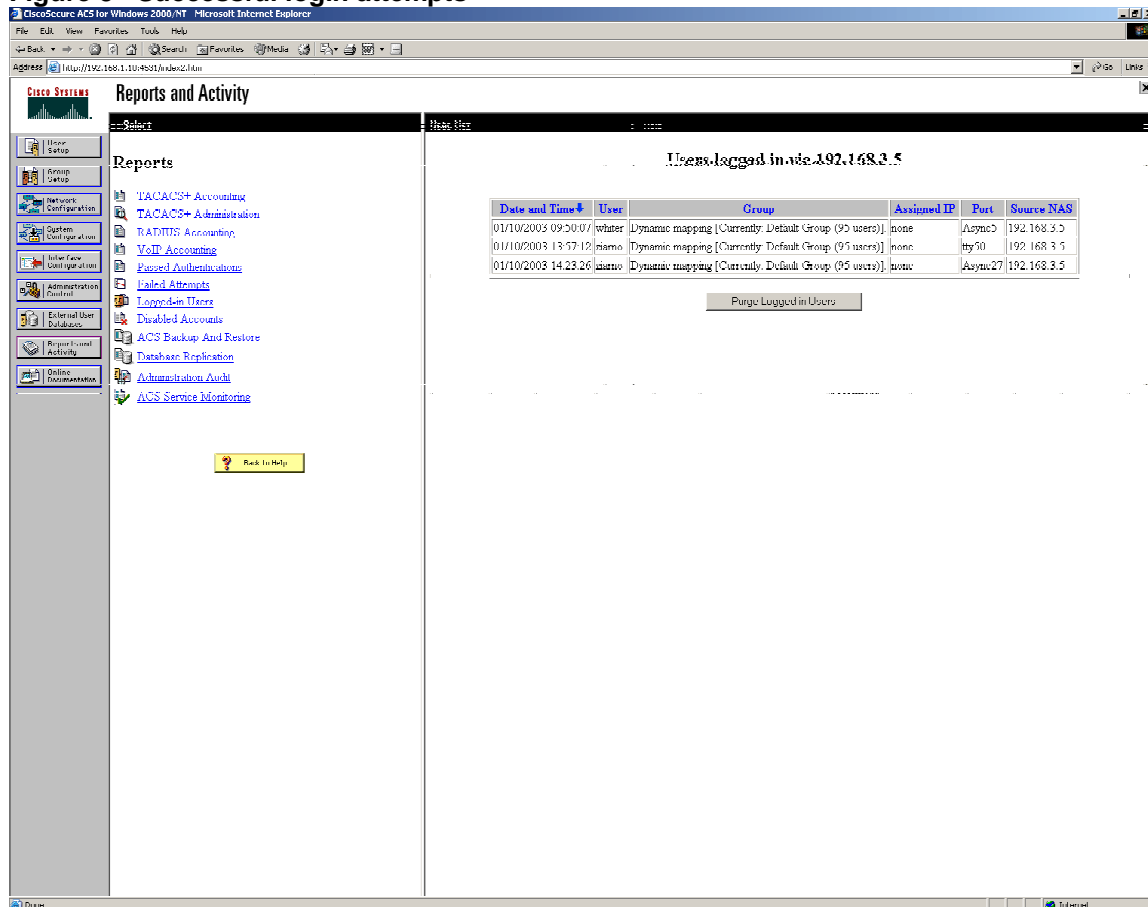
The interface is divided into two main panes. The left pane, titled "Reports and Activity", contains a "Select" dropdown menu and a list of reports including:

- TACACS+ Accounting
- TACACS+ Administration
- TranSTIS Accounting
- VoIP Accounting
- Failed Authentications
- Lopped-in Users
- Disabled Accounts
- ACS Backup And Restore
- Database Replication
- Administration Audit
- ACS Service Monitoring

The right pane, titled "Failed Attempts active.csv", displays a table of failed authentication attempts. The table has the following columns: Data, Time, Message-Type, User-Name, Group-Name, Caller-ID, Authen-Failure-Code, Authen-Failure-Code, Authen-Data, NAS-Port, and NAS-IP-Address.

Data	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Authen-Failure-Code	Authen-Data	NAS-Port	NAS-IP-Address
01/10/2003	14:14:42	Authen Failed	ziarno	Default Group	7036966228/7036965269	External DB user invalid or bad password	Async24	192.168.3.5
01/10/2003	14:12:49	Authen Failed	ziarno	Default Group	7036966228/7036965269	External DB user invalid or bad password	Async22	192.168.3.5
01/10/2003	13:57:06	Authen Failed	ziarno	Default Group	192.168.1.154/	External DB user invalid or bad password	my10	192.168.3.5
01/10/2003	09:17:57	Authen Failed	schlossberg	Default Group	7033235670/7036965269	External DB user invalid or bad password	Async6	192.168.3.5

A "Back to Help" button is visible at the bottom of the left pane.

