

How To Conduct A Security Audit

Information security encompasses more than just IT systems - people who use the systems can also inadvertently open security loopholes. A security audit aims to detect and highlight any problem areas within the IT infrastructure and staff behaviours.

By Justin Kapp

Before you can assess what you are securing or about to audit it is important to understand what it is you are protecting. Your final goal is to have your information secured and to minimise the risk of losing this information.

Firstly we should define what information security is. Information is an asset; like other important business assets it has a value to an organisation and consequently it needs to be protected. Information security protects this business asset from a wide range of threats in order to preserve business continuity, maximise return on investment and reduce damage to business.

Information exists in many forms. It can be printed or written on paper, stored electronically, transmitted by post or email. Whatever form the information takes and however it is stored, it's important to protect it appropriately.

Information security is characterised as the preservation of confidentiality, integrity and availability of the information under your control. Information security is achieved by implementing a suitable set of controls - policies, practices, procedures, organisational structures and software functions. Information security is not just about your IT measures but also about the human interface to the information.

The Security Audit

A security audit is a policy-based assessment of the procedures and practices of a site, assessing the level of risk created by these actions. A secu-

rity audit comprises a number of stages, summarised in Figure 1. These stages will be covered in more detail later.

You can choose to focus the audit on different areas, such as the firewall, host or network. However, a security audit will address issues with your IT systems, including software and hardware, your infrastructure (such as mains power, telecomms), your procedures and business processes and your people.

Information is key. Once the audit has been completed you will have information on the compliance level of the users and systems under your control, with an idea of the risk exposure and security level of these systems. You will also have an idea of the potential damage that could occur if the worst came to the worst - this enables you to plan and develop a strategy to ensure minimal damage.

You can choose to carry out an audit internally or to use an external contractor. Whoever carries out the audit should have the relevant technical ex-

pertise and ability to communicate the findings of the audit.

It is also important that the auditor has an understanding of the organisation under review. When auditing systems that hold data which requires security clearance from government, then the auditor must have the required clearances in order to access the systems holding the data.

When you perform a security audit it is important to look beyond the IT systems and consider also the human interface to your IT. Your IT system may be perfectly secure, but your users may be involved in practices that compromise the security of the IT systems in place.

As a result any audit must attempt to identify all the possible risks. Your IT systems are at risk from compromise from a number of sources, including poorly-managed or badly-configured systems, internal users, external users and external attackers (sometimes known as crackers or hackers).

Even authorised system users can be the source of a security breach, so

“When performing your audit you will use any security policy that your organisation has as a basis for the work you are undertaking. You need to treat the policy initially as a threat.”

identifying possible lapses that could allow this is just as important as preventing external attack.

Risk Analysis

During the audit you will need to understand a little about Risk Analysis and Risk Management - a security audit is all about assessing the risks of loss, compromise or damage to information.

Risk analysis is the process of identifying and assessing the risk of something happening. Space does not allow us to cover risk management and analysis in detail, but its principles are summarised here:

- The establishment of mechanisms to keep risks under review and to make sure they are being addressed
- A means of identifying the potential risks to the business
- An assessment of the likelihood of each risk materialising
- An assessment of the probable impact of each risk
- The formulation of measures to avoid each risk occurring
- The development and deployment of fallback measures to mitigate the risks if avoidance actions fail
- The determination of the urgency of the risk and of taking appropriate counter measures.

It is recommended that those who will be carrying out the security audit familiarise themselves further with risk management and analysis theory before commencing.

Preparation

During your preparation for the audit you have to decide how you are going to bias your audit. You need to decide in what depth you are going to audit the systems.

IT systems comprise a number of components, including hosts, servers, firewalls and the network; you must decide how deep you plan to delve into each of these components. Some systems, by their nature, require a greater level of scrutiny to determine the security issues that may be present.

It is also important to plan the angle

of attack for the audit of the IT systems. During the audit you may need to restrict access to some of the systems under test; these tests should be performed out of business hours to minimise impact on day-to-day operations. You will also need to schedule time with a selection of staff members to assess how they operate within the security policy. You need to prepare a series of questions to use during the discussions with staff members.

Before you begin you need to verify your audit tools and environment. This includes the golden rule of all security auditing - you must verify that all tools used for the audit are untampered with; if the results of the auditing tools cannot be trusted, the audit is useless.

