GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

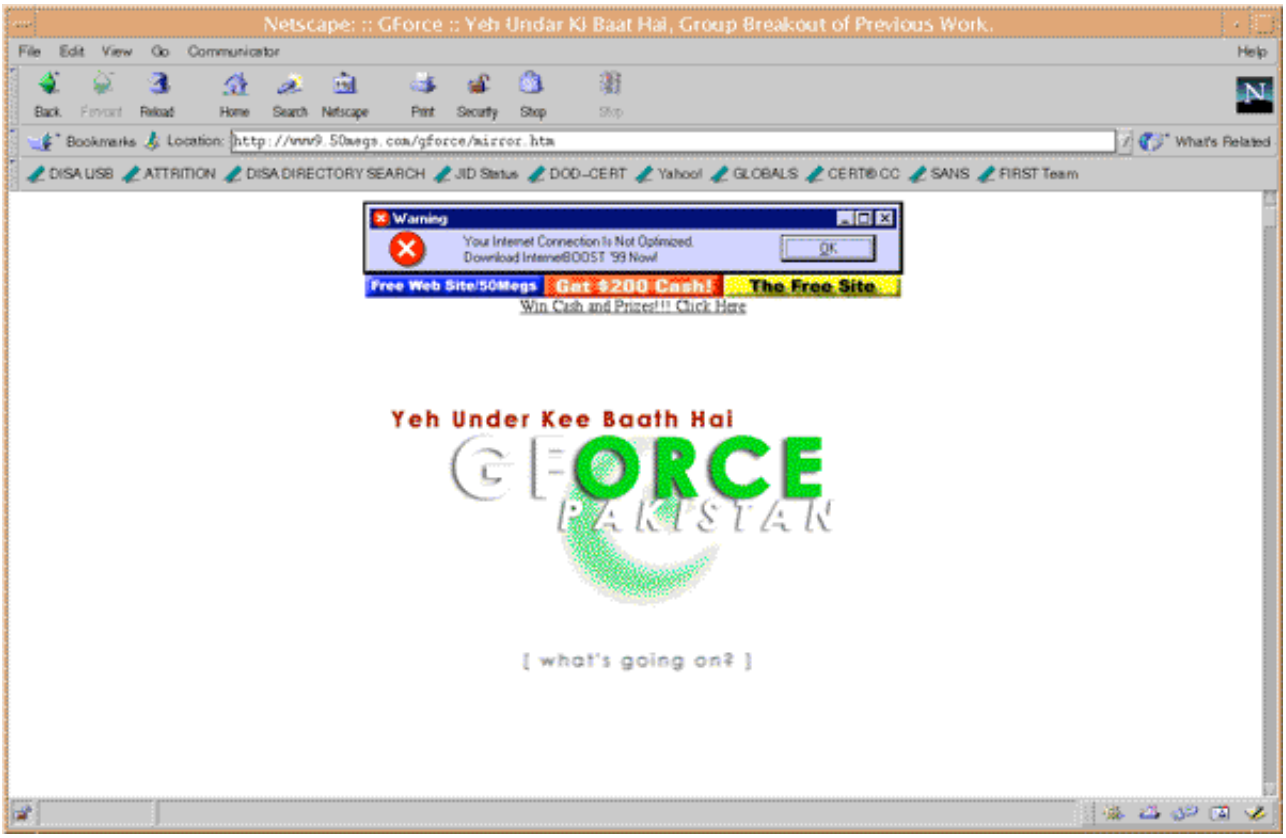
Hacktivism: Compromise Techniques Used by GFORCE-Pakistan
Michael L. Jenkins
October 24, 2000

Introduction

The sport for some hackers is to hack and alter the homepages of companies, groups, organizations, and even political parties. Hackers have realized that the Internet is the perfect forum for acts of electronic civil disobedience. The term "Hacktivism helped to put the spotlight on this new form of protest.

Hacktivism is the convergence of the term hacking with activism. Here, "hacking" is used to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help hacking tools. Hacktivism is civil disobedience in cyberspace.

