SANS/GIAC Practical Assignment
for GCIH Certification

Root Access Incident:

A CSIRT Directs the Handling of an Incident

By Robert Beauregard

Table of Contents

Section 1 - Executive Summary

The Computer Security Incident Response Team (CSIRT) of a large international company handled the root access intrusion incident described in this report. This incident is unusual in that the initial report of a possible compromise came from an anonymous company. The anonymous company reported that the source was probably compromised because of the attempted connections against their network that had occurred. The source Internet Protocol (IP) address was from one of our constituents that was at a different geographical location, a small company that had been recently acquired by our company.

This incident is also unusual in that it shows the actions taken by the CSIRT in the handling of the incident. The CSIRT is a third party in that it was not the intruder, it was not the one to identify the problem, and it was not the one to directly investigate and recover from the compromise. The CSIRT directed the actions of the constituent and provided assistance as they handled the incident.

This report describes the actions of the CSIRT as it handled the root access incident with the constituent. The report is organized to describe the six phases of incident handling as they pertain to this incident. The uniqueness of the incident was the fact that the CSIRT was the organization to inform the constituent of the compromise and directed their actions. The usual process begins with a constituent notifying the CSIRT.

Many circumstances combined to create the failure of network security policy that compounded and caused the incident. These include a lack of preparation, a failure to implement policy, faulty security practices, and a flawed organizational approach by the company. The follow-up and lessons learned section describes these in detail.

The CSIRT played an important role in directing and assisting the constituent in the handling of the incident and improving the security of the constituent's network.

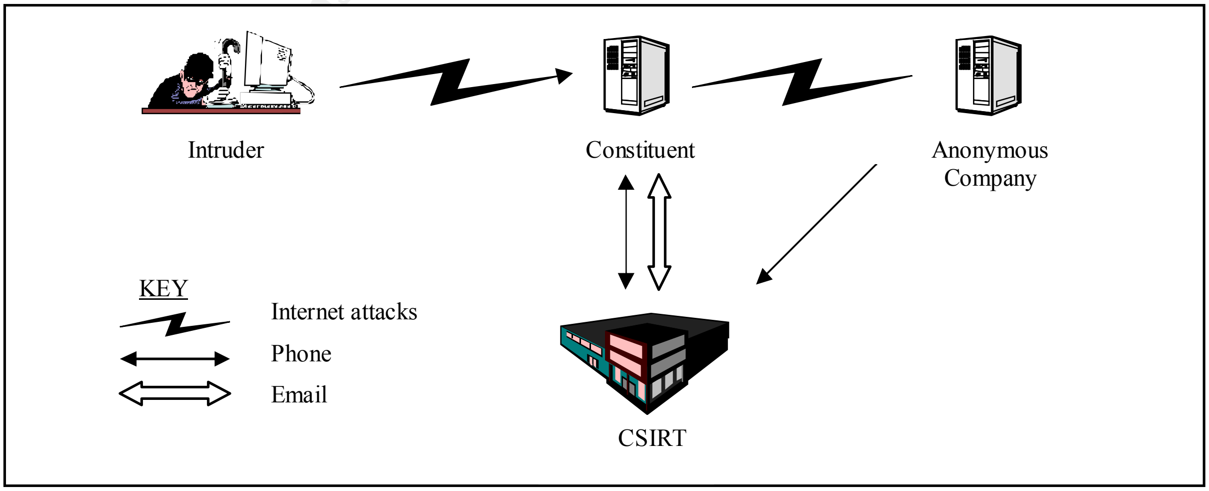

Figure 1. Incident Overview.

Incident Summary:

- Intruder accessed constituent's machine
- Intruder exploited rpc.statd vulnerability to gain root
- Intruder created user and root level accounts
- Intruder scanned anonymous company
- The anonymous company contacted the CSIRT
- CSIRT contacted the constituent
- CSIRT assisted and directed identification, containment, eradication, recovery, and follow-up

Section 2 - The Six Phases of Incident Handling

This section describes the six phases of the computer security incident handling process and how they were applied in the handling of this incident. The SANS Institute developed these six phases in cooperation with many other computer security professionals throughout industry, government, and education, see ref [1]. The phases described in this report shows the unique approach taken from a perspective of a CSIRT of a large international company directing the constituent in the handling of an incident.