You many suffer from a "chicken and egg" problem when it comes to verifying your audit tools. In order to verify your audit tools you need to use the audit tools. So how do you establish the trust in your audit tools? You could write them yourself or find a trusted source such as a person or company. The easiest solution is to use a tool such as md5sum to create a checksum of the file, which can be used to verify the tool later - or to use a digital signature of the tool created with PGP.

What Tools?

Over the last few years a number of tools have been developed to aid the system administrator. These tools run on a number of platforms including Win32 (Windows NT/9x), Linux, Solaris and FreeBSD. There are a number of types of tool - those that detect changes in system configuration, tools that test for known security issues and a class of tools that are used to monitor systems in real time, such as network sniffers.

Figure 2 shows a small selection of the audit tools that are available today. Tools that run on Windows platforms tend to be commercial in nature. A large number of the tools available for the various types on Unix are non-commercial and can be obtained at no charge from the Internet. Unix tools are often supplied in source code, so testing the authenticity of the tool is easier.

You must decide which platform to use for your audit. The best choice will have a high level of security. It should not run any network services, and should be configured as if the machine was to be used as a firewall or other form of secure host. Another important factor is that physical access is required to use the machine.

The ideal hardware platform is a notebook computer, with a good display, 64 MB of RAM and a large hard disk (4 GB plus). It is also important to have network connectivity (usually via a PC Card); in order to provide filtering and logging, in fact, it is useful to have more than one network connection. There are many brands of notebook available which would fit the bill - for instance, the HP Omnibook 4150. Sometimes discreet monitoring may be required, so machines such as the sub-notebook, which can easily be hidden, are often useful.

On the audit platform a suitable operating system (OS) should be chosen. The operating system considered should be able to be secured, have suitable audit tools available, have various development tools available such as Perl and a C/C++ compiler. It is also a large advantage to have the OS source code to prove the security of the operating system. Another important feature for the audit platform operating system is that, once put into a network to be audited, the operating system doesn't alter the normal operation of the environment to be tested.

If you are choosing a Unix, then you have a number of choices including Linux, FreeBSD, Solaris and SunOS. Choosing the right one depends on the hardware you are planning to use and

Stage	% Of Total Time
Preparation	10
Reviewing Policy/Docs	10
Talking/Interviewing	10
Technical Investigation	15
Reviewing Data	20
Writing Up	20
Report Presentation	5
Post Audit Actions	10

Figure 1 - Summary of the stages of a security audit.

Security Audit

“You need to determine usage patterns, and whether users have seen and read the security policy. Find out what they can and can’t do, in their own words.”

the features required by the audit tools you are using. For instance, a tool such as nmap will require certain OS features in order for you to get the best out of the tool.

If you are choosing a Windows platform you only have one real choice - Windows NT Workstation. This should be configured with the latest service packs and hotfixes. However, some of the more useful tools do not run on Windows platforms.

It is a good idea to be able to boot the machine into more than one operating system. That way you have access to multiple test platforms to try different tools to audit the network. Once you have built your test platform it is a good idea to create a machine image using an application such as Norton Ghost, and to burn the image

to CD. This tamperproof image can then later be used to restore the test machine to a known state if required during the audit - or for a future audit.

The Security Policy

When performing your audit you will use any security policy that your organisation has as a basis for the work you are undertaking. When performing an audit, you need to treat the policy initially as a threat. You need to determine whether the policy covers all the basic components of security policy documents. Are the security configurations comprehensive?

Is the policy a threat? Badly written policies are worse than none at all; however, good policies are very rare. So it is important to look for clearly

written policies in plain English - many of the people who have to read these documents are not technically minded.

It is also important to look for completeness in the policy document. You need to determine whether the policy components specify who can use the resources and whether they define the proper use of the resources available. Information needs to be provided regarding the procedure for granting access by administrators and what should be done with sensitive information. Information should be provided regarding the types of privileges available to administrators and to users.

Consider whether the security configurations are comprehensive. The details are important; do they address specific technical issues? Is allowable trust clearly outlined, and are specific tools that are used defined?

You also need to determine the dissemination procedures for the security policy. A security policy is worthless unless people read and understand the document. You need to assess how well staff understand the security policy. It is important that there is a procedure for disseminating the document; this procedure could use any transport method but, once received, it is important that there is a method for acknowledging the receipt and reading of the document.