Figure 8 - Successful login attempts**Figure 9 – The Running Config on the ACS Server (Auditing and Authentication)**

```

AS5300#show running-config
Using 2467 out of 126968 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname AS5300
!
logging buffered 10000 debugging
no logging console
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default tacacs+
aaa authorization exec default tacacs+
aaa authorization network default tacacs+
aaa accounting exec default start-stop tacacs+
aaa accounting network default start-stop tacacs+
enable secret XXXXXXXXXXXXXXXXXXXXXXXXXXXX

```



```
enable password XXXXXXXX
!
username user password 0 passwd
ip subnet-zero
!
async-bootp dns-server X.X.X.X X.X.X.X
async-bootp nbns-server 192.168.1.15
isdn switch-type primary-5ess
mta receive maximum-recipients 0
!
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
controller T1 1
shutdown
clock source line secondary 1
!
controller T1 2
shutdown
!
controller T1 3
shutdown
!
!
!
interface Loopback0
no ip address
no ip directed-broadcast
!
interface Ethernet0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0:23
ip unnumbered Ethernet0
no ip directed-broadcast
dialer rotary-group 1
dialer-group 1
isdn switch-type primary-5ess
isdn incoming-voice modem
no cdp enable
!
interface FastEthernet0
ip address 192.168.3.5 255.255.255.0
ip directed-broadcast
no ip route-cache
no ip mroute-cache
duplex full
!
interface Group-Async1
ip unnumbered FastEthernet0
```

```
ip helper-address 192.168.1.15
ip directed-broadcast
encapsulation ppp
no ip route-cache
ip tcp header-compression passive
no ip mroute-cache
async mode interactive
peer default ip address pool setup_pool
no cdp enable
ppp authentication pap
group-range 1 48
hold-queue 10 in
!
interface Dialer1
no ip address
no ip directed-broadcast
no cdp enable
!
ip local pool setup_pool 192.168.3.10 192.168.3.50
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
no ip http server
!
logging trap debugging
logging 192.168.1.15
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
tacacs-server host 192.168.1.10 single-connection
tacacs-server timeout 10
tacacs-server key XXXXXXXX
!
line con 0
exec-timeout 0 0
logging synchronous
login authentication no_tacacs
transport input none
line 1 48
autoselect during-login
autoselect ppp
modem Dialin
line aux 0
line vty 0 4
exec-timeout 20 0
password XXXXXXXX
!
scheduler interval 1000
end

AS5300#
```

3. Authentication	
Procedures Taken	Logging into the network with incorrect passwords was attempted. Policies and procedures were reviewed that were applicable to how clients will authenticate remotely. The auditor attempted to log into the laptop that was used for testing with standard accounts such as administrator and guest. The Cisco ACS server was checked in the System Configuration/Password Validation tab for complexity settings along with the Windows domain user account password policies that were existent on the domain. The auditor attempted to change the user password used during the audit to a non-complex password and test results.
Conclusion	The auditor was unable to login to the network remotely with incorrect passwords. The auditor also tried to login to the laptop through the use of standard Windows accounts. The Cisco ACS server was not set to use complexity but the Windows 2000 domain accounts were. Since the client doesn't use the CiscoSecure database, the complexity did not apply. The client does not use at least two-factor authentication. The auditor was unable to change the user account password to a non-complex password.
Compliance/Rating	Failure

© SANS Institute

Figure 10 - Cisco Secure Complexity

System Configuration

Edit

Password Validation Options

Password length between and characters

☐ Password may not contain the username

☐ Password is different from the previous value

☐ Password must be alphanumeric

[Back to Help](#)

[Submit](#) [Cancel](#)

Help

- [Password length between X and Y characters](#)
- [Password may not contain the username](#)
- [Password is different from the previous value](#)
- [Password must be alphanumeric](#)

Password length between X and Y characters

Type the minimum and maximum number of characters that you want to require for the user's password, or leave the numbers set to the default of 4 and 32 characters.

[Back to Top](#)

Password may not contain the username

Select this check box to require that the user's password does not contain the username anywhere within it.

[Back to Top](#)

Password is different from the previous value

Select this check box to require the user's new password to be different from the previous password.

[Back to Top](#)

Password must be alphanumeric

Select this check box to require the user's password to contain both letters and numbers.

[Back to Top](#)

[Section Information](#)

4. Remote Access Security

Procedures Taken	The administrator checked the physical security of the remote users laptop, checking specifically for locks and BIOS passwords. The laptop was checked for a configured firewall and anti-virus software that was configured and updated. The laptop was also checked for local file encryption and file integrity software. Additionally the laptop was checked for the Active X and Java settings in its installed browser and the type of case the machine was in. Lastly, the administrator checked for supporting remote access user policies and procedures.
Conclusion	There was no encryption running on the laptop nor was their integrity checker software installed. The laptop was located in a leather laptop bag with the client's logo on it and Internet browser controls were not enabled. The laptop did not have a BIOS password set or a lock implemented. The laptop

	had no local firewall running but did have an updated and configured Norton Anti-virus software running. There were no written remote access use policies and procedures implemented.
Compliance/Rating	Failure

5. Systems Management

Procedures Taken	Research was done to find out if any type of management software was being used in conjunction with the AS5300 and the ACS Server. The router table was checked for the existence of logging and if SNMP was configured on the router. The AS5300 was also checked to check to see if in band or out-of-band management was being used.
Conclusion	The process of managing the system and its performance was non-existent. SNMP was not enabled on the router for use of management. The AS5300 also was being configured through in band management only. Modem performance was being checked once a week manually by running the show modem command when in enable mode. Modems were not functioning at 100 percent capabilities
Compliance/Rating	Failure

