IT Audit:
Security Beyond the Checklist

Copyright SANS Institute

Author Retains Full Rights

This paper is from the SANS IT Audit site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"20 Critical Security Controls: Planning, Implementing and Auditing (SEC440)"
at http://it-audit.sans.orghttp://it-audit.sans.org/events/

Auditing a Linux Point-to-Point Tunneling Protocol (PPTP) Virtual Private Network (VPN) Server: An Auditor's Perspective

GSNA Practical Version 2.1, July, 2003

Eric Tong

© SANS Institute 2003, Author retains full rights.

Abstract

This paper is submitted as the requirement for a practical in the GSNA certification track. The subject of this audit is a Linux PPTP VPN server that is used in a corporate environment. The VPN server is to enable telecommuters to remotely access the software source code repository on a server in the corporate network. The goal of the practical is to ensure that the VPN server is operating in a reasonably secure state following the industrial best practices.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract

Assignment 1 - Research in Audit, Measurement Practice, and Control 4
1.1 The scope of the audit 4
1.2 Risk Evaluation 4
Administrative Risk 4
Technical Risk 5
1.3 Current State of Practice 7

Assignment 2 - Create an Audit Checklist 8
2.1 Audit Checklist – Administrative 8
Checklist Item CL-ADM1 – Security Policy Documentation 8
Checklist Item CL-ADM2 – Security Awareness Training 8
Checklist Item CL-ADM3 – Security Incident Response 9
2.2 Audit Checklist – Technical – VPN Service 9
Checklist Item CL-VPN1 – Data Confidentiality and Integrity 9
Checklist Item CL-VPN2 – VPN Authentication Protocol Enforcement 11
Checklist Item CL-VPN3 – Policy Enforcement for New Password 13
Checklist Item CL-VPN4 – Policy Compliance for Existing Password 14
Checklist Item CL-VPN5 – VPN Access Control 15
Checklist Item CL-VPN6 – VPN Network Authorisation 15
Checklist Item CL-VPN7 – VPN Configuration Files Permission 16
Checklist Item CL-VPN8 – VPN Authentication Logging 17
2.3 Audit Checklist – Technical – VPN Server Operating System 18
Checklist Item CL-SVR1 – Server Patching Level 18
Checklist Item CL-SVR2 – Server Network Services 18
Checklist Item CL-SVR3 – Server Hardening 19
Checklist Item CL-SVR4 – Server Secure Remote Management 19
Checklist Item CL-SVR5 – Remote Management Configuration Files Permission 20
Checklist Item CL-SVR6 – Server Firewalling 20
Checklist Item CL-SVR7 – Remote Management Logging 21
Checklist Item CL-SVR8 – Server Fail-Safe Configurations 22
Checklist Item CL-SVR9 – Server Vulnerability 22
2.4 Audit Checklist – Technical – VPN Client Workstation Operating Environment 23
Checklist Item CL-CLT1 – Client Workstation Authentication Enforcement .. 23
Checklist Item CL-CLT2 – Client Microsoft Networking Binding 23
Checklist Item CL-CLT3 – Client Firewall and Anti-virus Protection 24

Assignment 3 - Audit Evidence 25
3.1 Audit Evidence 25
Audit Evidence 1/CL-VPN1 – Data Confidentiality and Integrity 25
Audit Evidence 2/CL-VPN2 – Authentication Protocol Enforcement 28

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit Evidence 3/CL-VPN3 – Policy Enforcement for New Password ……28
Audit Evidence 4/CL-VPN5 – VPN Access Control ……29
Audit Evidence 5/CL-VPN6 – VPN Network Authorisation …….. 30
Audit Evidence 6/CL-VPN7 – VPN Configuration Files Permission …… 32
Audit Evidence 7/CL-VPN8 – VPN Authentication Logging …… 32
Audit Evidence 8/CL-SVR2 – Server Network Services …… 33
Audit Evidence 9/CL-SVR6 – Server Firewalling …… 33
Audit Evidence 10/CL-SVR9 – Server Vulnerability …….. 34
3.2 System Auditability …….. 36

Assignment 4 - Audit Report …… …… 37
4.1 Executive Summary …… 37
4.2 Audit Findings …….. 37
4.3 Background / Risk …… 39
4.4 Audit Recommendations …… 40
4.5 Costs …… 40
4.6 Compensating Controls …….. 41

5. References …… 42

© SANS Institute 2003, Author retains full rights.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 1 - Research in Audit, Measurement Practice, and Control

1.1 The scope of the audit

The objective of this audit is to review the current state of security of the corporate VPN service and benchmark against the best practices in the industry. Recommendation for improvement will be provided. This VPN service enables software development telecommuters to remotely access the soft ware source code repository in the corporate network.

The audit will be focused primarily on a PPTP VPN server, including its VPN service server application and its underlying operation system environment. It is also decided that the VPN operating envi ronment of client workstations will be included in the audit. However, full audit of the underlying operating system of the client workstation is out of the scope of the audit.

The VPN server is located within the corporate network which is protected by a hardware based device that acts as both a Network Address Translation (NAT) firewall and a router. The NAT firewall allows unrestricted outgoing traffic to the Internet but allows only incoming VPN traffic to pass through using port -forwarding to the VPN server.

The VPN server is built on a Red Hat 9 Linux distribution running kernel version 2.4.20-18, Poptop PPTP server version 1.1.4 b4 and iptables Firewall which is built -in to the Linux operating system. The VPN client software is built -in to the Windows 2000 or Windows XP operating system.

It is understood that the selected VPN client workstation for this audit exercise is a good representation of the standard corporate laptop or notebook computers environment.

1.2 Risk Evaluation

Administrative Risk

Category	***Threats***	***Impact***	***Exposure***	***Consequences***
Corporate secret	Software source code being stolen.	Very High	Low	Company may lose credibility and revenue. It may even lead to close of business.
Security Policy for the use of VPN	Insufficient and/or unclear security policy.	High	High	Personnel may not understand the security requirements of the company and do not have the guidelines to follow.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Category	*Threats*	*Impact*	*Exposure*	*Consequences*
User Education	Insufficient security awareness training or program..	High	High	Personnel may not have appropriate awareness on security. One of the most common security problem is social engineering where users may give out important corporate private information to hackers unawarely.
Security Incident Response	Lack or insufficient of effective security incident response guideline.	High	High	Personnel may not know how to report and handle security incidents. Appropriate responsive action will be delayed and it may cause additional and unnecessary damage to the company.

Technical Risk

Category	*Threats*	*Impact*	*Exposure*	*Consequences*
Documentation	Lack of or insufficient documentations including baseline configuration, backup/restore procedure, operation procedure, etc.	High	High	System security being compromised due to inappropriate operation of system.
Data Confidentiality and Integrity	Use of inappropriate VPN technology.	High	Medium-Low	VPN traffic data confidentiality and integrity are not ensured. Authentication credential and/or software source code can be obtained by hacker.
Authentication	Use of weak authentication protocol and/or mechanism for VPN access authentication.	High	Medium-High	Intruder can obtain unauthorised access to the corporate network.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Category	*Threats*	*Impact*	*Exposure*	*Consequences*
Authorisation	Lack of effective authorisation capability to control access to internal network resources.	High	Medium	Unable to enforce access control for access to internal network resources. In case of intrusion, intruder can obtain free access to all corporate network resources.
Accounting	Insufficient logging capability.	Medium -High	Medium	Unable to respond to security incidents.
Accounting	Lack of centralised logging facility.	Medium	Medium-High	Delay in respond to security incidents.
Network Security	Corporate network being compromised.	High	High	Unauthorised access to all corporate network resources.
Server Security	VPN server being compromised.	High	Medium	Intruder can compromise VPN authentication credentials and obtain free access to all corporate network resources.
Server Security	VPN server unable to provide service to the VPN users due to security incidents such as denial of service attack.	Medium	Medium-Low	Telecommuters unable to perform their work.
Client Security	VPN client workstation being compromised.	High	Medium	Intruder can potentially piggy - back on the VPN c onnection and obtain free access to all corporate network resources.
Client Security	VPN client workstation unable to connect to the Internet due to denial of service attack.	Low or Medium	Medium	Telecommuters unable to perform their work. It can be more serious if it is executed by sophisticated hackers who are able to hijack the client's IP address in attempt to access the corporate network.
Intrusion Detection	Lack of intrusion detection capability.	Medium -High	High	Intrusion into compromised corporate network, going stealth and undetectable.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.3 Current State of Practice

Initial research on the topic was performed on keywords, *PPTP VPN audit checklist* , using popular Internet search engines such as Google, Yahoo and Alta Vista. There are virtually no useful resources out of the hundred's of the hits returned. A more generic attempt on keywords without *PPTP* does yield a bit more useful information, including some of the previous submitted SANS practical on similar subject.

