

CGO

6 oktober 2004

Computer&netwerk beveiliging

- Blokkering externe toegang desktops:
 - Waarom
 - Wat zijn de veranderingen
 - Consequenties
 - Alternatieven
- Nog meer maatregelen (sorry!)
 - Secure imap/pop3 mail clients
 - Beveiliging guestnet

De aankondiging

Date: Wed, **15 Sep 2004**
From: Wim Heubers <wimh@nikhef.nl>
To: cgo-list@nikhef.nl
Subject: externe toegankelijkheid linux desktops

Aan: contactpersonen CGO.
Betreft: externe toegankelijkheid Linux desktops

De Linux desktop systemen zijn direct toegankelijk vanuit het internet. Om redenen van **veiligheid** hebben wij het voornemen om op afzienbare termijn deze directe toegankelijkheid te **blokkeren**.

[meer tekst]

... .. vragen wij de contactpersonen van het CGO om voor 1 oktober hun achterban hierover in te lichten en een **inventarisatie** te maken van mogelijke problemen die door de blokkering zullen ontstaan.



De reacties

Iets wat misschien voor problemen zou kunnen zorgen is dat je **locale harde schijf**, d.w.z. `/stage/polymorf/computer/`, niet meer **direct** toegankelijk is van buiten af.

Als bv de **scp** functie niet meer beschikbaar is vanaf zeg `lxplus` naar de lokale desk-tops zijn we behoorlijk "de aap geloggeerd". Dit gebruiken we zeer intensief voor grote bestanden.

Ja, met **remote X sessies** die gebruik maken van een ssh tunnel en die op een bepaalde machine moeten plaatsvinden (b.v. nodig voor initialiseren on-chamber elektronica).

Dat is vlot samengevat: ik zal **mijn werk niet meer kunnen doen**. Ik **log** vanuit Utrecht **in** op mijn machine in Amsterdam (Loki) om bij de data, mijn programma's en mijn schrijfsels te kunnen.

Ondertussen op CERN

Date: Thu, **23 Sep 2004**

From: Denise Heagerty <Computer.Security@cern.ch>

Subject: ALERT: **major break-in** with passwords discovered

CSIRTS and Security Teams,

CERN's central **Linux service**, LXPLUS suffered from a major security incident today. During the night, an attacker replaced the SSH client binary with a trojan version that **sent out passwords** that were typed.

This means that passwords for users connecting from CERN to other collaborating sites during the morning of Thu 23 Sep (Geneva localtime) have very likely been exposed.

I strongly recommend that you **closely monitor your sites** for similar activity and compromised accounts.

Denise Heagerty

CERN Computer Security Officer.



en op FNAL

Date: Thu, **30 Sep 2004**

From: dane@fnal.gov

Subject: Yet another probable source address for the lxplus cluster intruder

On Sep 27 at 07:14 UTC FNAL observed an HTTP download from a reported SSH trojan distribution site. The attacker is believed to have gained access to the **cuevas FNAL user account** using the cuevas account on machine fanae09.geol.uniovi.es (156.35.88.179). This account name **corresponds** to one of those listed in the CERN lxplus compromise.

It is our belief that the CERN attackers may now be working their way **around the HEP collaboration sites** using stolen passwords and/or hijacking sessions on compromised machines.

Dane Skow

Fermilab Computer Security Executive (Deputy)



en op SLAC

Date: Thu, **30 Sep 2004**

From: "Cowles, Robert D." <rdc@slac.stanford.edu>

Subject: Incident at SLAC - **klog backdoor**

We have discovered a number of machines at SLAC running a backdoor klog process - **collecting keystrokes** from other sites and sending them on.