Phase 1 – Preparation

The Preparation Phase of incident handling involves the establishment of policy that identifies the company's approach to network security. The approach includes the establishment of network security policy (e.g. user password and firewall services policy). It also addresses the need to protect the company legally by providing logon-warning banners for all connections and warn users that they may be monitored. In addition to policy, preparation includes the establishment of a centralized location for dealing with the issues of network security on an operational basis.

CSIRT Preparation

The large international company has network security and user policies that are formally published and issued throughout the company. These policies include specific procedures for ensuring a high degree of network security throughout the company. Among the most important is the use of a firewall policy. The firewall policy that my company uses is strict in that it was designed to allow the minimal of services. If a division within the company needs to use additional services, they must obtain authorization from management.

Users who receive new accounts are briefed and sign statements of understanding of the company's network security and presumption of privacy policies. They also sign a statement indicating that they have read and understand that any activity on the company's systems is considered the property of the company. The user is warned that unacceptable behavior can result in termination of their employment.

Another area of policy that our company has in place is the use of logon warning banners. The warning banner reminds users of the company policy each time they log on. By signing on, the user indicates that they understand and agree to abide by the policy.

Our CSIRT is relatively new. It is modeled after and functions similar to the Computer Emergency Response Team Coordination Center (CERT/CC) of the Software Engineering Institute (SEI) at Carnegie Mellon University, Pittsburgh, PA. To create our CSIRT, we combined the existing computer security policy and technical staff and responsibilities that already existed at the company headquarters. The CSIRT responsibilities include identifying network vulnerabilities, alerting constituents to new vulnerabilities, and providing an incident response capacity for the entire company. Our role has expanded and we have added the capability to scan company networks for vulnerabilities.

The communications for our CSIRT were set-up like a help-desk. There is an established CSIRT email address, toll-free phone number, fax-machine, and after-hours pager number. The pager is routinely passed around amongst the CSIRT members on a weekly basis. CSIRT members have a copy of a recall list of key members within the organization. Non-urgent email requests and incident reports are managed using a trouble-report tracking application, which assigns an incident tracking number and allows for the databasing of related information.

To improve the knowledge and skills of the CSIRT staff, we have provided additional training. This training included the introductory, advanced, and management level incident handling courses provided by the CERT/CC. Additionally, we have expanded the training that is provided to our CSIRT personnel to include the various levels of training and certification provided by the SANS Institute.

The CSIRT has worked previously with law enforcement and continue to build that relationship. In this incident, the CSIRT directed the constituent to work with their local law enforcement. We directed actions that would preserve the evidence and provide for a chain of custody.

Constituent Preparation

Our company had recently acquired the constituent involved in this incident. They did have network security policies that were similar to the parent company, but they were not strictly enforced. The particular machine that was compromised in this incident was a unique situation that was allowed to fall out from under those policies. The constituent did have a policy on presumption of privacy and also had logon-warning banners.

The management of the constituent was fully supportive of all actions to secure the information systems when made aware of the problem. Management was willing to listen and learn both from the system administrator and the CSIRT.

The constituent had good security policies but employed poor security practices. Additionally, the policy of the large international company was not overlooked in this incident. The recently acquired company, the constituent, did not know the policies existed.

Phase 2 – Identification

The Identification Phase of incident handling involves being able to identify that something is out of the ordinary and taking appropriate actions to identify the cause. When incidents occur, they may be obvious, but often are not. The key to successful identification is performing audits on your systems.

Initial Indication

The CSIRT received the telephone notification from the Anonymous Company October 22, 1999, at 9 A.M. The Anonymous Company reported that one of our constituents might be compromised because of the attempted connections they were seeing against their network. They provided us with dates, times, source IP/ports, and target IPs/ports. The activity was blocked by their firewall and they had blocked the source IP at the router.

Incident Handling Team Members

For the constituent, there was no option as to who would be part of the incident handling team; the one system administrator and her assistant would comprise the team. As for the CSIRT, the team was comprised of the incident handler who first received the information and had notified the constituent.

CSIRT Directed Identification Actions

The fact that the Constituent was recently acquired; it took a little time to gather Point of Contact (POC) information. When we found the information we notified the constituent using the telephone. We had to discuss the roles of the CSIRT because they were not familiar with us. We provided them with the information we had received and exchanged contact information including email addresses. We directed them to begin investigating and told them that we would immediately follow up with an email.

The email that we sent them included the information that we had received from the Anonymous Company and a summary of what had been discussed on the telephone. The Constituent was not sure how to proceed in the investigation so the email included very specific actions that were required.