In addition to the rese arch works that previous students, *Eric Skovfoged*[1], *John Dietrich*[2], *John Blair*[3] and *Dan Strom*[4], had done, the IT Security Guideline [5] developed by the Information Technology Services Department of the Government of the Hong Kong Special Administrative Regi on also provides some hints on generic VPN security:

- Personnel accountability of unauthorised use of client workstation
- Security policy of VPN client
- One-time or PKI authentication
- VPN session inactivity timeout
- VPN session timeout limit
- Split tunneling
- Personal firewall on VPN
- Anti-virus software with up -to-date signature on VPN client

The follow-on research was then focused on PPTP itself. Microsoft is the major player in the definition of PPTP, research on the Microsoft site however does not yield much information.

The following PPTP specific information was found that aided the development of the audit checklist:

- Strength of MPPE encryption protocol (Kevin Townsend [6])
- Authentication Protocol MS -CHAPv2 (Counterpane Internet Security Inc [8, 9])

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 2 - Create an Audit Checklist

2.1 Audit Checklist – Administrative

Checklist Item CL-ADM1 – Security Policy Documentation

Checklist Item	CL-ADM1
Control Objective	Ensure policy, baseline, guideline and/or procedure documentation are sufficient and in place for the use of VPN remote access system.
Risk	Absence or lack of clear policy, baseline, guideline and/or procedure will put the company in great risk as personnel will not understand the position of the company as well as their expected behaviour in using the VPN service. These documents also serve a very important role as the baseline of the audit to be conducted. *Importance*: High *Likelihood*: High
Compliance	Written documentation should be in place regardless its formality, it can be a formal document or a company memo or note, etc. Policy and baseline should state explicitly the position of the company on the specific system and/or the subject matter. Guidelines and procedures should present clearly handling of the specific system and/or the subject matter.
Test	Determine if the provided documentation is sufficient and rational. Interviews with appropriate personnel such as security manager may be required to determine if there exists any non-written policy, baseline, guideline and/or procedure.
Subjective / Objective	The compliance is subjective as the rationale may vary with different companies as well as the auditor's experience.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-ADM2 – Security Awareness Training

Checklist Item	CL-ADM2
Control Objective	Ensure security awareness training or information are sufficient and effective.
Risk	Absence or lack of personnel security awareness will put the company in great risk. One of the most common security problem is social engineering where users may give out important corporate private information to hackers. *Importance*: High *Likelihood*: High

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-ADM2
Compliance	Written documentation must be in place regardless its formality, it can be a formal document or a comp any memo or note, etc.
Test	Determine if there is sufficient and rational training and/or information readily available to personnel. Interviews with administrative personnel may be required if documentation is insufficient.
Subjective / Objective	The compliance is subjective as the rationality may vary with different companies as well as the auditor's experience.
Reference	Best practice in the industry and personal experience.

Checklist Item CL -ADM3 – Security Incident Response

Checklist Item	CL-ADM3
Control Objective	Ensure security incident response guideline and/or procedure documentation are sufficient and in place.
Risk	Absence or lack of clear guideline and/or procedure will put the company in great risk as personnel will not know how to repor t and handle security incident. Appropriate responsive action will be delayed and it may cause additional and unnecessary damage to the company. *Importance*: High *Likelihood*: High
Compliance	Written documentation must be in place regardless its formality , it can be a formal document or a company memo or note, etc.
Test	Determine if the provided documentation is sufficient and rational.
Subjective / Objective	The compliance is subjective as the rationality may vary with different companies as well as the auditor's experience.
Reference	Best practice in the industry and personal experience.

2.2 Audit Checklist – Technical – VPN Service

Checklist Item CL -VPN1 – Data Confidentiality and Integrity

Checklist Item	CL-VPN1
Control Objective	Ensure the encry ption in use for VPN data confidentiality and integrity is in compliance with the corporate standard.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN1
Risk	The VPN traffic can be intercepted by hackers on the Internet. Hackers can obtain authentication credentials and valuable data if the VPN traffic is not encrypted. The corporate standard encryption for VPN use is Microsoft Point - to-Point Encryption (MPPE). It is considered weak compare to today's security technology [6]. Hence there is certain risk even though MPPE is in place for VPN access. *Importance*: High *Likelihood*: High
Compliance	128-bin MPPE is used and enforced for VPN session.

© SANS Institute 2003, Author retains full rights.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN1
Test	On the VPN server, verify if 128 -bit MPPE is enabled in the PPTP configuration file: 1) Examine the file */etc/ppp/options.pptpd* to ensure the *require-mppe* option exists and is not commented out; 2) Examine the file */etc/ppp/options.pptpd* to ensure *+mppe-40* option either does not exit or is commented out; 3) At root prompt, verify if MPPE is loaded on the system by: *# modprobe ppp-compress-18* 4) Turn on a network sniffer to c apture VPN network traffic; On a VPN client, use the provided VPN authentication testing account: 5) Verify if VPN connection attempt FAILED with encryption not required or optional; 6) Verify if VPN connection attempt with *Maximum Strength Encryption* can be established to the VPN server successfully; On the VPN server: 7) Verify if the following message is found in the system log file */var/log/messages*: *July 01 10:13:18 black pppd[5518]: MPPE 128 -bit stateless compression enabled* 8) Examine if plaintext authenticat ion credential information can be found in the captured VPN traffic packet; On the VPN client: 9) Ping an internal server: *C:\>ping xxx.xxx.xxx.xxx* 10) Examine if any ICMP *echo-request* or *echo-reply* data as a result of the ping command can be found in the capture d VPN traffic packet.
Subjective / Objective	Objective.
Reference	RedHat 9.0 HOWTO [12] and personal experience.

Checklist Item CL -VPN2 – VPN Authentication Protocol Enforcement

Checklist Item	CL-VPN2
Control Objective	Ensure the authentication protocol in use for VPN authentication is in compliance with the corporate standard.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN2
Risk	The VPN access is subjected to attack by hackers on the Internet. Hacker can attempt to access the corporate network by compromising weak authentication protocols. The following authentication protocols are considered to be weak: Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP), Challenge Handshake Authentication Protocol (CHAP) and Microsoft Challenge Handshake Authentication Protocol (M S-CHAP) version 1. Automated hacker tools are readily available to launch brute -force attacks to compromise PAP and sniff MS -CHAPv1 authentication credentials. The standard authentication protocol for VPN use is Microsoft Challenge Handshake Authenticati on Protocol version 2 (MS -CHAPv2). Although it is better than the protocols mentioned above, it is considered weak in today's security technology [8, 9]. Hence there is certain risk even though MS -CHAPv2 is in place for VPN access. *Importance*: High *Likelihood*: High
Compliance	The corporate standard authentication protocol MS -CHAP version 2 only must be enforced for VPN authentication.