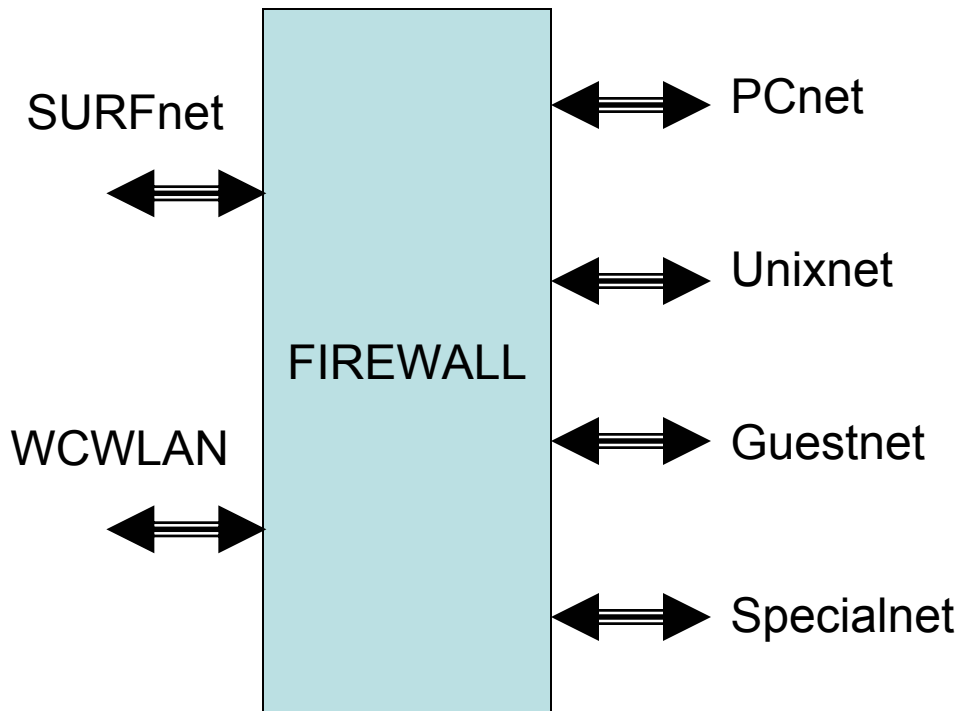
Please see the attached emails for the full list of machines the user logged into. The legitimate user was at a site compromised about a month ago, and does **not** have login at CERN.

As far as we can tell at this time, no machines at SLAC were actually compromised. The klogd was running with user privileges.

Bob Cowles
SLAC Computer Security Officer



Firewall



Firewall 'policy' instellen per:

- Netwerk (ip range)
- Machine (ip nummer)
- Service (port nummer)

Verschillende policies voor:

- Van buiten naar binnen
- Van binnen naar buiten
- Interne netwerken onderling

Services (port nummers):

- < 1024 gestandaardiseerd
- > 1024 niet

Voorbeelden:

- SSH voor alle Linux desktops
- HTTP beperkt tot web server

SSL: secure socket layer:

- Encrypted SSH sessies
- Encrypted web pages (bv webmail)
- Ssh, sftp, scp, https, imaps, rdsk, etc

De huidige configuratie



Van buiten naar binnen

- Externe toegang Windows servers/desktops:
 - Alle poorten dicht, met uitzondering van:
 - SFTP naar 'paling' (secure file transfer)
- Externe toegang Unix servers/desktops:
 - Alle poorten < 1024 dicht, met uitzondering van:
 - SSH voor alle desktops
 - Specifieke poorten naar specifieke servers:
 - Bv http(s) naar www.nikhef.nl; imap(s) naar imap.nikhef.nl; ldap naar ldap.nikhef.nl.
 - Alle poorten > 1024 open, met uitzondering van:
 - Poorten naar bekende riskante services:
 - Bv NFS (network file system), rootkit, fontserver, etc

Van binnen naar buiten

- Alles open op enkele speciale protocollen na

Intern

- Intern vanuit PCnet en guestnet geen NFS en SunRPC

Waarom directe toegang naar alle services op Linux desktops blokkeren???