© SANS Institute 2003

Figure 11 - Show Modem Statement in Enable Mode

[illegible]

6. Firewall Review

Procedures Taken	Remote access was gained on the laptop and full network functionality was checked. Services such as FTP and HTTP were checked for validity plus general network script and file access. Non-approved services were also checked. In this instance we attempted to use Instant Messenger. The firewall rules were checked to assure remote users were isolated in the rule base.
------------------	---

Conclusion	Full functionality was gained to the network remotely including HTTP access and file access. Network mapping scripts ran correctly when the user logged into the domain. The firewall logged the activity correctly. The firewall rules were reviewed and it confirmed that remote access users had full access to the internal corporate network. Non-approved services, such as Instant Messenger in this case, also were denied correctly.
Compliance/Rating	Pass

Figure 12 -Clients going to the Domain Controllers for scripts

8	NetworkHosts NetworkDialin NetworkUsers NetworkUsers2	DC2 DC1	Any	accept	Short	Gateways	Any
9	NetworkHosts NetworkDialin NetworkUsers NetworkUsers2	DC2 DC1	Any	accept	Short	Gateways	Any

Figure 13 - Remote users being blocked from various dangerous services

15	NetworkDialin NetworkHosts NetworkUsers NetworkDMZ NetworkTest NetworkHosts2	ICQ AOL-IM Yahoo-IM MSN	Any	drop	Short	Gateways	Any
16	NetworkUsers NetworkDialin NetworkHosts NetworkDMZ NetworkTest NetworkUsers2 NetworkHosts2	Any	AOL NFS pcANYWHERE Napster pop SunRPC Gnutella ICQ Port Yahoo Port SOCKS	drop	Short	Gateways	Any

Figure 14 - Remote users having full access to the internal network

32	NetworkUsers NetworkDialin NetworkHosts NetworkDMZ NetworkTest NetworkUsers2 NetworkHosts2	NetworkDMZ NetworkBlaze NetworkHosts NetworkDialin NetworkUsers2 NetworkHosts2	Any	accept	Short	Gateways	Any
----	--	---	-----	--------	-------	----------	-----

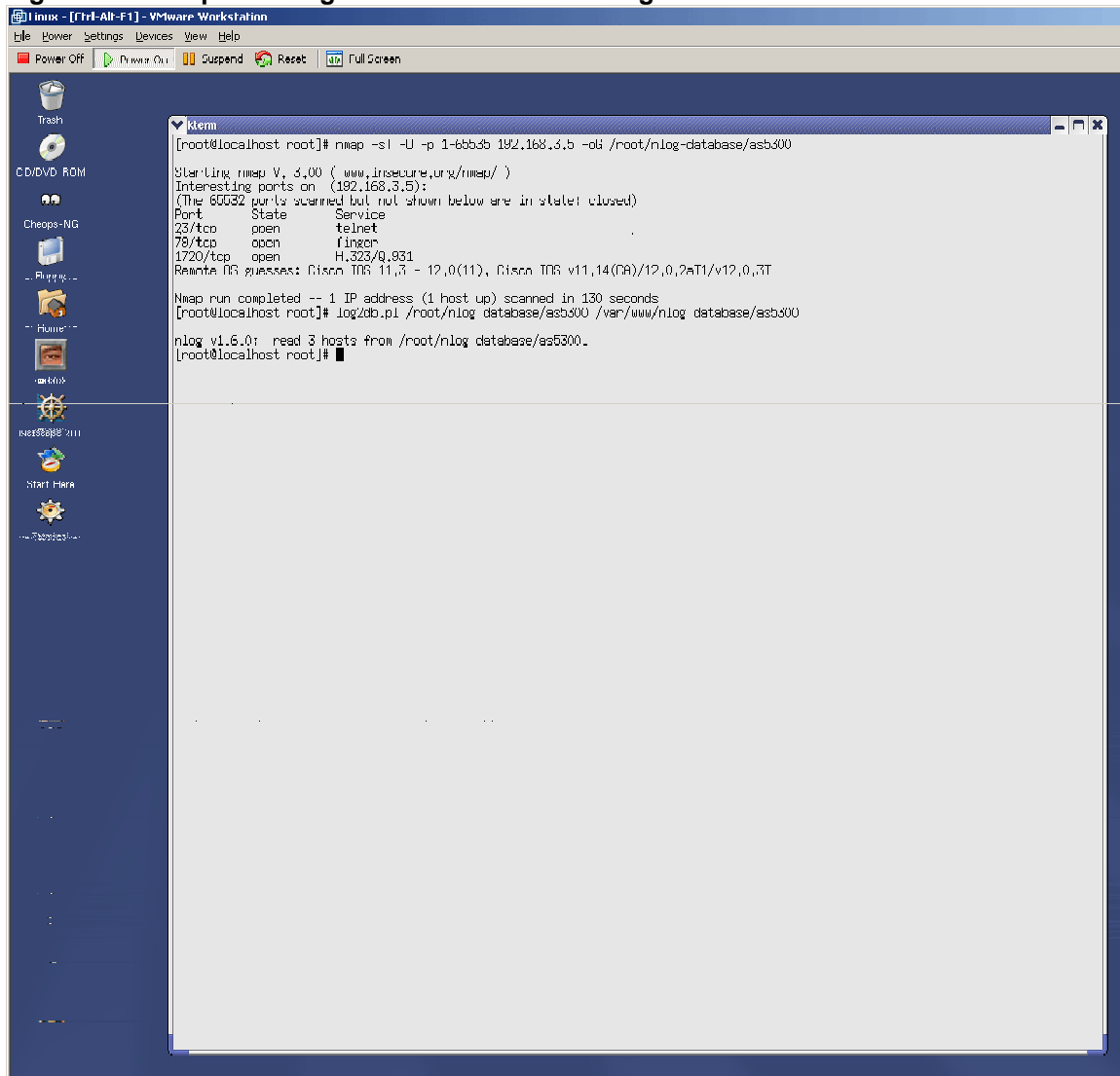
Figure 15 - Remote user being accepted and blocked on firewall log