The following is a list of the specific guidance that was provided:

1. Notify management.
2. Document all of your actions.
3. Search for signs of a compromise use the appropriate intrusion detection checklist below, ref [2] and [3]:
    a. For Unix, utilize CERT/CC's Intrusion Detection Checklist, http://www.cert.org/tech_tips/intruder_detection_checklist.html

   b. For Windows/NT, utilize CERT/CC's Windows NT Intruder Detection Checklist, http://www.cert.org/tech_tips/win_intruder_detection_checklist.html

4. If signs of a compromise exist, disconnect the machine from the internet/network with management's approval.
5. Make an initial report to the CSIRT utilizing the following form, ref [4] (which is similar to our CSIRT's Report Format):
   a. CERT/CC's Incident Reporting Form, http://www.cert.org/reporting/incident_form.txt
6. The CSIRT will provide additional guidance at that time.

Note: Please contact the CSIRT at any time for assistance.

The CSIRT called the constituent later that day. The constituent reported that they had not yet found anything, but would continue searching. The next morning, the constituent reported that they were compromised at the root level.

Constituent Identification Actions

The constituent followed the CSIRT recommended actions and reported the following morning that the machine in question was compromised at the root level. The machine was a Sun Ultra2 UltraSparc operating with SunOS 5.4, IP address XXX.XXX.22.20. The machine was using a proprietary software application for the sole purpose of collecting telephone statistics and monitoring telephone activity. The static connection to the Internet was with a local Internet Service Provider (ISP). The machine was not connected with the other, primarily Windows NT, servers on a class C subnet. These machines were behind a firewall and were not compromised. The Sun machine was not behind a firewall.

When the constituent reported, we also learned that the compromised machine was not configured with security in mind. The OS did not have the current patches and unnecessary services were allowed that provided easy access to an intruder.

It was further discovered that a contractor had installed the Sun machine under contract. The contract had called for the installation of the machine and proprietary software and for the maintenance of the machine for a period of one year. The one-year period had recently ended and the responsibility for administration of the machine had been turned over to the constituent's system administrator two weeks prior to the incident.

The contractor had all auditing features disabled, which the system administrator had not changed, and no log files were available. When the contractor was providing the support, there were no problems and the support was flawless. The performance and functionality of the machine remained reliable even after the transition from the contractor. From the system administrators' point of view, it was working fine and there were no problems with it.

Incident Identification

The constituent reported that the intruder gained access to the machine, probably by using anonymous ftp, and gained root access. No immediate evidence was discovered to indicate that any data files had been modified or deleted. The intruder had obtained root access, created two accounts (with user and root privileges), and covered his tracks by deleting logfiles. The following is a summary of what was discovered by the Constituent and reported to the CSIRT:

1. Compromised at root level
2. Two new accounts were created (one user and one root level)
3. Intruder had deleted logfiles to protect his tracks. The constituent was not able to provide any log files and explained that the intruder must have deleted them.
4. No data files appeared to be deleted or modified
5. Intruder had installed various tools
6. An old user account was also discovered as being active recently. This indicates that the Intruder had captured the password file and probably had all account passwords (by using a password cracking tool against it). The password file was not shadowed out.
7. The first-layer source IP of the intruder was not discovered. All auditing and logging features were turned off or never enabled to begin with.

Phase 3 – Containment

The Containment Phase of incident handling involves taking steps to prevent the incident from getting worse. This includes taking the compromised machine offline (with management's approval), conducting full backups, changing passwords, and checking other systems.

CSIRT Directed Containment Actions

When the Constituent reported that they had found signs of a root compromise, we provided them with additional actions to take. The CSIRT tried to provide the constituent a calm approach with clear, specific guidance, which would help them investigate and contain the incident. These included:

1. Continue to document all actions.
2. Verify that the machine is disconnected from the internet/network (with management's concurrence).
3. Perform a full backup of the compromised system. The backups may be used for law enforcement purposes.
4. Label the tapes with the following information:
   a. Company name
   b. Point of contact name
   c. Point of contact phone number
   d. Date and time
   e. Type of backup performed
   f. Machine type and operating system
5. Limit access to the backups by locking them in a secure location with a limited amount of access.
6. Change all root and user passwords.
7. Contact local law enforcement.
8. Verify other machines have not been compromised. See Identification guidelines previously provided.
9. Provide an updated report to the CSIRT.
10. Contain the incident by utilizing the following checklist, CERT/CC's Steps for Recovering from a UNIX or NT System Compromise, ref [5]: http://www.cert.org/tech_tips/win-UNIX-system_compromise.html (Note: This provided guidance for the Containment, Eradication, and Recovery Phases.)
11. Provide an updated report to the CSIRT.