- Continue aanvallen vanuit het internet:
 - Automatische 'port scans', toeslaan wanneer zwakke plek gevonden is, bv het installeren van een 'backdoor', die van binnen uit contact zoekt met ...
 - Automatische scans accounts/password voor login:

```
Oct  4 20:06:46 triton.nikhef.nl sshd(pam_unix)[17479]: check pass; user unknown
Oct  4 20:06:47 thorin.nikhef.nl sshd(pam_unix)[27244]: check pass; user unknown
Oct  4 20:06:51 oberon.nikhef.nl sshd(pam_unix)[19657]: check pass; user unknown
Oct  4 20:06:52 parsival.nikhef.nl sshd(pam_unix)[21143]: check pass; user unknown
Oct  4 20:06:52 thorin.nikhef.nl sshd(pam_unix)[27256]: check pass; user unknown
```
- Toegang beperken tot 1 systeem:
 - Zorgvuldige monitoring van 1 ipv ruim 200 systemen.
 - De toegang van dit systeem naar 'binnen' strikt definiëren.

Is dat dan voldoende?

- Nee, een zwakke plek is en blijft het 'statische' password.
- Suggesties om hier iets aan te doen:
 - Password aging (afdwingen periodieke vernieuwing password)
 - Strong authenticatie mbv 'one time passwords'
 - Of een andere opzet mbv PKI, CA's, etc (zoals grid).
 - En zeker geen account/password sessies over niet encrypted connecties (wel imaps en pop3s en niet imap en pop3).
 - Blokkeren cq opheffen van 'slapende' accounts (zoals van bijvoorbeeld ex-medewerkers, studenten, etc).
- Alert blijven: de ketting is net zo sterk als de zwakste schakel

Consequentie blokkeren Linux desktops

Naar aanleiding van reacties tot nu toe:

- Het zal niet meer mogelijk zijn, om buiten het nikhef.nl domain rechtstreeks:
 - in te loggen op de desktop
 - Dus geen 'ssh mydesktop.nikhef.nl'
 - bestanden van de lokale schijf op de desktop te benaderen.
 - Dus geen 'scp mydesktop.nikhef.nl:myfile .'
 - een X-sessie op de desktop op te starten.
 - andere services op de desktop te gebruiken.
- Wat nog meer?