3966546	13Jan2003	12:04:45	E190... GW	log	accept	http	ziarnolaptop
3966632	13Jan2003	12:04:53	E190... GW	log	drop	ICQ-Port	ziarnolaptop

7. Router/Router Table Security

Procedures Taken	Nmap was run against the AS5300 routers IP address with the command: nmap -sT -O -p 1-65535 -v 192.168.3.5 -oG /root/database/as5300 to collect what ports are currently running on the device and spit it out to a log file that we can convert using nLog. After putting the Nmap data into the Nlog data for future use, RAT was run on the AS5300 router table to test for router table vulnerabilities with the command rat 192.168.3.5 and generated the as5300.html file that noted the vulnerabilities. Nessus was then ran against the router to check for penetration vulnerabilities.
Conclusion	The router was found to have a couple of vulnerabilities. Firstly, the router did not have ACL's that were being used for telnet access to protect who was access it. Also no line passwords for the vty connections so a person could not access the lines without being prompted nor were the passwords required to be encrypted. There were also no exec timeouts set on the router. Direct broadcast was not disabled along with ip proxy-arp. Nessus output instructed finger service as a vulnerability along with Telnet and general TCP, UDP and ICMP statements.
Compliance/Rating	Failure

© SANS Institute 2003

Figure 16 - Nmap and Nlog Statement Commands against router

The screenshot shows a Linux terminal window titled "Linux - [Ctrl-Alt-F1] - VMware Workstation". The terminal is running as root on localhost. The user enters the command `nmap -sI -U -p 1-65535 192.168.3.5 -oG /root/nlog-database/asb300`. The output shows Nmap version 5.00, scanning 192.168.3.5, and finding open ports 23/tcp (telnet), 79/tcp (finger), and 1720/tcp (H.323/Q.931). The user then enters `nlog v1.6.0: read 3 hosts from /root/nlog database/asb300`, and the output shows the hosts read from the database.

```
[root@localhost root]# nmap -sI -U -p 1-65535 192.168.3.5 -oG /root/nlog-database/asb300

Starting nmap V. 5.00 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.3.5):
(The 65532 ports scanned but not shown below are in state: closed)