© SANS Institute 2003, Author retains full rights.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN2
Test	Verify if MS-CHAPv2 is enabled and is the sole authentication method allowed in the PPTP configuration: 1) Examine the file */etc/ppp/options.pptpd* to ensure *require-mschap-v2* option exists and is not commented out; On the VPN client, with *Require Encryption* or *Maximum Strength Encryption* selected, select each available authentication protocol one at a time and attempt to aut henticate to the VPN server, repeat steps 2 and 3 except for MS -CHAPv2: 2) Verify if VPN connection attempt FAILED with a wrong password; Verify if VPN connection attempt FAILED with the right password; For authentication protocol MS -CHAPv2: 3) Verify if VPN con nection attempt FAILED with a wrong password; 4) Verify if VPN connection established successfully with only MS-CHAPv2 is selected; On the VPN server: 5) Verify if the following messages are found in the system log file */var/log/messages* : *July 01 10:13:18 black pppd[5518]: CHAP peer authentication succeeded for eric* *July 01 10:13:18 black pppd[5518]: MPPE 128 -bit stateless compression enabled*
Subjective / Objective	Objective.
Reference	RedHat 9.0 HOWTO [12] and personal experience.

Checklist Item CL -VPN3 – Policy Enforcement for New Password

Checklist Item	CL-VPN3
Control Objective	Ensure the compliance of the corporate password policy is enforced in VPN authentication credentials creation and modification effectively.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN3
Risk	Weak passwords may be used for VPN authentication credentials if no enforcement exists to ensure a password is compliant to the corporate password policy. Password authentication is always subjected to password guessing and brute-forcing attack. The stronger the password strength, the longer it takes to be compromised and hence the risk is lower. *Importance*: High *Likelihood*: High
Compliance	Mechanism is in place to enforce the compliance of the corporate password policy in VPN authentication credentials creation and modification.
Test	Determine if enforcement is in place and it is effective. Verify the effectiveness of any existing program or script for that purpose, if there is any.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-VPN4 – Policy Compliance for Existing Password

Checklist Item	CL-VPN4
Control Objective	Ensure the current state of VPN authentication credentials are compliant to the corporate password policy.
Risk	Password authentication is always subjected to password guessing and brute-forcing attack. The stronger the password strength, the longer it take to be compromised and hence the risk is lower. *Importance*: High *Likelihood*: High
Compliance	VPN user password must be at least 8 characters including at least a upper case and numeric and one special characters.
Test	Verify if all passwords in the authentication credential file */etc/ppp/chap-secrets* meet the minimal requirement. If there exist no program or script, a script has to be developed for that purpose.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item CL -VPN5 – VPN Access Control

Checklist Item	CL-VPN5
Control Objective	Ensure VPN resources are only accessible from pre -approved source network address.
Risk	The VPN access service is open to attack by hackers on the Internet if access control is not enforced to allow connection from only known source network addresses. *Importance*: Medium *Likelihood*: Medium
Compliance	Firewall filtering rules should exist for all VPN users with static IP address or a dynamic IP address from a known network address pool. VPN access from any other network should be denied.
Test	1 Examine the file */etc/sysconfig/iptables* to ensure that VPN access rules for all VPN users are correctly in place, deny otherwise; 2 Use nmap to perform a port scan to the VPN server from a IP address defined in the iptables ruleset; *C:\nmap>nmap -p 1723 xxx.xxx.xxx.xxx* 3 Repeat step 2) with an unauthorised IP address. where xxx.xxx.xxx.xxx is the IP address of the VPN servers
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL -VPN6 – VPN Network Authorisation

Checklist Item	CL-VPN6
Control Objective	Ensure VPN authorisation is enforced to allow access to approved network resources only.
Risk	Lack of authorisation enforcement of VPN access allows unrestricted access to all corporate network resources by all VPN users, or intruders in the case that VPN acc ess has been compromised. Enforcement of authorisation allows finer access control to specific internal network resources, it can limit potential damage by intruder access. *Importance*: Medium *Likelihood*: Medium

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN6
Compliance	All VPN access should be assigne d a specific internal private network IP address. Network authorisation should be enforced based on the assigned IP address.
Test	1 Verify if specific IP address exists for each client entry in the configuration file */etc/ppp/cap-secrets*. 2 Examine if specific firewall rulesets exist in firewall configuration file */etc/sysconfig/iptables*; 3 Verify if IP address matches with the assignment on VPN connection; 4 Ping an approved internal server; *C:\>ping xxx.xxx.xxx.xxx* 5 Ping an internal server that is not approved; *C:\>ping xxx.xxx.xxx.xxx*
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-VPN7 – VPN Configuration Files Permission

Checklist Item	CL-VPN7
Control Objective	Ensure VPN configuration files are protected from unauthorised modification.
Risk	Failure to protect the PPTP configuration files from unauthorised modification can allow hackers to enable weak authentication protocol and password, and/or disable VPN tunnel encryption. Data confidentiality and integrity can be compromised. *Importance*: Medium *Likelihood*: Medium
Compliance	All PPTP configuration files should be owned and can only be modified by user *root*. Credential database should be readable by user *root* only.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-VPN7
Test	Verify the following files are owned and can be modified by user root only: */etc/modules.conf* */etc/pptpd.conf* */etc/ppp/options.pptpd* Verify the following files are owned, readable and can be modified by user root only: */etc/ppp/chap-secrets* */etc/ppp/pap-secrets*
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-VPN8 – VPN Authentication Logging

Checklist Item	CL-VPN8
Control Objective	Ensure sufficient level of logging for VPN access authentication.
Risk	Logging of VPN authentication provides record of VPN access attempts for incident response and/or forensics analysis. Insufficient logging can cause difficulties in tracking the event. Moreover, sufficient logging may be required by regulation and/or legislation as duty of care. Lack of remote centralised log server may delay incident correlation and provide intruders an opportunity to cover their tracks. *Importance*: Medium *Likelihood*: Medium
Compliance	Both successful and failed VPN access authentication attempts should be logged in local system log and/or remote syslog server, if applicable.
Test	Verify if there is remote centralised logging facility. Examine if local system log file */var/log/messages* contains both successful and failure VPN authentication attempt.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.3 Audit Checklist – Technical – VPN Server Operating System

Checklist Item CL -SVR1 – Server Patching Level

Checklist Item	CL-SVR1
Control Objective	Ensure all appropriate security fixes are in place and all relevant security advisories from vendors have been followed.
Risk	Software security holes are by far the most common cause of security breaches. All relevant software security bugs on direct Internet connected servers should be patched as soon as possible. *Importance*: High *Likelihood*: High
Compliance	All relevant software on the VPN server should be patched to the secure stable version.
Test	Verify if all relevant software on the Linux VPN server is of version not earlier than the version specified in the security advisories of RedHat Linux 9 [14]. Verify if the PPTP daemon, pptpd has to be upgraded due to any security bug of the Poptop project. Visit the Poptop Project Home Page [15] and the Bug Tracker Page [16].
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL -SVR2 – Server Network Services

Checklist Item	CL-SVR2
Control Objective	Ensure only necessary network services are running on the VPN server.
Risk	Any unnecessary network services can open up incoming connections from the Internet. The more network services enabled, the more potential vulnerabilities, hence increases the risk for remote attack. *Importance*: High *Likelihood*: High
Compliance	Only necessary network services should be running on the VPN server and listening on TCP/IP ports.
Test	Verify that only the necessary TCP/IP ports are being opened by known processes: *# netstat -an*