Note: Please contact the CSIRT at any time for assistance.

Constituent Containment Actions

The constituent performed the recommended steps that we provided. The administrative functions of the server were such that the decision was made by management to disconnect the machine and continue with the investigation. The system administrator changed all root and user level passwords after the initial backups were made. The constituent did not find signs of compromise on the machines that were behind the firewall.

Phase 4 – Eradication

The Eradication Phase of incident handling involves taking the steps to identify and remove the vulnerability that was exploited to compromise the system. Eradication also includes the actions necessary to harden the system.

CSIRT Directed Eradication Actions

A very popular vulnerability that was being exploited at the time period of the incident was the vulnerabilities associated with rpc.statd. The CSIRT had searched vulnerabilities associated with SunOS 5.4 and sent the constituent the following to aid in the eradication:

- CERT® Advisory CA-99-05 Vulnerability in statd exposes vulnerability in automountd, ref [6], http://www.cert.org/advisories/CA-99-05-statd-automountd.html

- CERT Incident Note IN-99-04 Similar Attacks Using Various RPC Services, ref [7], http://www.cert.org/incident_notes/IN-99-04.html

Constituent Eradication Actions

The system administrator went through the intrusion detection checklist and the steps for recovering from a compromise checklist and made the appropriate fixes. They reported that the vulnerability exploited was the rpc.statd vulnerability, ref [6].

The steps taken to remove the cause of the incident and improving defenses included:

a. Locating the most recent clean, full backup. Note: These were from just over two weeks prior. This backup appeared to the latest before the intrusion. One issue was the reliability of the data. No applications (e.g. Tripwire) were being used to ensure the integrity of the data.
b. Installing the patch for the rpc.statd vulnerability, see ref [8]. Available at http://sunsolve.Sun.COM/pub-cgi/findPatch.pl?patchId=102769&rev=07.
c. Unnecessary services were disabled and commented out.
d. The passwords were placed in the shadow file so only "root" would have access.
e. Inactive accounts and accounts without password were disabled.
f. Before any of the fixes were performed, the most recent, clean full backup was installed.
g. The compromised system was reconfigured to be behind the firewall.
h. The firewall policy was modified to be in compliance with our stricter firewall policy.
i. Anti-viral software was updated.

Phase 5 – Recovery

The Recovery Phase of incident handling involves taking actions to restore and validate the system. This phase also requires that the system be monitored after the system is restored.

CSIRT Directed Recovery Actions

When the constituent had completed all recovery actions, the CSIRT performed a vulnerability scan using the Internet Security Systems (ISS), Internet Scanner, see section 3 and ref [9].

Constituent Recovery Actions

After the system was restored from the most recent, clean backups and installing the required patches, the constituent performed another full backup prior to placing the machine back on the network.

The fact that the system wasn't being monitored before, which probably would have identified the intruder's activity sooner, it was vital that system be monitored closely, now that the system was placed back in operation.

The system administrator made checks to ensure machine worked. Users were asked to try it also. Afterwards, management was told of the status and approved placing it back on-line. However, the machine was not connected to the Internet directly. It was determined that it was connected to the Internet so that the contractor could access it remotely.

Based on the actions performed to this point, management had made the decision to place the machine back on-line.

After the CSIRT had performed the vulnerability scan, the constituent fixed the identified vulnerabilities and performed yet again, another full backup.

Phase 6 – Follow Up / Lessons Learned

The Follow Up & Lessons Learned Phase of incident handling involves learning lessons from the incident that had occurred and to improve computer network security. Follow-up is required to ensure that required actions are completed.

Follow Up

The follow-up taken by the CSIRT was to prepare an incident summary that documents the general facts of the incident. This summary report was provided to management at both locations.

A subsequent network vulnerability scan was conducted a couple of months after the incident described in this report. This second scan resulted in only a small list of "low" vulnerabilities identified.

The company has also incorporated many of the actions identified in the below list of lessons learned. The two most significant changes that resulted from this incident include the company-wide annual vulnerability scanning and the incorporation of network security related issues into the company's merger/acquisition planning documents. These changes have resulted in a greater workload for the CSIRT staff but have provided the sense of reward by knowing that our company's networks are more secure.