```

Port	State	Service
23/tcp	open	telnet
79/tcp	open	finger
1720/tcp	open	H.323/Q.931

```

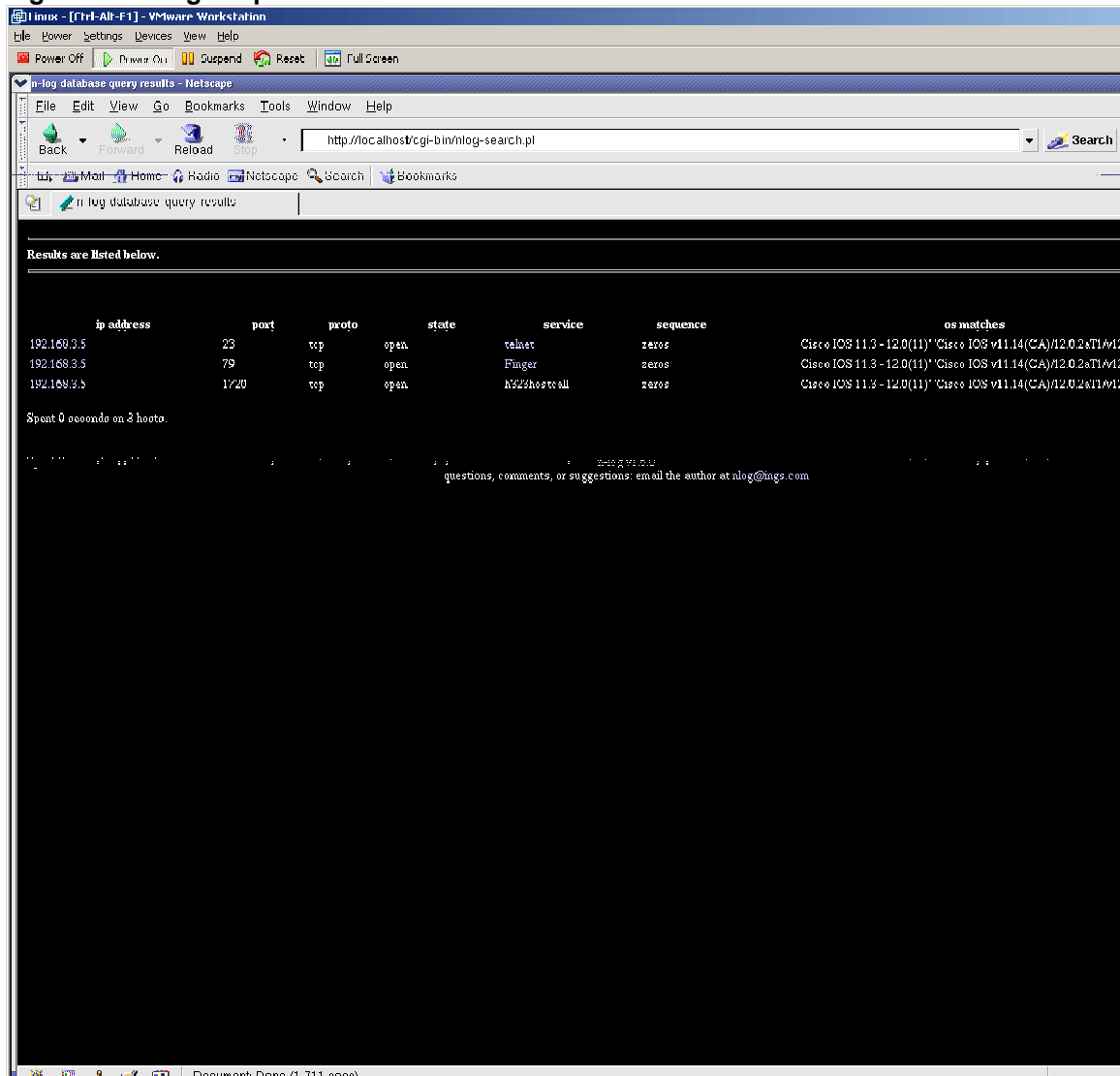
Remote OS guesses: Cisco IOS 11.3 - 12.0(11), Cisco IOS v11.4(9A)/12.0.2aT1/v12.0.3T

Nmap run completed -- 1 IP address (1 host up) scanned in 130 seconds
[root@localhost root]# log2db.pl /root/nlog database/asb300 /var/www/nlog database/asb300

nlog v1.6.0: read 3 hosts from /root/nlog database/asb300.
[root@localhost root]#
```