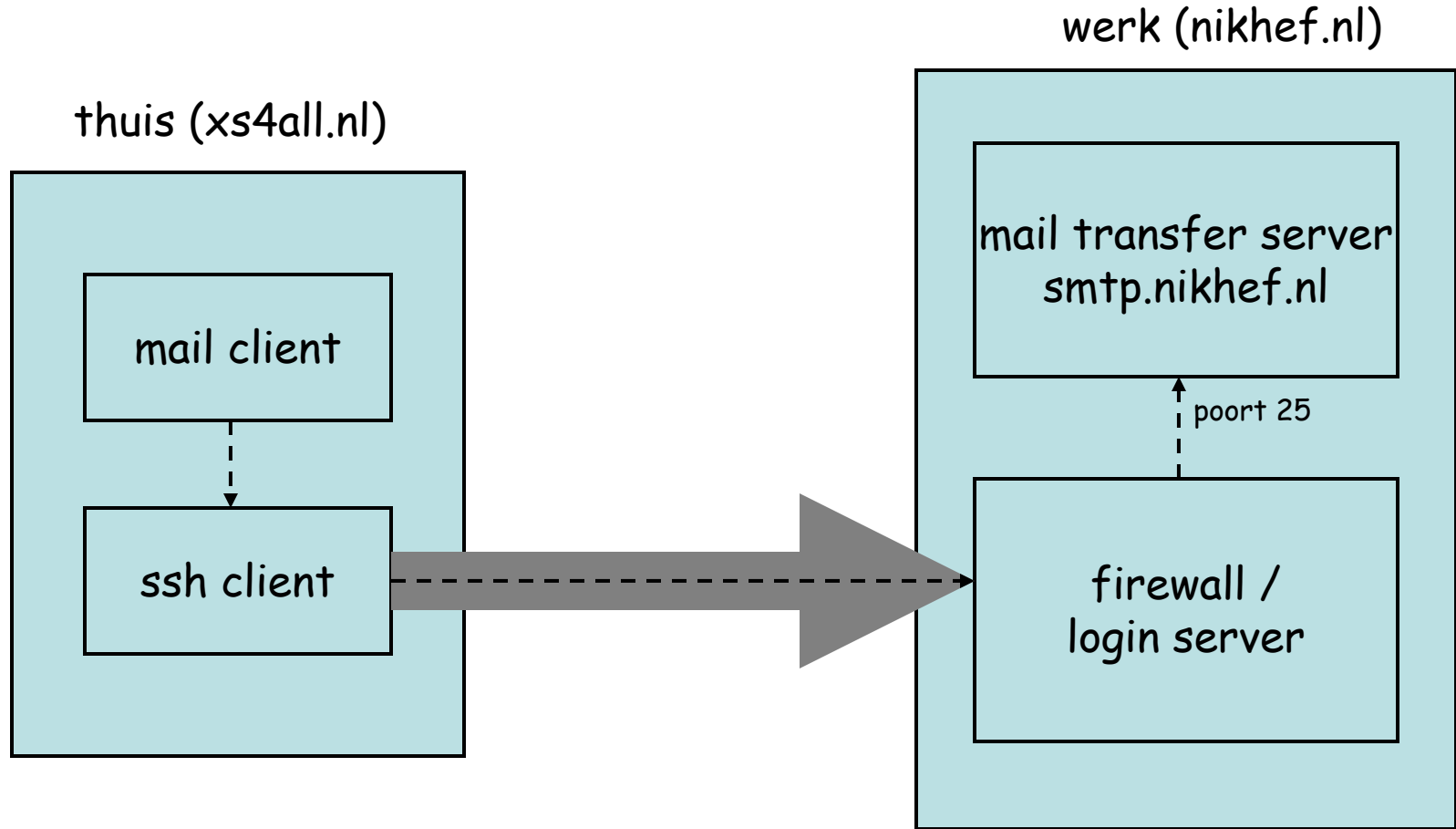
De voorgesteld wijzigingen in de firewall configuratie

- Blokkeren externe toegang alle desktops in het lokale 'Unixnet' (Linux en Solaris).
- Blokkeren externe toegang voor niet veilige varianten van imap en pop3 mail clients.
- [Mogelijk blokkeren van de directe toegang tot de SFTP server 'paling']

Een secure alternatief

- Port forwarding (tunneling) met SSH
 - Voor Windows en Linux clients
 - Werkt voor op TCP gebaseerde services
- X forwarding met SSH
 - Speciaal geval van forwarding voor X sessies.
- Port forwarding vereist het opzetten van een 'tunnel' in een geaccepteerde SSH verbinding.

Port forwarding



Voorbeeld: forward/tunnel poort 25 (smtp) van 'localhost' naar remote server

Port forwarding configuratie

- Stap 1: start SSH client naar 'login.nikhef.nl' met gewenste tunneling configuratie.
- Stap 2: start applicatie die van de tunneling gebruik gaat maken.

Voorbeeld: forward/tunnel poort 25 (smtp) van 'localhost' naar remote server

Linux:

1. Ssh -L2001:localhost:25 login.nikhef.nl
2. Start mail client (smtp server=localhost)

Windows:

1. Config. entry in 'tunnel' tab van 'profile':
listen port=25
dest host=smtp.nikhef.nl
dest port=25
en start SSH client naar login.nikhef.nl
2. Start mail client (smtp server=localhost)

Ten slotte ...

- Nog een secure alternatief: VPN ?
 - Vooral bedoeld voor standaard 'KA' toepassingen.
 - Centraal beheer client kant (bv thuis)
- Guestnet:
 - Beveiligen op MAC address
 - Gedragsregels ten aanzien van beheer laptops:
 - Updates Windows/Linux systeem
 - Updates Virus scanner definities
 - (voorbeeld gedragsregels binnenkort beschikbaar via ASTRON).

Vragen?