What happens if there isn't a security policy? In order to complete a security audit successfully you need to have an idea of boundaries. If there is no defined security policy it may be necessary, before you start, to define one or, at least, once the audit is complete, recommend that one is created. If you continue without a security policy then, while the audit is underway, you should use a guide to best practice for policy guidance. The *“Site Security Handbook, RFC 2196”* is a good starting point.

Gathering Info

The actual audit involves performing interviews with staff members and talking to people in a more informal manner. This element is often overlooked and it is quite important. You

Tool	Platforms	Type
COPS/Tiger	Linux, Solaris, Other Unix	Change/Intrusion Detection
Crack	Windows, Linux, Solaris, Other Unix	Password cracking
L0phtCrack	Windows NT	Password cracking
ISS	Windows NT, Linux, Solaris, HP-UX	Suite - Port scanner, network information
nmap	Linux, Solaris, Other Unix	Port Scanner
tcpdump	Linux, Solaris, Other Unix	Network Monitoring
sniffit	Linux, Solaris, Other Unix	Network Monitoring
CyberCop Security Scanner	Windows NT, Linux	Suite - Port Scanner, Password cracking, network information
Nessus	Linux, Windows NT, Other Unix	Exploit tester
TripWire	Unix	Change/Intrusion Detection

Figure 2 - Useful audit tools.

should be considering more or less every staff member; you should not only talk to technical staff but also “normal” system users, managers and even cleaning staff. Anyone who has access to the site and as a result the computer systems should be included.

You need to determine usage patterns, and whether users have seen and read the security policy. Find out what they can and can't do, in their own words. Are they able to obtain root or system admin privileges? Find out what the systems are used for, and which are the critical systems. Finally you need to determine how the users view the security audit.

You must review all the documentation that exists already for the systems in place, paying particular

attention to details that have a security bias. You need to review your hardware and software inventory, the network topology, key personnel and contact details for emergencies. You need to look at documentation for emergency procedures and reporting incidents.

Technical Investigations

Your technical investigations should include performing scans with various static audit tools such as ISS, CyberCop or SATAN. These tools gather a vast amount of information based on what the tools have pre-programmed into them; they automate the processes of gathering information and are extremely useful, as they can be set off running and usually require

little user intervention, thus saving you a large amount of time in the process. These tools should be run in a reconnaissance mode, thus not performing invasive or DoS-style tests.

You need to review the system logs for all systems being audited; look for usage patterns, sites which disallow or restrict user access, and possible suspicious use. It is important to check systems against known vulnerability advisories from groups such as CERT, bugtraq, NTBugtraq and other alternative groups such as L0pht (see box below). Groups like L0pht are the so-called “white hat” hacker groups; these people spend an awfully large amount of time investigating common systems to look for vulnerabilities and publish this information on the Internet.

You should also spend time looking at the startup processes of the systems being audited. You need to look for processes that aren't supposed to be there, and compare the startup with the applications that are supposed to be installed on the machine or have been previously documented. You need to examine the static items of the systems to check for alteration and to determine if they include unnecessary or dangerous commands.

It is important to search the systems for applications and programs that run in a privileged state - anything that runs as root. You need to examine the environment, execution and configuration files for these applications.

Check for network services that are surplus to requirements, such as Web and Usenet servers. Also check for replacement programs such as TCP wrappers and wu-ftpd. Check for programs that are disguised as legitimate services, such as Back Orifice, NetBus and even the SETI@Home client. Look for services that are not supposed to be running - for example, a user may have installed the Windows DUN server on their machine with a modem connected, which would pose a serious security risk as this is not a sanctioned network service.

You should examine the trust relationships between the components of the network, such as your Windows NT domain trust relationships and replication of your servers. There are

Resources

It is important when conducting a security audit that you have as much information as possible in order to better assess security issues. Remember that there are both “Black Hat” and “White Hat” Web sites that contain security information, and they are both equally useful. Some of the more useful starting points are detailed below:

packetstorm.security.com

PacketStorm Security is a very good source of the latest security issues.

www.rootshell.com

Rootshell is another source of security issue information. This site hasn't been updated in a while - however, the information provided is useful.

www.securityfocus.com

Bugtraq is a mailing list for the discussion and announcement of computer security vulnerabilities. Details of how to subscribe and archive for the mailing list can be found at the above Web site.

www.ntbugtraq.com

NTBugtraq is the Windows platform version of the Bugtraq mailing list.

www.cs.purdue.edu/coast/coast.html

COAST (Computer Operations, Audit and Security Technology) is a research project into computer security at the Computer Sciences Department at Purdue University. COAST also boasts a large catalog of security and audit-related applications in their ftp archive.

www.ciac.org/ciac/

CIAC (Computer Incident Advisory Capability) provides tools and advisory information.

www.cert.org

CERT (Computer Emergency Response Team) provides information regarding many security issues, including advisory information.

www.l0pht.com

L0pht is a “Black Hat” group that performs testing of commonly used tools for security issues. L0pht also produces a number of useful tools for testing system security.