© SANS Ins

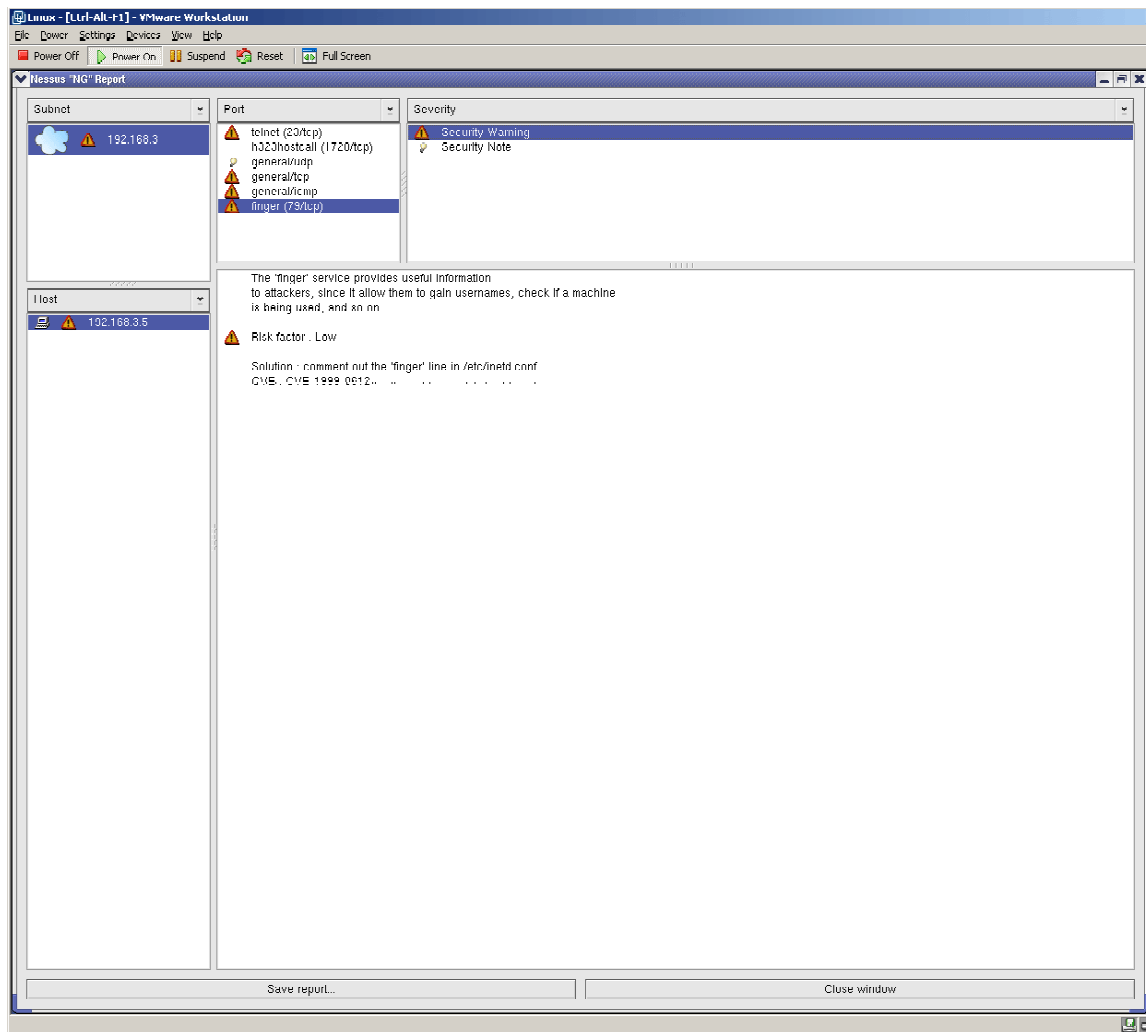
Figure 17 - Nlog Output of Router



© SANS Inst

Figure 17 - RAT Output of Router Vulnerabilities

[illegible]

Figure 19 - Nessus Output of Router – Finger Vulnerability

8. NTP Configuration	
Procedures Taken	The router table and the ACS server were examined to see if they were updating from a NTP server.
Conclusion	The router table showed no NTP server settings configured on it. When looking at the ACS server, the server was running on a Windows 2000 server in a Windows 2000 domain. By default, Windows machines on a Win2K domain get their time from the Domain Controllers. The time was changed and evaluated if it changed back after reboot and it did. The time on the ACS server was perfectly synchronized with the domain controller but the

	router time was not synchronized with the ACS server. The router command show clock was issued and it was noted that the router was over three years behind.
Compliance/Rating	Failure

9. Administrative Control

Procedures Taken	The Administration Control Tab/Access Policy IP address ranges were evaluated to check for IP address access to the ACS server along with port access. Under the Administration Control/Session Policy Tab, the Session Configuration attributes were evaluated for short timeout values and the disabling of automatic login. Responses to invalid IP connections were noted along with failed login attempts. The check for the minimum of two or more administrators was implemented.
Conclusion	There was only one administrator that was specified therefore making it near impossible to track who makes changes to the ACS server. Failed login attempts were also not being tracked. Since there was only one administrator, that account had full menu functionality and control, never less allowing anyone with access to the computer to make any kind of change. Automatic login was enabled allowing anyone in the computer room to also have access to changing the ACS settings that was locally logged on the machine. Multiple changes were made locally at the console without having to login. Five attempts to login remotely with incorrect passwords never neither showed up in the logs nor locked out the administrator account.
Compliance/Rating	Failure

10. Physical Security

Procedures Taken	Checked the location of the ACS server and the AS5300 router and confirmed it was in a locked and secured location with ample air condition. Assured a valid authorization document resides outside the control with names and contacts of who has official authorization.
Conclusion	The AS5300 and the ACS server were both in a secured state in a locked facility with official documentation that stated authorized individual

	access. Phone calls were made to the person of official contact and that officer confirmed the list. The AS5300, ACS server and firewall were all in rack mounted, locked server cabinets.
Compliance/Rating	Pass

The Residual Risk

The scope of this organization's system was to provide a remote access system that gives the client twenty-four hour remote access to their internal network, modeling their desktop from their laptop. When looking at this type of system the client requires there were remote threat risks such as laptops being compromised along with their passwords and internal threats such as bad configuration management, policies and contingency planning. During this audit many different types of vulnerabilities were found from policy and procedures to actual technical configuration issues.

After reviewing the twenty checklist steps we used for our audit, it was found that most of the vulnerabilities found could be fixed with no purchase costs to the client. The costly part of eliminating the risks would be the man-hours that would be involved to fix them and maintain the solutions. The audit proved that the client's solution truly gave them what they functionally needed but they didn't meet many of the security aspects of the remote access solution.

Audit failures they incurred such as the lack of contingency planning, life cycle management and policies and procedures take time to configure and draft up but need to be done in order to enforce many of the problems the organization faces. 24x7 support is the only residual risk that is not possible within this environment. The AS5300 router is only capable of using one power supply and one fan. The AS5300 also has only one phone line jack that goes into it and one network cable that goes into the local area network. If any of these fail, there is no way to keep the guaranteed 24x7 support unless another standby unit was implemented. The customer would be required to move to another solution, especially because the AS5300 is at its end of life cycle.

Is the system auditable?

The AS5300 remote dial-in environment is highly auditable. During the testing phases of the checklists that were obtained, each test was objective. These objective tests gave us the ability to recreate the audit process easily and repeatedly if need be. It is possible to go to any other AS5300 remote access system in an organization and repeat the same steps and come up with similar, precise results.

During the audit of this environment, many of the policies and procedures were missing. For example, there were no laptop policies for users nor were there contingency planning or life cycle policies and procedures available. In this

respect, it is not possible for us to audit something we do not have. If there were policies in place we could have audited the policy for precise documentation. The missing policies and procedures are the missing audit part of this system.