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-SVR2
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-SVR3 – Server Hardening

Checklist Item	CL-SVR3
Control Objective	Ensure the operating system of VPN server is reasonably hardened.
Risk	Hardened Internet servers provide more resistant to attack and impose more restriction to intruders in case of security breaches, hence decrease the potential damage in case of intrusion. *Importance*: High *Likelihood*: High
Compliance	The operating system should be hardened to certain extend either manually according to industrial recognised guideline such as the SANS Securing Linux guide [17] or using industrial recognised hardening tools such as the Bastille Linux Project [18]
Test	Determine if the operating system is reasonably hardened by using industrial recognised Linux auditing tools, CIS Linux Level -I Benchmarks and Scoring Tool for Linux [19], and Linux Security Auditing Tool (LSAT) [20].
Subjective / Objective	Highly subjective - the degree of hardening may vary with the experience of the system administrator if manual approach is adopted. On the other hand, the auditor's technical expertise vary as well.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-SVR4 – Server Secure Remote Management

Checklist Item	CL-SVR4
Control Objective	Ensure secure remote management access to VPN server is deployed.
Risk	Insecure protocol such as Telnet can be compromised easily. Use of insecure protocol for server remote management purpose can put the server in high risk. *Importance*: High *Likelihood*: High
Compliance	Only secure protocols such as SSH should be used for server remote management purposes.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-SVR4
Test	1 Verify if SSH daemon is running and listening on port 22: *# ps -ef | grep sshd* *# netstat -an | grep 22* 2 Verify if Telnet is listening on port 23: *# netstat -an | grep 23*
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-SVR5 – Remote Management Configuration Files Permission

Checklist Item	CL-SVR5
Control Objective	Ensure configuration file for remote management access services SSH is protected from unauthorised modification.
Risk	Failure to protect the SSH configuration files from unauthorised modification can allow hackers to enable weak authentication and encryption. Data confidentiality and integrity of remote management traffic including authentication credentials can be compromised. Importance: Medium *Likelihood*: Medium
Compliance	SSH configuration file should be owned and can only be readable and modified by user *root*.
Test	Verify the following file is owned, readable and can be modified by user root only: */etc/ssh/sshd_config*
Subjective / Objective	Objective.
Reference	Best practice in the industry.

Checklist Item CL-SVR6 – Server Firewalling

Checklist Item	CL-SVR6
Control Objective	Ensure sufficient firewalling is enabled on the VPN server to protect itself.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-SVR6
Risk	Insufficient firewalling of the VPN server can open up unnecessary network services to the Internet, hence increase the risk for remote attack. *Importance*: High *Likelihood*: High
Compliance	Only VPN and remote management services originated from pre-approved source should be allowed from the Internet and/or internal network.
Test	1 Verify if the iptables configuration file /etc/sysconfig/iptables is set to allow only SSH and PPTP from specific source and deny otherwise; 2 Verify by performing a port scan from the Internet: *C:\nmap>nmap -p 1-65535 xxx.xxx.xxx.xxx*
Subjective / Objective	Objective.
Reference	Linux iptables HOWTO [13], best practice in the industry and personal experience.

Checklist Item CL-SVR7 – Remote Management Logging

Checklist Item	CL-SVR7
Control Objective	Ensure sufficient level of logging for remote SSH management access authentication is in place.
Risk	Logging of SSH authentication provides a record of remote management access attempts for incident response and/or forensics analysis. Insufficient logging can cause difficulties in case of intrusion. Moreover, sufficient logging may be required by regulation and/or legislation as duty of care. Lack of remote centralised log server may delay incident correlation and provide intruder an opportunity to cover their tracks. *Importance*: Medium *Likelihood*: Medium
Compliance	Both successful and failed SSH access authentication attempts should be logged in local system log and/or remote syslog server, if applicable.
Test	Verify if there is remote centralised logging facility. Examine if local system log file /var/log/messages contains both successful and failed SSH authentication attempt.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-SVR7
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-SVR8 – Server Fail-Safe Configurations

Checklist Item	CL-SVR8
Control Objective	Ensure the VPN server configurations are fail-safe.
Risk	Any ad hoc changes to the server configurations without proper change management can cause server not to function as it was supposed before restarting. Server to be audited should be restarted prior to all auditing activities to ensure it is in a healthy state for audit. However, not all production servers can be restarted due to potential interruption of the business. *Importance*: Medium *Likelihood*: Medium
Compliance	The VPN server should be restarted prior to all auditing activities.
Test	All auditing activities on the checklist.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-SVR9 – Server Vulnerability

Checklist Item	CL-SVR9
Control Objective	Ensure that all network services have no known vulnerabilities with high or medium risk.
Risk	Network services vulnerability can be exploited remotely from the internal network or the Internet. Server can be compromised if vulnerability is exploited. *Importance*: High *Likelihood*: Medium
Compliance	No vulnerability of *High* or *Medium* risk is found by the vulnerability scanner.
Test	Perform vulnerability scan using security scanners, e.g. Nessus or ISS Internet Scanner. The black box approach is preferable and that would be the most thorough test, however more time is required.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-SVR9
Subjective / Objective	Objective.
Reference	Best practice in the industry.

2.4 Audit Checklist – Technical – VPN Client Workstation Operating Environment

Checklist Item CL-CLT1 – Client Workstation Authentication Enforcement

Checklist Item	CL-CLT1
Control Objective	Verify if user authentication is enforced on VPN client workstation.
Risk	Lack of user authentication can put the corporate network in risk. Laptop or notebook computers can be lost or stolen due to its mobility. Moreover, VPN user credential is always stored on the workstation to enable automatic authentication. *Importance*: High *Likelihood*: High
Compliance	User should be authenticated before entering operating system session.
Test	Verify if authentication is required before user session can be started.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-CLT2 – Client Microsoft Networking Binding

Checklist Item	CL-CLT2
Control Objective	Ensure network binding for Microsoft Networking is disabled on the Internet connection interface of the VPN client workstation.
Risk	Microsoft Networking provides a lot of opportunities for hackers to compromise the workstation and hence very dangerous if service is provided to the Internet. *Importance*: High *Likelihood*: High
Compliance	Network binding for *File and Printer Sharing for Microsoft Networks* and *Client for Microsoft Networks* should be disabled on the broadband Internet connection interface.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist Item	CL-CLT2
Test	Verify if the items: *File and Printer Sharing for Microsoft Networks* and *Client for Microsoft Networks* are not checked under the *Security* tab of the broadband Internet connection properties.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

Checklist Item CL-CLT3 – Client Firewall and Anti-virus Protection

Checklist Item	CL-CLT3
Control Objective	Ensure that Firewall and Anti-virus software with up-to-date signature are installed, configured according to corporate security policy and activated on the VPN client workstation.
Risk	High-bandwidth Internet connected workstation without proper firewall and anti-virus protection is subjected to high risk of being compromised. Intruder can obtain authorised access to corporate intranet connection by piggy-back on the VPN connection and obtain free access to all corporate network resources. *Importance*: High *Likelihood*: High
Compliance	Firewall and Anti-virus software with up-to-date signature should be installed, configured according to corporate security policy and activated on the workstation.
Test	Verify if Firewall and Anti-virus software with up-to-date signature is installed, configured according to the provided security policy and activated on the workstation.
Subjective / Objective	Objective.
Reference	Best practice in the industry and personal experience.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 3 - Audit Evidence