An additional follow-up that was performed was the release of a CSIRT Advisory throughout the company that provided general good security practices. The alert addressed the areas of auditing, performing backups, firewall policy, passwords policy and password file protection, vendor patches and updates, common web-site vulnerabilities, and the importance of maintaining keeping anti-viral software updated. The alert also included a summary of company-required actions to take when an incident is suspected. This CSIRT Advisory was one that management was very happy about.

Lessons Learned

The CSIRT learned the importance of documenting all actions. The process of creating this report has shown the weaknesses of the CSIRT's documentation processes. We learned that even though our large international company is proactive when it comes to network security, it will take more proactive measures to ensure policies are in place at all company locations. Perhaps the biggest lesson learned was the failure of the company's acquisition/merger transition plans to adequately address network security issues.

The constituent learned to abide by security advisories released by the CSIRT and vendors. They have learned to incorporate good network security practices such as protecting all assets with a firewall, conducting auditing, protecting password files, and remaining current on vendor patches and fixes for known vulnerabilities. The constituent also learned about the company's policies, CSIRT services, and incident reporting requirements.

It was determined that the true cause of the root level intrusion was a total lack of security policy implementation on the machine that was compromised. Basically, using the OS out of the box allowed unneeded services. Additionally, available patches had never been installed. The machine compromised was the only machine that was not behind a firewall. In this incident, there were no symptoms that indicated that anything suspicious was going on. The only indication that something may be wrong was the report that we had received from the anonymous company. This was a result of not performing auditing.

The incident described in this report occurred primarily because of a failure of network security policy implementation. The reasons for the failure are great (which explains the long list below). There is a positive outcome from this incident - the company's network security policies and practices have improved as a result of this incident.

Company Policy Lessons Learned:

- ❑ Incorporate detailed network security guidelines into merger and acquisition transition plans.
- ❑ Direct annual network security scanning of all company network assets.
- ❑ Direct password checks.

CSIRT Lessons Learned:

- ❑ Obtain detailed, specific information when receiving an incident report from outside of the company. The report should include logfiles that support the reported activity and specific details of what was discovered.
- ❑ Utilize alternative communications when working with a constituent whose network has been compromised. Depending on the extent of the compromise, the intruder may have seen the emails and could have taken measures to cover his tracks and possibly take destructive actions.
- ❑ Obtain and retain copies of the logfiles that show the activity of an incident, regardless of how the incident was reported.
- ❑ Prepare CSIRT Incident Pre-planned Responses or "Jump Bag."
- ❑ Develop a company wide policy for performing backups and maintaining off-site storage.
- ❑ Develop detailed network security guidelines for inclusion into company merger and acquisition transition plans.
- ❑ Develop a company wide password policy that includes authority to check passwords using tools such as L0phtcrack and Crack, see refs [10] and [11].
- ❑ Develop a company wide policy for the use of file integrity tools such as Tripwire, see ref [12]. The use of these tools would have aided during the handling of this incident.
- ❑ Proactively contact system administrators and security managers of new constituents to obtain POC information and ensure compliance with company network security policy.
- ❑ Prepare a proposal to obtain resources to contract a network security consultant to perform a network security review at all of company locations worldwide.
- ❑ Develop a list of company network assets to better understand and serve our constituents. This knowledge would help focus our search for vulnerabilities and make us more

proactive in the issuing of advisories to our constituents. The list could include the following:

- Contact Information (including email address, pager and after-hours numbers)
- System Administrator information such as training, experience, and certifications
- Hardware
- Operating Systems and Applications
- Network configuration and architectures
- Firewalls/routers
- Anti-virus software

Constituent Lessons Learned:

- ❑ Perform auditing of all network assets.
- ❑ Maintain operating systems and applications with current vendor patches and updates.
- ❑ Maintain firewall policies and router access lists in accordance with company policies and good security practices.
- ❑ Maintain network assets behind a firewall. Exceptions may include public web servers.
- ❑ Protect password files by creating shadowed password files.
- ❑ Document all actions taken and facts discovered during the investigation of an incident.
- ❑ Make two full backups to document evidence of an incident; one backup is for law enforcement evidence and the second backup is kept for recreation of the incident.
- ❑ Enforce strict password policy.

