
Vulnerability Summary

March 2005



Paul Asadoorian
Lead IT Security Specialist
Brown University

Topics

 Windows LAND Attack

 OS X Security Update

 Linux Local Privilege Escalation

- Secure Remote Desktop For Free
- Future Topics Overview

Windows LAND Attack

- Affected products include Windows XP and Windows Server 2003
- Launch a TCP LAND attack (SYN packet) for DoS condition
- Requires that firewall allow traffic

Windows LAND Attack

- LAND attack is a packet with the same source and destination IP address
- Used to be able to hang Windows 95 and NT
- Its legacy lives on...

Windows LAND Attack

- No patches available
- Posted to public mailing list on March 3rd
- Exploit code exists, runs on windows

Windows LAND Attack

- Block all ports with a firewall
- Use a firewall to block this attack
 - Netscreen (Screen settings)
 - Checkpoint
- Most Intrusion Prevention systems

Windows LAND Attack

- Original advisory - <http://www.security.nnov.ru/docs7998.html>
- Exploit - <http://www.security.nnov.ru/files/newLand.zip>
- Original Advisories from 1997:
 - Windows NT Slows Down - <http://support.microsoft.com/default.aspx?scid=kb;en-us;165005>
 - Windows 95 Stops Responding - <http://support.microsoft.com/kb/177539/EN-US/>

OS X Security Update

- Security update 2005-003
- 11 total security fixes released
- Covers the following:
 - AFP (Apple Filesharing Protocol)
 - Bluetooth
 - Core Foundation Environment Buffer Overflow
 - Cyrus (IMAP & SASL)

OS X Security Update

- Folder Permissions (777)
- Mailman
- Safari (IDN Fix)
- Samba (Buffer Overflow)
- SquirrelMail

OS X Security Update

- Local privilege escalation exploit exists!
 - <http://downloads.securityfocus.com/vulnerabilities/exploits/xosx-cf.c>
- Run software update
- More info on all vulnerabilities:
 - <http://docs.info.apple.com/article.html?artnum=301061>

Linux Local Privilege Escelation

- Linux Kernels 2.4 and 2.6 vulnerable to local buffer overflow
- `uselib()` function can cause race condition which allows privilege escalation
- Worked on Gentoo x86 kernel 2.4.26

Linux Local Privilege Escalation

```
paulda@Sofie paulda $ id
uid=1001(paulda) gid=100(users) groups=100(users)
```

```
paulda@Sofie paulda $ ./pwned
linux kernel msync race condition
bug discovered by sd, further research by sd and *****
this is development-in-progress code, redistribution prohibited!
=====
creating fakepage
done fakepage
done 61440 Kb
creating swapfile
<SNIP>
y4'r3 1uCky k1d!
```

```
root@Sofie paulda # id
uid=0(root) gid=0(root) groups=100(users)
```

```
root@Sofie paulda # uname -a
Linux Sofie.pauldotcom.com 2.4.26 #1 Sat Mar 23 11:12:35 i686 Pentium
II (Deschutes) GenuineIntel GNU/Linux
```

Linux Local Privilege Escelation

- Claims to have been discovered in May 2004, vulnerability not public until January 2005
- Exploit code:
 - <http://www.packetstormsecurity.com/filedesc/pwned.c.html>
- Write-up:
 - <http://www.securityfocus.com/bid/12190>
- Upgrade or patch your kernel (Distribution dependent)

Secure Remote Desktop For Free

- Manage Windows from OS X
- Use SSH as the transport
- Make it easy to use (Coming soon)

Secure Remote Desktop For Free

- Applications required:

- TightVNC

- ▶ <http://www.tightvnc.com>



- OpenSSH For Windows

- ▶ <http://sshwindows.sourceforge.net>

- Chicken of the VNC

- ▶ <http://www.geekspiff.com/software/cotvnc/>

Secure Remote Desktop For Free

- Windows System Setup
 - Install TightVNC for VNC client/server
 - Install OpenSSH package (includes Cygwin)

Secure Remote Desktop For Free

- OS X System Requirements
 - Install OS X VNC for VNC server
 - Install Chicken of the VNC for VNC Client
 - Enable SSH in system preferences

Secure Remote Desktop For Free

- Configure TightVNC to only listen on localhost (127.0.0.1)
- Configure Windows SSH server to allow X11 connections
- Open Windows firewall to allow SSH
- Start both servers

Secure Remote Desktop For Free

- Connect to Windows SSH server:

```
$ssh -L 5900:localhost:5900 winhost
```

- Use Chicken to connect to VNC server on localhost
- Enjoy your secure remote desktop connection!

Secure Remote Desktop For Free

- Bonus
- Install RDC client for OS X and use RDP

```
$ssh -L 3389:localhost:3389 winhost
```
- Now just use RDC to connect to localhost
 - Make certain Remote Desktop is enabled and allowed through firewall
- Bask in your secure remote desktop glory

Threat Summary

Brown University

March 22, 2005

IP	Local Hosts Contacted	Port	Application
012.152.100.052	39,807	2100 TCP	Unknown
024.106.118.135	16,455	2082 TCP	Unknown
012.034.168.024	10,042	1521 TCP	Oracle
062.022.120.226	9,280	8000 TCP	Hp Web JetAdmin
063.207.135.203	8,982	Ping Sweep	Any

Future Topics Overview

- Hardening Windows XP
- Battle Spyware And Win
- Package-Based Linux with Gentoo
- Going behind the Campus Firewall
- Patch Management
- More Secure Remote Desktop

Article Of The Month

Local Man Finds His Tax Return on Internet

<http://www.wtoctv.com/Global/story.asp?S=3117022&nav=0qq6XpfR>

“Don Bodiker uses a popular file sharing program to swap music and other information over the internet. He also uses his computer to prepare his taxes. He never thought the two had anything to do with each other...”

/* The End */

Questions? Comments? Flame Mail? Donations?
Paul_Asadoorian@brown.edu

This presentation:

<http://www.brown.edu/Research/SysAdmins/vuln-march-2005.pdf>

Paul's Essential Security Links

<http://packetstormsecurity.nl/>

<http://www.security.nnov.ru/>

<http://www.cert.org>

<http://www.whitehats.com>

<http://rr.sans.org>

<http://www.incidents.org>

<http://www.astalavista.com/>

<http://www.l0t3k.org/>

<http://www.securiteam.com/>

<http://www.k-otik.com>