3.1 Audit Evidence

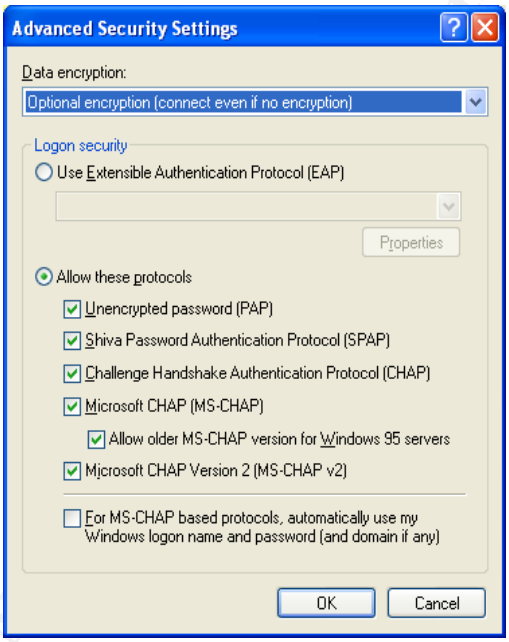
Audit Evidence 1/CL-VPN1 – Data Confidentiality and Integrity

Reference	CL-VPN1
Control Objective	Ensure the encryption in use for VPN data confidentiality and integrity is in compliance with the corporate standard.
Compliance	Microsoft Point-to-Point Encryption (MPPE) of 128-bit should be used and enforced for VPN session.

© SANS Institute 2003, Author retains full rights.

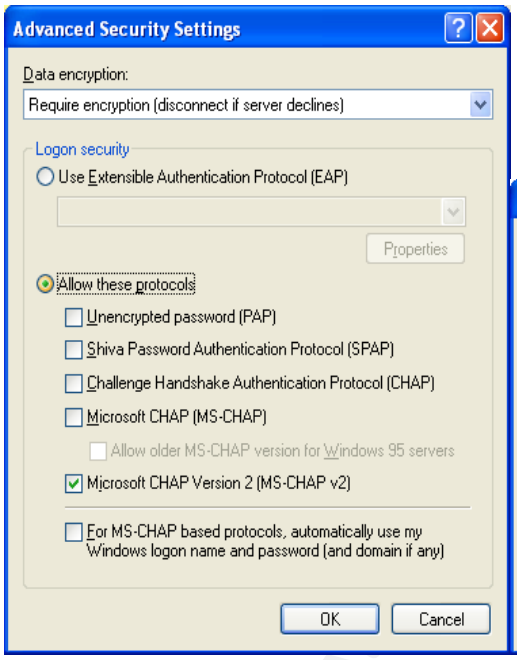
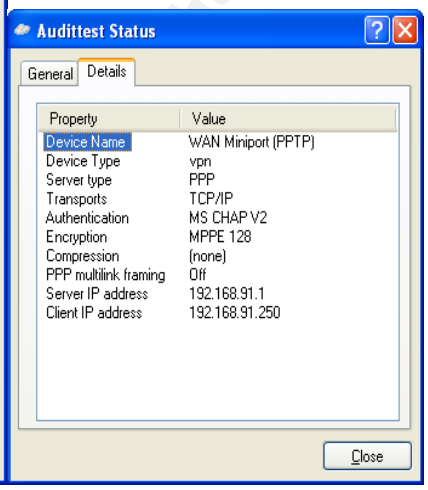
©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN1
Audit Results	1 In */etc/ppp/options.pptpd* , *require-mppe option* found and not commented out; 2 In */etc/ppp/options.pptpd* , there was no *+mppe-40* option; 3 MPPE was loaded with the following warning message: *Warning: loading /lib/modules/2.4.20 - 8/kernel/drivers/net/ppp_mppe.o will taint the kernel: non -GPL license - BSD without advertisement clause* *See http://www.tux.org/lkml/#export -tainted for information about tainted modules* *Module ppp_mppe loaded, with warning s* 4 Network sniffer turned on and capturing network traffic; 5 VPN connection attempt FAILED with encryption not required or optional; 

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN1
Audit Results (Cont.)	6) VPN connection attempt was SUCCESSFUL with encryption required;   7) The following message was found in the system log file */var/log/messages*: *July 01 10:13:18 black pppd[5518]: MPPE 128 -bit stateless compression enabled* 8) No plaintext authentication credential information was found in the captured VPN traffic packet; 9) The internal server was r eachable: *C:\Temp>ping xxx.xxx.xxx.xxx* *Pinging xxx.xxx.xxx.xxx with 32 bytes of data:* *Reply from xxx.xxx.xxx.xxx bytes=32 time=22ms TTL=64* *Reply from xxx.xxx.xxx.xxx bytes=32 time=20ms TTL=64* *Reply from xxx.xxx.xxx.xxx bytes=32 time=21ms TTL=64* *Reply from xxx.xxx.xxx.xxx bytes=32 time=20ms TTL=64* 10) No ICMP *echo-request* or *echo-reply* data was found in the captured GRE and PPP packet.
Residual Risk	The audited system enforces all VPN connection to be encrypted. The data confidentiality and integrity is pr eserved by encryption. The residual risk is then related to the strength of the encryption use. As discussed in section 2.2 CL -VPN1, MPPE is considered weak. Taking encryption strength into account, the residual risk is medium.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN1
Objective Achieved	Satisfactory

Audit Evidence 2/CL-VPN2 – Authentication Protocol Enforcement

Reference	CL-VPN2
Control Objective	Ensure the authentication protocol in use for VPN authentication is in compliance with the corporate standard.
Compliance	The corporate standard authentication protocol MS-CHAP version 2 only must be enforced for VPN authentication..
Audit Results	1 In */etc/ppp/options.pptpd* , *require-mschap-v2* option found and not commented out; 2 VPN connection attempt FAILED with a wrong password for PAP, SPAP, CHAP , MS-CHAP; 3 VPN connection attempt FAILED with the right password for PAP, SPAP, CHAP, MS-CHAP; 4 VPN connection attempt FAILED with a wrong password for MS-CHAPv2; 5 VPN connection attempt was SUCCESSFUL with right password for MS-CHAPv2; 6 The following messages were found in the system log file */var/log/messages*: *July 01 10:13:18 black pppd[5518]: CHAP peer authentication succeeded for eric* *July 01 10:13:18 black pppd[5518]: MPPE 128-bit stateless compression enabled*
Residual Risk	The audited system uses only MS-CHAPv2 for authentication. The residual risk is then related to the strength of the authentication protocol. As discussed in section 2.2 CL-VPN2, MS-CHAPv2 is considered weak. Taking that into account, the residual risk is medium.
Objective Achieved	Satisfactory

Audit Evidence 3/CL-VPN3 – Policy Enforcement for New Password

Reference	CL-VPN3
Control Objective	Ensure the corporate password policy is effectively enforced in VPN authentication credentials creation and modification.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN3
Compliance	Mechanism is in place to effectively enforce the compliance of corporate password policy in VPN authentication credentials creation and modification.
Audit Results	There was no tool available for strong password checking or enforcement to ensure credentials were created or modified in compliance with the corporate password policy. Manual procedure was used to enter new or modify password in the credential database, i.e. */etc/ppp/chap-secrets*.
Residual Risk	Manual procedure for entering new or modifying password is not robust and subject to errors. There is a high probability that some VPN authentication passwords do not comply with the corporate password policy. Simple passwords are easy to compromise. There is a high risk that the VPN access service can be compromised.
Objective Achieved	FAILED

Audit Evidence 4/CL-VPN5 – VPN Access Control

Reference	CL-VPN5
Control Objective	Ensure VPN resources are only accessible from pre-approved source network address.
Compliance	Firewall filtering rules should exist for all VPN users with static IP address or a dynamic IP address from a known network address pool. VPN access from any other network should be denied.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