Because hacking incidents are often reported in the media, hacked websites can generate considerable publicity for both the activists and their causes. The hacker group GFORCE-Pakistan has been very active recently and has become one of the best known Hacktivist. GFORCE-Pakistan conducted 189 root/web compromises since 3 July 2000. They were thought to be a state sponsored hacking group, but new information has given way to a group located in the U. S. with ties to the country. This Hacktivist organization uses several known vulnerabilities to hack into systems. Shared information received from various organizations reveals a pattern of compromise and targeted vulnerabilities that were commonly used by GFORCE-Pakistan. GFORCE-Pakistan is actively exploiting the S-ADMIND, WU-FTPD and ToolTalk vulnerabilities on the Internet. An explanation of each of these vulnerabilities is provided to help raise awareness. Once the computer had been compromised, the group then downloaded Apache Web Server software and turned the computer into a web server to function as a vehicle for their political rhetoric.



The Common Vulnerabilities

The S-ADMIND program is installed by default in Solaris 2.5, 2.5.1, 2.6, and 7. In Solaris 2.3 and 2.4, S-ADMIND may be installed if the Sun Solstice Adminsuite packages are installed. The S-ADMIND program is installed in /usr/sbin. It can be used to coordinate distributed system administration operations remotely. The S-ADMIND daemon is started automatically by the inetd daemon whenever a request to perform a system administration operation is received. All versions of S-ADMIND are vulnerable to a buffer overflow that can overwrite the stack pointer within a running S-ADMIND process. Since S-ADMIND is installed as root, it is possible to execute arbitrary code with root

© SANS Institute 2000 - 2005 Author retains full rights.

privileges on a remote machine.

A vulnerability exists with certain configurations of the SITE EXEC command in the Washington University FTPD also known as WU-FTPD. Exploitation of this vulnerability may allow root access from any account on the system. The vulnerable configuration is known to exist in numerous Linux distributions and is currently being actively exploited by GFORCE-Pakistan. It should be noted that this vulnerability is not necessarily limited to Linux but may exist on any WU-FTPD installation. Thus, all users of the wu-ftpd program, not just the Linux users, should take this opportunity to verify the configuration of their daemons. Note that versions of WU-FTPD before the 2.4 release contain serious security vulnerabilities and should be updated immediately.

An implementation fault in the ToolTalk object database server allows a remote attacker to run arbitrary code as the superuser on hosts supporting the ToolTalk service. The affected program runs on many popular UNIX operating systems supporting CDE and some Open Windows installs.

Technical Details:

Another twist to the compromise is that GFORCE-Pakistan would take previously non web machines and load web software that changed the machines into web servers. The information below is an example of how the compromise might be accomplished and what to look for on possibly compromised machines:

- rpc.ttdbserverd exploit used to invoke root shell on ingreslock port (1524/tcp) using /tmp/bob configuration file.
- Backup copies of etc/passwd and /etc/shadow made as etc/.tp and /etc/.ts
- Machine accepts telnet connection from source.
- Root kit retrieved from source to local system and placed in /usr.
- Root kit extracted
- Root kit installed using setup.sh. Replaced ls, ps, netstat, and login with trojaned versions. Touched modification times on trojan to match /bin/sh.
- Modifies the inode times on /usr/bin/ls, files in ' /usr/. '. Perhaps a backup.
- Compromised system receives another telnet connection from different source ip
- Intruder builds and installs apache. Source distribution in ' /../apcshe_1.3.6'. Installed in /usr/local/apache.
- User named "stmp" created
- inftpd invoked, machine connects via in ftpd[21900] from source ip
- /www content created

Possible IP addresses associated with compromises are 61.11.234.xxx

Recommendations

Ensure installation of all vendor patches. Disable the service daemon to prevent the vulnerabilities from being exploited and encourage sites to block all unused ports, specifically inbound ports 111/TCP & 111/UDP at the premise router and port 80, 8080, 443 to internet portion of network.

Summary

Hacktivism will always have a home on the Internet. But there are ways we can minimize of its use. Following security guidelines and remain constant and consistent with the security of our network, will not allow hackers like GFORCE-Pakistan to take advantage of basic exploits.

Sources

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism" The Internet as a Tool for Influencing Foreign Policy, Georgetown University .URL: http://www.infowar.com/class_2/00/class2_020400b_j.shtml

Attrition http://www.attrition.org/mirror/attrition/

CERT® Coordination Center, CERT® Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind, CERT® Advisory CA-98.11, CERT® Advisory CA-1995-16 wu-ftpd Misconfiguration Vulnerability, URL: http://www.cert.org/

© SANS Institute 2000 - 2005 Author retains full rights.