Section 4 – The Audit Report

Executive Summary

During this audit process the client's Cisco remote access network was evaluated. The Cisco remote access network was a combination of an AS5300 Network Access Server and a Cisco Secure Access Control server. The two systems were separated by a Checkpoint FW-1 Firewall, which passed all of the two systems traffic.

The audit objectives for these three main components on the client's remote access network were successful. The first objective of the audit was to analyze the managerial issues that were involved with the systems such as policies and procedures. The goal was to see if they were in place and being followed by the client. The second objective was to analyze the technical findings on each part of the system that affected or could affect the client's functionality.

The remote access system was fully functional to the client. Each system integrated well and provided every service they needed to meet their business objectives. The client was able to do work just as residing on the corporate internal local area network.

The major findings during the analysis of the audit of the system were the lack of policies and procedures in all areas excluding password complexity in the Windows 2000 domain. These policies and procedures are crucial in keeping and maintaining a high level of security among systems. The systems also had many technical security problems associated with them and could not uphold true 24x7 support, which the client required for successful accomplishment of its business objective.

Audit Finding 1 – Contingency Planning (Page 27)

The client possesses no contingency planning policies and procedures associated with either of the two systems and do not perform any backups of any kind on either system. Neither system is fault tolerant for 24x7 support.

Background/Risk

In the case the administrator would lose the ACS or AS5300 configuration's due to some type of outage on the machine, they will lose all of their user databases along with all configuration settings and audit logs. By losing all of the systems configuration settings, a new system would have to be rebuilt and then reconfigured causing wasted man-hours and system and productivity downtime.

Audit Recommendations

It is recommended that the AS5300 and ACS servers be backed up with some type of operating system specific or third party backup software. It is also recommended that the AS5300 router images be transported via TFTP to a server for backup access. Policies and procedures should be drafted and implemented that state what the policy is when backing up systems, such as how many times a week and what type of backup and how to do them. These preventive measures can allow for quick rebuild of a system in the case of wrong configuration problems or physical breakdown of the actual equipment. It is also recommended to look into a different dial in solution that fault tolerant for both systems to provide true 24x7 support.

Costs

The costs for implementing a fully fault tolerant system would be exceptionally high due to the need to by another AS5300 router solution. Being there are many remote access solutions, we can't pinpoint an exact cost. The client already possesses a Computer Associates backup system software and the accompanying tapes for it. The costs are the man-hours to draft and implement the policies and procedures, which would be approximately two hours.

Compensating Controls

There are no compensating controls for the client.

Audit Finding 2 – Auditing (Pages 29-33)

The ACS server is successfully auditing all events on the ACS server such as user failures and logins. The shortfall is that the client has no policies and procedures that require administrators of the systems to check the audit logs therefore increasing their security risks. The audit logs are good tools as long as they are being used. The AS5300 router is not logging because the client does not posses a log server therefore any activity such as router reboots or images uploads are not being logged.

Background/Risk

Without functional auditing working on the AS5300 server, the router could incur security attacks to it without any administrators knowing about it possibly causing a non-functioning router ending in lack of productivity for the client. The router could also be physically down and without the use of log servers, the only way administrators will knows its down is when a client calls and let's them know of the problem. No logging and auditing forces the administrators to work on systems in a reactive state and not a proactive state.

Audit Recommendations

It is recommended that the client implement policies and procedures that require administrators to review audit logs on the AS5300 and ACS servers. It is also recommended to implement some type of logging server. By implementing these

policies and procedures it renders the administrators to be proactive and be able to respond to remote access problems, such as a user's password being locked, in a timely and fashionable manner increasing productivity.

Costs

The costs for implementing these recommendations are minimal. The cost is the drafting of the policies and procedures and the man-hours to review the audit logs, which is approximately one hour a day. The syslog server would require the license for the operating system, hardware and software. Many flavors of UNIX are free and offer free syslog servers.

Compensating Controls

There are no compensating controls.

Audit Finding 3 – Authentication (Page 34-35)

The clients authenticated to the network through complex passwords but lacked two-factor authentication along with authentication corporate policies.

Background/Risk

When authenticating without the use of two or three factor authentication, if the password of the user is compromised, they will have full access to the corporate local area network.

Audit Recommendations

Implement two or three factor authentication into the authentication policy of the organization.

Costs

The cost of two-factor authentication would require the purchase of a device such as a key fob or smart card. These prices vary along with the software that is required depending on what vendor the client would choose.

Compensating Controls

There are no compensating controls.

Audit Finding 4 – Remote Access Security (Page 35)

The client does not possess remote access policies and procedures for end users. The client also does not implement alternate security controls such as encryption, firewalls and file integrity checkers.

Background/Risk

Insufficient security controls and inappropriate use of laptops due to the lack of organizational policies open the agency to a high amount of security risks that could compromise the remote system and the corporate internal LAN causing productivity and monetary loss.

Audit Recommendations

Implement file integrity checkers, firewalls, BIOS passwords and other security controls on laptops. It is also recommended to draft up formal policies and procedures that users are required to sign before the use of remote access laptops. It also should be ensured that the laptop bag is an inconspicuous bag that does not share what agency it belongs too.