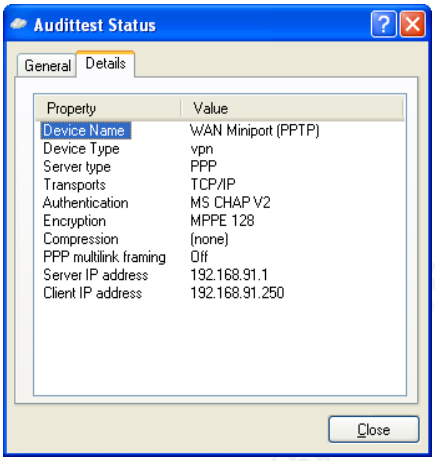
Reference	CL-VPN5
Audit Results	1 The corresponding ruleset found match with the expected results: *-A IntLockdown -INPUT -p tcp -m tcp -s yyy.yyy.yyy.yyy -d xxx.xxx.xxx.xxx -dport 1723 –syn -j ACCEPT* *-A IntLockdown -INPUT -p tcp -m tcp –syn -j DROP* 2 Perform a port scan from an authorised IP address: *C:\nmap>nmap -p 1723 xxx.xxx.xxx.xxx* *Starting nmap V. 3.30 (www.insecure.org/nmap/)* *Interesting ports on (xxx.xxx.xxx.xxx):* *Port State Services* *1723/tcp open pptp* *Nmap run completed – 1 IP address (1 host up) scanned in 10 seconds* 3 Perform a port scan from an unauthorised IP address: *C:\nmap>nmap -p 1723 xxx.xxx.xxx.xxx* *Starting nmap V. 3.30 (www.insecure.org/nmap/)* *Interesting ports on (xxx.xxx.xxx.xxx):* *Port State Services* *1723/tcp filtered pptp* *Nmap run completed – 1 IP address (1 host up) scanned in 10 seconds* where xxx.xxx.xxx.xxx is the IP address of the VPN servers yyy.yyy.yyy.yyy is the IP address of the VPN client workstation
Residual Risk	PPTP port 1723 cannot be reached from unauthorised IP address. Though it is possible that hackers can spoof as authorised IP addresses, sophisticated kills are required. Hence, the residual risk is negligible.
Objective Achieved	Satisfactory

Audit Evidence 5/CL -VPN6 – VPN Network Authorisation

Reference	CL-VPN6
Control Objective	Ensure VPN authorisation is enforced to allow access to approved network resources only.
Compliance	All VPN access should be assigned a specific internal private network IP address. Network authorisation should be enforced based on the assigned IP address.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN6
Audit Results	1 Each client entry has a specific IP address in */etc/ppp/chap-secrets*, e.g. # client server secret IP address eric purple Pass$3work 192.168.91.250 2 There was no specific firewall ruleset for to restrict VPN users access to any defined network resources in */etc/sysconfig/iptables*; 3 Verify if the IP address matches with the assignment on VPN connection;  The IP address matched with the one configured in */etc/ppp/chap-secrets*. 4 Approved internal server was reachable; *C:\>ping xxx.xxx.xxx.xxx.* *Pinging xxx.xxx.xxx.xxx with 32 bytes of data:* *Reply from xxx.xxx.xxx.xxx bytes=32 time=22ms TTL=64* *Reply from xxx.xxx.xxx.xxx bytes=32 time=22ms TTL=64* *Reply from xxx.xxx.xxx.xxx bytes=32 time=22ms TTL=64* *Reply from xxx.xxx.xxx.xxx bytes=32 time=22ms TTL=64* 5 Non-approved server was unreachable; *C:\>ping xxx.xxx.xxx.xxx .* *Pinging xxx.xxx.xxx.xxx with 32 bytes of data:* Request timed out. Request timed out. Request timed out. Request timed out. where xxx.xxx.xxx.xxx is the IP address of the VPN servers

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN6
Residual Risk	VPN authorisation is in place but loosely enforced. That would potentially allow in truder to access internal network resources without any restriction in case of VPN being compromised. The residual risk is medium.
Objective Achieved	Partial satisfactory

Audit Evidence 6/CL -VPN7 – VPN Configuration Files Permission

Reference	CL-VPN7
Control Objective	Ensure VPN configuration files are protected from unauthorised modification.
Compliance	All PPTP configuration files should be owned and can only be modified by user *root*. Credential database should be readable by user *root* only.
Test	*# ls -la /etc/modules.conf /etc/pptpd.conf* *-rw-r—r-- 1 root root 473 Jun 30 14:23 modules.conf* *-rw-r—r-- 1 root root 473 Jul 1 09:15 pptpd.conf* *# ls -la /etc/ppp/options.pptpd /etc/ppp/chap -secrets /etc/pap -secrets* *-rw-r—r-- 1 root root 473 Jul 1 09:23 op tions.pptpd* *-rw-——--- 1 root root 473 Jul 1 10:35 chap -secrets* *-rw-——--- 1 root root 473 Jul 1 10:35 pap -secrets* All files are owned and modified by root only. Credential databases are readable by root only.
Residual Risk	Modification to configuration fi les required root privilege. Credential database can only be read by root. The residual risk is negligible.
Objective Achieved	Satisfactory

Audit Evidence 7/CL -VPN8 – VPN Authentication Logging

Reference	CL-VPN8
Control Objective	Ensure sufficient l evel of logging for VPN access authentication.
Compliance	Both successful and failure VPN access authentication attempt should be logged in local system log and/or remote syslog server, if applicable.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-VPN8
Audit Results	Both successful and failure VPN authent ication attempts were found in the local system log file */var/log/messages*: Success: *July 01 10:13:18 black pppd[5518]: CHAP peer authentication succeeded for eric* Failure: *July 01 10:13:18 black pppd[5518]: MPPE required, but MS - CHAP[v2] auth not performe d.*
Residual Risk	Both successful and failed VPN authentication attempts are logged. However, lack of remote centralised log server may delay incident correlation and provide intruder an opportunity to cover their tracks. The residual risk is low.
Objective Achieved	Satisfactory

Audit Evidence 8/CL -SVR2 – Server Network Services

Reference	CL-SVR2
Control Objective	Ensure only necessary network services are running on the VPN server.
Compliance	Only necessary network services should be running on the VPN server and listening on TCP/IP ports.
Audit Results	Verify the network services running on the server that are listening on TCP/IP ports: *# netstat -an* *tcp 0 0.0.0.0:6000 0.0.0.0:* LISTEN* *tcp 0 0.0.0.0:22 0.0.0.0:* LISTEN* *tcp 0 0.0.0.0:1723 0.0.0.0:* LISTEN*
Residual Risk	There is no unnecessary network services running. The residual risk is negligible.
Objective Achieved	Satisfactory

Audit Evidence 9/CL -SVR6 – Server Firewalling

Reference	CL-SVR6
Control Objective	Ensure sufficient firewalling is enabled on the VPN server to protect itself.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-SVR6
Compliance	Only VPN and remote management services originated from pre - approved source should be allowed from the Internet and/or internal network.
Audit Results	1 Only SSH and PPTP were the protocols found to allow connection to the VPN server from specific source IP address in */etc/sysconfig/iptables* ; *-A IntLockdown -INPUT -p tcp -m tcp -s yyy.yyy.yyy.yyy -d xxx.xxx.xxx.xxx -dport 22 --syn -j ACCEPT* *-A IntLockdown -INPUT -p tcp -m tcp -s yyy.yyy.yyy.yyy -d xxx.xxx.xxx.xxx -dport 1723 --syn -j ACCEPT* *-A IntLockdown -INPUT -p tcp -m tcp --syn -j DROP* *-A IntLockdown -INPUT -p udp -m udp -j DROP* 2 Results of a port scan from an authorised IP address: *C:\nmap>nmap -p 1-65535 xxx.xxx.xxx.xxx* *Starting nmap V. 3.30 (www.insecure.org/nmap/)* *Interesting ports on (xxx.xxx.xxx.xxx):* *(The 65533 ports scanned but not shown below are in state: filtered)* *Port State Services* *22/tcp open ssh* *1723/tcp open pptp* *Nmap run completed – 1 IP address (1 host up) scanned in 3722 seconds* 3 Results of a port scan from an unauthorised IP address: *C:\nmap>nmap -p 1-65535 xxx.xxx.xxx.xxx* *Starting nmap V. 3.30 (www.insecure.org/nmap/)* *All 65535 scanned ports on (xxx.xxx.xxx.xxx) are: filtered* *Nmap run completed – 1 IP address (1 host up) scanne d in 3713 seconds* where xxx.xxx.xxx.xxx is the IP address of the VPN servers yyy.yyy.yyy.yyy is the IP address of the VPN client workstation
Residual Risk	All access to server is restricted to approved source IP address only. The residual risk is negligible.
Objective Achieved	Satisfactory