Section 3 - Assessing and Containing the Incident – The Process

This section describes the process and actions taken to assess and contain the incident. This section will not present the actions described previously in this report. The information presented is for the specific compromise of the one UNIX machine. However, similar steps were also taken with the Windows NT machines. No compromise was discovered on the Windows NT machines, however, vulnerabilities were discovered in the process and those security vulnerabilities were also secured.

The CSIRT did not have an established incident "Jump Kit." The guidance the CSIRT provided was based on the experiences that we have had. However, the guidance and support that we provide should be formalized as a list of pre-planned response or "Jump Kit." The CSIRT did provide the system administrator with checklists to use to look for signs of compromise and recover from the incident.

After the constituent system administrator had completed the Eradication Phase, the CSIRT performed a vulnerability scan of the constituent's entire network using ISS Internet Scanner. The vulnerability scan identified a large number of high, medium, and low vulnerabilities. The constituent system administrator took the actions required to secure the vulnerabilities identified in the scan.

Section 4 - Backing Up the System – The Process

This section describes the process to back up the machine that was compromised. The machine was a Sun Ultra2 UltraSparc operating with SunOS 5.4 without security patches. When it was discovered that the machine was compromised, the CSIRT directed that a full back up be performed to provide law enforcement with evidence.

The constituent's system administrator, reportedly, was routinely performing backups and was familiar with the procedure. Additionally, the contractor who had recently turned over the machine had shown the system administrator how to perform the backups.

The full backup performed was performed using the "**dd**" command and the back up was to a Sun Digital Data Storage Drive using 4mm Data Tapes (12GB).

The next section describes how the backup tapes were labeled and handled.

Section 5 - Evidence Handling – The Process

This section describes the process and actions taken to handle the evidence from the intrusion of the UNIX machine. When it was discovered that the machine was compromised, the CSIRT directed that law enforcement be notified after the backup was completed. The CSIRT directed that the backup tapes be labeled with the following information:

- Company name
- Point of contact name
- Point of contact phone number
- Date and time
- Type of backup performed
- Machine type and operating system

The CSIRT also directed that the backup tapes be locked in a safe until given to law enforcement. The tapes were locked in a manager's safe. Only the manager and his assistant had the combination. The backup tapes were given to law enforcement when they arrived and they conducted brief interviews and took statements from management and the two system administration personnel. Law enforcement had left a copy of a custody document that had been signed by both the law enforcement agent and the constituent system administrator.

As described in the lessons learned phase, it would have been a good idea to make two backups. If two backups had been made, one could have been provided to law enforcement and the system administrators could have used the other for incident reconstruction. Consequently, a second backup tape would have been helpful in preparing this report.

Law enforcement later indicated that the incident was closed primarily due to lack of evidence. They also indicated that the because of limited resources and the relative insignificance of the case, the investigation would not move forward. However, they maintained possession of the tapes for evidence if the case is ever reopened.

References

[1] The SANS Institute, Computer Security Incident Handling: Step-by-Step, available for purchase at http://www.sans.org/newlook/publications/incident_handling.htm and table of contents viewable at http://www.sans.org/newlook/publications/incident_handling_toc.htm

[2] CERT/CC's Intrusion Detection Checklist,
http://www.cert.org/tech_tips/intruder_detection_checklist.html

[3] CERT/CC's Windows NT Intruder Detection Checklist,
http://www.cert.org/tech_tips/win_intruder_detection_checklist.html

[4] CERT/CC's Incident Reporting Form,
http://www.cert.org/reporting/incident_form.txt

[5] CERT/CC's Steps for Recovering from a UNIX or NT System Compromise,
http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

[6] CERT® Advisory CA-99-05 Vulnerability in statd exposes vulnerability in automountd,
http://www.cert.org/advisories/CA-99-05-statd-automountd.html

[7] CERT Incident Note IN-99-04 Similar Attacks Using Various RPC Services,
http://www.cert.org/incident_notes/IN-99-04.html

[8] SunOS5.4 patch for rpc.statd vulnerability,
http://sunsolve.Sun.COM/pub-cgi/findPatch.pl?patchId=102769&rev=07

[9] Internet Security Systems, Internet Scanner,
http://www.iss.net/securing_ebusiness/security_products/security_assessment/internet_scanner/index.php

[10] L0phtcrack (for Windows/NT),
http://www.securitysoftwaretech.com/l0phtcrack/index.html

[11] Crack (for UNIX), http://www.users.dircon.co.uk/~crypto

[12] Tripwire 2.2.1 (Commercial version), http://www.tripwiresecurity.com