Costs

The client is a member of the Air Force DoD, which owns a site wide license for Norton Personal firewall. There are free file integrity checkers that are available on the Internet. Implementing BIOS passwords on laptops is free of charge and the organizational logo is a sticker, which cannot be easily removed. The cost incurred would be the man-hours to achieve this.

Compensating Controls

There are no compensating controls.

Audit Finding 5 – Systems Management (Pages 36-37)

The client does not implement systems management on either the ACS or AS5300 servers nor do they possess policies and procedures that cover the requirement of systems management on the systems.

Background/Risk

Without the use of systems management on either of the systems, the client cannot be proactive to system dial-in problems for remote clients. System performance, network problems and hardware problems cannot be detected and put the client in a reactive mode causing productivity loss to the end user.

Audit Recommendations

It is recommended that the client implement SNMP management on the AS5300 and ACS servers. The drafting of the policies and procedures will help in the implementation of this.

Costs

The client already owns site licenses for Cisco Works and HP Openview, which are viable products to implement this. The costs are the man-hours needed to implement the solution. This could be done in less than 40 hours.

Compensating Controls

There are no compensating controls.

Audit Finding 6 – Router/Router Table Security (Page 38-43)

The router table was not secured sufficiently. The finger service was turned on and the line connections to the router were not set to timeout. There were no

ACL's set to check Telnet access to the router.

Background/Risk

The lack of excess service reduction causes security risks in this case to the internal network. An internal user or administrator could exploit the router by attacking the finger service. The finger service is not needed in the operation of the AS5300 to operate correctly. The lack of ACL's being implemented on Telnet access allows any person to access the router through Telnet access possibly getting in a corrupting and changing configurations along with finding passwords on the router table if they get enable access. The ACL's are an important part of the security of this router because the client allows in band access to it.

Audit Recommendations

Configure ACL's for in band management access or utilize only out of band management. Also disable any excessive services that are not needed, in this case the finger service.

Costs

There are no costs associated with this.

Compensating Controls

There are no compensating controls.

Audit Finding 7 – NTP Configuration (Page 43-44)

No NTP settings were configured on AS5300 or ACS server and no policies and procedures were in place defining NTP use in the organization.

Background/Risk

In the case that the AS5300 or ACS servers were rebooted or attacked or had other issues such as hardware problems, the logs would all be incorrect making it hard to track the events and when they happened. Also, if the client were using the Cisco Secure database instead of TACACS+, the users login auditing would be incorrect. In the case that the router had a syslog server configured or the systems were using SNMP, all SNMP events would be off time also. This would cause wasted man-hours due to bad configuration procedures.

Audit Recommendations

Configure the AS5300 and ACS server to use the approved NTP server for the agency.

Costs

There are no costs associated with this.

Compensating Controls

There are no compensating controls.

Audit Finding 8 – Administration Control (Page 44)

The Administration Control is configured insecurely.

Background/Risk

Only having one administrator account configured, forces the organization to have only one account that must have full access to the configuration of the ACS server interface. In the case of a misconfiguration, there is no way to track who made the changes because everyone logs in with the same account. In the clients case, there was only one administrator account created so if that person and his or her backup weren't there and clients accounts, for example, became disabled, there would be no way to give them access ending up in a loss of productivity. The way the Administration Control was set, anyone on any port could connect to the server and failed logins were not being tracked. All of these configurations cause change control management problems and possible downtime

Audit Recommendations

Configure the ACS server to have multiple administrators with specific rights for each, making sure there is appropriate segregation of duties. All of the duties should have a backup administrator and the accounts should overlap. It is recommended that the accounts have failed login attempts tracked and that only certain IP address are allowed to connect at a certain port.

Costs

The costs associated with this risk are the man-hours to configure the settings, which is less than an hour.

Compensating Controls

There are no compensating controls.

List of References

“DoD Information Technology Security Certification and Accreditation Process”, December 30, 1997,

http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdf

“National Information Assurance Certification and Accreditation Process”, April 2000, http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf

“Federal Information Processing Standards”, June 1974

<http://csrc.nist.gov/publications/fips/index.html>

“NISTS Special Publication SP 800-46, Security for Telecommuting and Broadband Communications”, September 2002,

<http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>

“NISTS Special Publication SP 800-12, An Introduction to Computer Security”; October 1995; <http://csrc.nist.gov/publications/nistpubs/800-12/>

“NISTS Special Publication SP 800-26, Security Self-Assessment Guide for Information Technology Systems”, November 2001,

<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>

“Department of Commerce Manual of Security Policies and Procedures”,

<http://www.osec.doc.gov/osy/SECURITYMANUAL/manualecuritypolicies.htm>

Herzog, Pete. “Open Source Security Testing Methodology Manual”, February 2002, <http://www.isecom.org/projects/osstmm.htm>

“NSA Router Security Configuration Guide”, November 21, 2001

The SANS Reading Room, <http://www.sans.org/resources/>

“Federal Information System Controls Audit Manual”, January 1999,

<http://www.gao.gov/special.pubs/ai12.19.6.pdf>

“System Security Authorization Agreement for the Certification and Accreditation of the Agency Computer Center”, April 1997