Audit Evidence 10/CL -SVR9 – Server Vulnerability

Reference	CL-SVR9

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference	CL-SVR9
Control Objective	Ensure that all network services have no known vulnerabilities with high or medium risk.
Compliance	No vulnerability of *High* or *Medium* risk is found by the vulnerability scanner.
Audit Results	Perform two vulnerability scans using the ISS Internet Scanners, one internal and the other external to the corporate perimeter. Make sure all tests are selected in the policy. There were no findings from the external scan. Two low risk vulnerabilities were found in the internal scan: 1) IcmpTstamp: ICMP timestamp requests (CAN-1999-0524) The target computer responded to an ICMP timestamp request. By accurately determining the target's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them. Remedy: Configure your firewall or filtering router to block outgoing ICMP packets. Block ICMP packets of type 13 or 14 and/or code 0. 2) traceroute: Traceroute can be used to map network topologies Traceroute is a utility used to determine the path a packet takes between two endpoints. Traceroute does this by sending a series of packets with particular TTL (Time To Live) values and examining the resulting ICMP replies. Sometimes, when a packet filter firewall is configured incorrectly, an attacker can traceroute the firewall to gain knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information. Remedy: Prevent or limit external tracerouting into internal networks using packet filtering.
Residual Risk	There is no high or medium risk vulnerability found by the security scanner. The two low risk vulnerabilities are only applicable to the internal network. Hence, the residual risk is negligible.
Objective Achieved	Satisfactory

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2 System Auditability

The system as a whole is auditable. The control objectives were set based on the expectation of the customer as well as the experience and technical expertise of the auditor. The audit planning and entrance conference exercises were conducted effectively such that both the expectation and technical feasibility were well understand by both party.

However, there are areas that can not be validated easily. The administrative control objectives such as policies, training and plans are always hard to audit due to human factors. It requires an experienced auditor in order to achieve a quality audit.

Other areas that require technical expertise are also worth mentioning. The encryption and authentication protocol are two highly technical fields that normal auditors would not be comfortable with. Though the theory behind it can be understood, there is virtually no recognised methodology or tools that can help auditors in their work. Technical experts are required to assist if a thorough audit has to be performed.

Otherwise, most network and system objectives are rather straight forward to audit.

© SANS Institute 2003, Author retains full rights.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 4 - Audit Report

4.1 Executive Summary

The objectives of this audit are to review the current state of security of the corporate VPN service and benchmark against the best practices in the industry. The audit was completed and the objective were achieved. Recommendation for improvement will be provided.

This audit reviewed the corporate VPN server, a standard VPN client workstation and the associated corporate policy, baseline, guidelines and procedures rela ted to the use of VPN. The VPN service is secure overall. However, there are a few areas not meeting the best practices in the industry.

In particular, weak passwords are used for VPN authentication. Weak passwords are easy to guess and break. In the event of password being compromised, intruders may obtain unrestricted access to all internal network resources, including the important software source code repository. Although the VPN server firewall provides source network filtering, it may become a s ingle point of failure in security. It is recommended in high priority that tools should be deployed to ensure all VPN passwords, both new and existing, meet the strong password standard as described in the corporate password policy.

It was also discover ed that VPN users currently have unrestricted access to all internal resources. In the event of password being compromised, intruders will only have limited access if restrictive access is enforced. It is recommended that restrictive network authorisatio n should be enforced.

In the longer term, the company may consider evaluating more secure alternative VPN solutions such as IPSec and deploying centralised log server and/or intrusion detection system.

4.2 Audit Findings

All findings reviewed by the a udit exercise are prioritised below in their level of risk.

Item	***Status***	***Findings***	***Risk***	***Audit Evidence Reference***
Policy Enforcement for New Password	Fail	• The corporate password policy is not enforced for creation or modification of credentials. • No tool exists for strong password enforcement.	High	3/CL-VPN3

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Item	*Status*	*Findings*	*Risk*	*Audit Evidence Reference*
VPN Network Authorisation	Partial Satisfactory	• VPN network authorisation mechanism in place but loosely enforced.	Medium	5/CL-VPN6
Data Confidentiality and Integrity	Satisfactory	• The corporate standard encryption in place for VPN communication. • MPPE encryption is weak.	Medium	1/CL-VPN1
Authentication Protocol Enforcement	Satisfactory	• The corporate standard authentication protocol in place for VPN authentication. • MS-CHAPv2 authentication protocol is weak.	Medium	2/CL-VPN2
VPN Authentication Logging	Satisfactory	• Successful and failure authentication were logged. • Lack of remote centralised log server.	Low	7/CL-VPN8
VPN Access Control	Satisfactory	• Source network access control enforcement in place.	Negligible	4/CL-VPN5
VPN Configuration Files Permission	Satisfactory	• Reasonable restrictive configuration files permission.	Negligible	6/CL-VPN7
Server Network Services	Satisfactory	• No unnecessary network services running.	Negligible	8/CL-SVR2
Server Firewalling	Satisfactory	• Firewalling in place to control network access to server.	Negligible	9/CL-SVR6
Server Vulnerability	Satisfactory	• No high or medium risk vulnerability. • Two low risk vulnerabilities exist but not exploitable directly from the Internet.	Negligible	10/CL-SVR9

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.3 Background / Risk

Based on the findings, the associated risks are explained below.

Risk	***Background / Analysis***
High	Corporate password policy not enforced: There is no appropriate tool to enforce password to be strong and compliant with the corporate password policy. Weak passwords exist in the existing credential database and they are easy to guess and break. In case of an intrusion, intruder can gain unrestricted access to all internal network resources, including all important assets of the company such as the software source code repository. Although the firewalling on the VPN server provides source network filtering, it is the sole control mechanism and does not provide defence in depth.
Medium	Unrestrictive VPN network authorisation: All VPN users currently have unrestricted access to all internal network resources, including resources that may not be required. In case of an intrusion, intruder will also have unrestricted access to all internal resources. Restriction should be imposed on important resources to reduce the risk of damage.
Medium	Weak encryption protocol: Microsoft Point-to-Point Encryption (MPPE) is fundamentally weaker than other encryption technology, according to security research [6]. It is comparatively easy to be compromised and is not recommended for high security requirement.
Medium	Weak VPN authentication protocol: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) is fundamentally weak, according to security research [8, 9]. It is comparatively easy to be compromised and is not recommended for high security requirement.
Low	Lack of remote centralised log server: In case of VPN server compromised, intruder can cover their tracks by erasing system logs. Remotely stored event records provide evidence to forensics analysis and investigation. More accurate, detailed and timely correlation of network and server events data can be achieved with a centralised log server.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4.4 Audit Recommendations

The following recommendations were developed for mitigation of the identified risks:

1) Appropriate tools should be deployed in high priority to allow system administrator to ensure new and existing VPN passwords are compliant to the corporate password policy.