Security Audit

various services that have some form of trust relationship between components. They include NIS, NFS, SQL Server, Oracle, DNS, Windows NT domains, WINS and directory services such as LDAP.

In-House Code

Any home-grown applications should be subjected to a full code review. This will often require the auditor to be assisted by the original developer or another developer if the auditor does not have the skills required for the language the application was developed in. The review should attempt to locate any possible developer errors that could result in a security issue developing.

The kind of errors that could occur can include buffer overflows or underflows, backdoors and poor coding. Also look for signs that the program attempts to elevate during execution the security context, such as changing from running as a normal user to running with a system account.

If the program doesn't have documentation or comments within the source code then this is a bad sign. It will also hamper your review and should be noted for the final report. Some applications on some systems may become naturally large; however, sometimes, on some operating systems, an application that is uncommonly large for its type can be a bad sign.

Dynamic Tools

On Unix there are a number of tools such as ps, netstat, lsof and top whose output is important in determining the dynamic status of a system. On Windows platforms you should use the Task Manager, NETSTAT and Perfmon on Windows NT systems along with third-party tools such as filemon and regmon from System Internals (www.sysinternals.com). On Windows 9x systems you should use a Process Viewer (one is available as part of the Microsoft Visual C++ and the Win32 SDK, and is called PVIEW.EXE) and NETSTAT along with the filemon and regmon tools.

Each of these tools provide a dynamic view of the various states of the machine. Netstat is available for both

“Interview staff to locate key hosts. Look for critical functionality or sensitive information, and also understand how these hosts fit into the network.”

Unix and Windows systems, provides a dynamic view of the currently open or active network connections on the machine, and is useful for locating network services that are running the machine. Tools such as filemon and lsof display the currently open files, while regmon shows which registry entries are open on Windows platforms. The various process viewers will show which applications are running on the machines.

Active Testing

The final part of the technical investigation stage is the active testing of the systems. Tools such as ISS, NESSUS and CyberCop all offer a series of tests that have the potential to cause “Denial of Service” (DoS) attacks. The idea is to determine exactly how good those defences you have in place really are.

If you manage to run through all these tests without causing any machine to fail it's a good sign. You should also try the various “exploits” that are available to determine their effect. Such tests may adversely affect the network and consequently should be run out of normal working hours. Before performing these tests you should decide if they are really necessary, as some of the tests can potentially cause actual damage. If you do choose to perform the tests then make sure that the systems are fully backed up and that the backups are usable.

Network Auditing

There are some differences between host and network auditing. When conducting a network audit you'll get mountains of audit information. You'll need to switch from a tactical to a strategic view when auditing. As networks tend to be understood less than

hosts, information and data may be incomplete.

The larger the network is, the more difficult it can be to get an accurate picture - so more time should be allowed for the audit. In view of the amount of information, it is important that the auditor understands how the network is used. It may be necessary to reduce the size of the audit. As a result, prioritise, choose key areas and hosts and perform random spot checks.

Interview staff to locate key hosts. Look for critical functionality or sensitive information, and also understand how these hosts fit into the network. You should gather extra host audit data for key hosts.

Look at network traffic: examine the flow, what, where and when. Look at the type of traffic - be it IPX, TCP/IP or NetBEUI - and note whether the traffic is encrypted. Look at the important hardware and software, such as switches, routers and home-grown or special software.

All in all, networks require more time to audit, so do more preparation. 99% of hosts should play no role, and you may never get the true picture. External connections can be hard to map, and network and host administration can be very different from site to site.

The Data

What happens to your collected data? All data collected during an audit, whether written or in electronic form, needs to be preserved for future reference. This data shouldn't be kept online - it should be stored in a secure location safe from unauthorised access and natural disasters.

Any electronic data should be stored in an encrypted form. Only the

“Any home-grown applications should be subjected to a full code review. The review should attempt to locate any possible developer errors that could result in a security issue developing.”

people who “need to know” should have access to the information. The information held on the test machine used for the audit should be archived to CD. A useful tool to use would be something like Norton Ghost, which creates a image of the machine which can be stored in a file and written to a CD-R.

At the end of the security audit you will have a large amount of information that needs to be presented. This should be presented in a report, which explains your findings clearly to your intended audience. Your audience may comprise board-level directors, (other) MIS/IT managers and your IT staff.

Report Structure

The level of technical detail should increase as the report goes on. Most high-level staff such as directors don't need to know the technical details, so having everything they need to know in the first quarter of the report is important, and it is essential to present this information in clear, non-technical language.

Commercial Tools

CyberCop Security Scanner
Network Associates Inc
www.nai.com

Internet Scanner
System Scanner
Internet Security Systems Inc
www.iss.net

Tripwire
Tripwire Security Systems Inc
www.tripwiresecurity.com

The report should have a logical structure, and should include an executive summary and prioritised recommendations, the scope of the audit, more detailed information, followed by final conclusions and detailed recommendations.

The executive summary should be no more than one or two pages, and should state the reasons for doing the audit and a brief overview of the systems audited. It should also include details of changes in security since the last audit if any, and should briefly detail the compliance status of the organisation to published policies.

The main report body should be complete and educate the reader. Explain and defend all the recommendations and claims with the evidence gathered during the audit. If there have been previous audits, then compare/contrast this audit with the previous audit. You need to break any problems into smaller pieces, providing details of what was looked at and why it was reviewed. If in previous audits problems were found, you should detail whether the problems were fixed and whether the policy was changed to reflect the problems. If previous problems were not fixed, why not? Were any new problems found, and what were they?

When breaking problems into smaller pieces, look for key elements such as host-level security and security architecture. Next discuss the scope of the section, the importance of this section to the audited systems, what tools and methods were used, and what was discovered as a result.

The final conclusions and detailed recommendations section unifies the executive summary and body into a

coherent message and outcome of the audit process. You should prioritise and summarise all recommendations. Grade or evaluate the total system level of security. Also detail the state of the collected audit data, where it is stored, how it is kept secure, how it can be recovered, who should be allowed access and how to gain access.

The appendices should include details of the tools used during the audit, and any details of the systems or networks examined that couldn't fit into the main report body. Include significant output from audit tools that couldn't fit into the report body - eg, cracked passwords, machine configuration data etc. Lists of security patches and OS updates that are required for the systems audited should be listed, with details of how to obtain them. A bibliography of suggested reading of books, papers, and Web sites should also be included.

Conclusion

Once the report has been written and presented, all responsible personnel should meet to discuss what action items should arise from the results of the audit. It is vital that due dates are attached to each action item in order to ensure that necessary changes are made swiftly, and before the company falls prey to one of the security problems identified.

PCNA

Copyright ITP, 2000

The Author

Justin Kapp (justin.kapp@itp-journals.com) is a consultant for Reaper Technologies, an IT security consultancy. He specialises in cryptography and Windows platform security, and is the original author of the RSAEuro Cryptographic Library.

Recent Reviews from [Tech Support Alert](#)

[Reviews of the Best Windows Backup Software](#)

In this detailed comparative review, we checked out eighteen backup software utilities designed for home or SOHO use. Many of the products reviewed were disappointing. However 6 products passed our tests with flying colors and 2 of these were so impressive, they were awarded our "Editor's Choice."

[Suppliers of Cheap Inkjet Printer Cartridges Reviewed and Rated](#)

With hundreds of companies all claiming to have the "*cheapest and best inkjet printer cartridges*," our editors decided to put their claims to the test. Not unexpectedly, many suppliers flunked but we did manage to come up with a number of web sites that sell good quality inkjet printer cartridges at heavily discounted prices.

[The Best Anti Trojan Software](#)

Our editors took a close look at the 6 leading anti-trojan/trojan remover software utilities. Unfortunately, they found only 2 products that were effective in their ability to detect and remove dangerous modern polymorphic and process injecting trojans.

[The 46 Best Ever Freeware Utilities](#)

This is our Editor, Ian "Gizmo" Richards, personal selection of the best freeware utilities. He's hunted down some real gems, many of which perform better than expensive commercial products.