2) Network Authorisation should be enforced. Important corporate assets should be restricted access to required and authorised personnel only. VPN users should be allowed to access the required resources only.

3) PPTP is fundamentally weaker in security than other VPN technology such as L2TP and IPSec because of the fundamental weakness of MPPE and MS -CHAP. The company may worth studying whether it is justify to upgrade to a more secure solution such as IPSec.

4) The company may also study the feasibility t o deploy a centralised syslog server to improve its security in a longer term.

4.5 Costs

The recommendations can all be achieved by inhouse development, hence the cost estimation will assume the inhouse manday cost to be $300. The estimated cost is summarised in the following table.

(manday) *Recommendations*	*Planning*	*Development*	*Testing*	*Deployment*	*Hardware*	*Total Cost*
1) Password Checking and Enforcing Tool	1	2	1	1	$0	$1,500
2) Restrictive VPN Authorisation Policy Enforcement	3	1	1	1	$0	$1,800
3) IPSec VPN Solution	3	5	5	3	$1,500	$6,300
4) Centralised syslog Server	2	1	1	1	$1,500	$1,500

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1) The development of a customised tool for password checking and enforcement to integrate with the existing system is estimated to be 5 mandays. The solution will not cause any impact to existing system. It is expected that the operation support cost will be lower as the automated tool will replace some of the manual operation procedure.

2) The development of a restrictive authorisation policy is estimated to be 6 mandays. It will be challenging to capture all the network resource requirements, build the policy and deployment may be painful. There will be no impact to current systems and the maintenance of the policy may only require minimal resource overhead if a role based approach is taken. There should not be any additional operation support cost required once the policy becomes stable.

3) The development of an IPSec VPN solution is estimated to be 20 mandays. In additional to the new server, new client may be required to be deployed to all VPN client workstations. The operation support cost will be slightly higher than the current solution due to the complication of IPSec.

4) The development of a centralised syslog server is estimated to be 5 mandays. The impact to network traffic volume and existing systems should be negligible. There will be additional operating cost for maintaining an additional server.

4.6 Compensating Controls

1) There is no known compensating controls available.

2) There is no known compensating controls available.

3) For IPSec based VPN solutions, there are a lot of cost effective hardware solution ton the market for consideration. Both the solution cost and operation support cost may be lower than an inhouse development solution.

4) Putting centralised syslog service on an existing server may be a cost effective solution. Additional cost for both hardware and operation support are not required.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. References

1. Eric Shovfoged
Auditing the S-Box Safe@SOHO VPN/Firew all
http:www.giac.org/GSNA.php

2. John Dietrich
Auditing A Checkpoint VPN1 Mobile User Virtual Private Network VPN
http://www.giac.org/GSNA.php

3. John Blair
Auditing the Checkpoint NG SecureClient (VPN -1 / Firewall-1)
http://www.giac.org/GSNA.php

4. Dan Strom
Auditing the Netscreen -5 Firewall Used as a VPN Gateway
http://www.giac.org/GSNA.php

5. Information Technology Services Department, The Government of the Hong Kong Special Administrative Region
IT Security Guideline
http://www.itsd.gov.hk/itsd/en glish/itgov/download/g3.pdf

6. Randy Franklin Smith
Is PPTP Safe?
http://www.winnetmag.com/Articles/Index.cfm?ArticleID=5188&pg=2

7. Kevin Townsend
Understanding VPNs and PPTP
www.itp-journals.com/nasample/t1807.pdf

8. Counterpane Internet Security, Inc
Analysis of Microsoft PPTP Version 2
http://www.counterpane.com/pptp.html

9. Counterpane Internet Security, Inc
Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS -CHAPv2)
http://www.counterpane.com/pptpv2 -paper.html

10. Ed Skoudis
Ask the Expert: Questions & Answers
http://searchsecurity.techtarget.com/ateQuestionNResponse/0,289625,sid14_cid498339_tax292733,00.html

11. Setting up PPTPD on Linux Kernel 2.4 HOWTO
http://poptop.sourceforge.net/dox/source -howto.html

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

12. James Cameron
RedHat 9.0 HOWTO
http://pptpclient.sourceforge.net/howto-redhat-90.phtml

13. Rusty Rusell
Linux iptables HOWTO
http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html

14. RedHat Linux 9 Security Advisories
https://rhn.redhat.com/errata/rh9-errata-security.html

15. Poptop Project Home Page
http://www.poptop.org/

16. Poptop Project Bug Tracker
http://sourceforge.net/tracker/?group_id=44827&atid=441003

17. SANS Securing Linux Guide
http://store.sans.org/store_item.php?item=83

18. Bastille Linux Project
http://www.bastille-linux.org/

19. Centre of Internet Security
CIS Linux Level-I Benchmarks and Scoring Tool for Linux
http://www.cisecurity.org/

20. Linux Security Auditing Tool (LSAT)
http://usat.sourceforge.net/

© SANS Institute 2003, Author retains full rights.

©SANS Institute 2003. As part of GIAC practical repository. Author retains full rig hts.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS IT Audit Training

Community SANS @ CANHEIT	Ottawa, ON	Jun 13, 2013 - Jun 14, 2013	Community SANS
SANSFIRE 2013	Washington, DC	Jun 14, 2013 - Jun 22, 2013	Live Event
Community SANS Chicago	Chicago, IL	Jul 08, 2013 - Jul 12, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201307,	Jul 08, 2013 - Aug 07, 2013	vLive
SANS Rocky Mountain 2013	Denver, CO	Jul 14, 2013 - Jul 20, 2013	Live Event
Critical Security Controls Summit	Washington, DC	Aug 12, 2013 - Aug 18, 2013	Live Event
Community SANS Dallas	Dallas, TX	Aug 19, 2013 - Aug 22, 2013	Community SANS
SANS vLive - AUD507: Auditing Networks, Perimeters, and Systems	AUD507 - 201309,	Sep 02, 2013 - Oct 16, 2013	vLive
SANS CyberCon Fall 2013	Online, VA	Sep 09, 2013 - Sep 14, 2013	CyberCon
Network Security 2013	Las Vegas, NV	Sep 14, 2013 - Sep 23, 2013	Live Event
Community SANS Miami	Miami, FL	Sep 16, 2013 - Sep 19, 2013	Community SANS
Network Security 2013 - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	Las Vegas, NV	Sep 16, 2013 - Sep 20, 2013	vLive
Mentor Session - SEC 566	Troy, MI	Oct 01, 2013 - Dec 10, 2013	Mentor
Community SANS Washington @ GWU	Washington, DC	Oct 07, 2013 - Oct 10, 2013	Community SANS
SANS Baltimore 2013	Baltimore, MD	Oct 14, 2013 - Oct 19, 2013	Live Event
SOS SANS October Singapore 2013	Singapore, Singapore	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, IL	Oct 28, 2013 - Nov 02, 2013	Live Event
Community SANS New York	New York, NY	Nov 04, 2013 - Nov 07, 2013	Community SANS
SANS Sydney 2013	Sydney, Australia	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS London 2013	London, United Kingdom	Nov 16, 2013 - Nov 25, 2013	Live Event
Community SANS Toronto	Toronto, ON	Nov 18, 2013 - Nov 21, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201312,	Dec 02, 2013 - Jan 15, 2014	vLive
Community SANS Vancouver	Burnaby, BC	Dec 09, 2013 - Dec 12, 2013	Community SANS
North America ICS Security Summit & Training 2014	Lake Buena Vista, FL	Mar 11, 2014 - Mar 20, 2014	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced