Penetration test: Background, Methods and Tools

SIMULATED INTRUSION

From the point of view of a hacker, your company network is often not half as safe as you might assume. However, security holes need to be found before they can be plugged. Viola Braeuer explains

The author

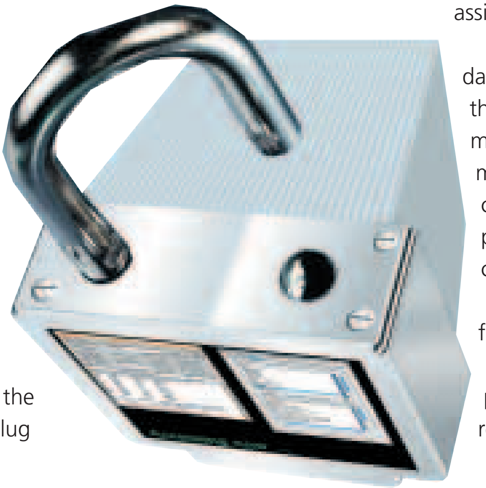
Viola Braeuer is a Bachelor of Information Technology and operates as an independent security advisor. She has been working with Linux since the start of her studies and with different aspects of IT security for the last four years.

It's a well-known fact that the Internet has not been spared the attentions of business spies and curious hackers alike. We might like to think they won't trouble us, or that our firewall will provide all the protection that we need, but the truth of the matter is often far different. What's really needed is prevention rather than damage control after the event.

Vulnerability assessment

In the world at large, people generally make sure their front doors are locked. A penetration test does pretty much the same thing across a system: it checks a computer network's possible weak spots looking for any vulnerabilities. The analysis takes the point of view of an aggressor looking for weak areas that could be exploited. What can someone who wants to enter your computer see? What information about operating systems, applications and data can they find out? Which targets will they pursue and which strategies will they use? The purpose of the penetration test is to clarify the answers to all these questions, pursuing the motto: "know your enemy".

A system's access to the Internet is the largest potential point of attack into company's network, in particular the network services (known or unknown) that are offered externally. However, the enemy could also be within your own camp: the majority of attacks on IT systems stem from frustrated employees. Another of the roles of the penetration test is therefore to identify who has Intranet access to what data.



On the whole, this is a weak point analysis of the actual state of the company network – and it quite relentlessly uncovers the gaps. The next step is to plug these holes by activating current patches and by changing the standard and trivial passwords. An internal investigation can also serve to investigate a network topology that has grown over time, i.e. which systems are actually on the domestic LAN and what runs on it?

Procedure

Despite all caution, a professional intrusion test can impair or even paralyse the examined systems. Both the client and the contractor should therefore find out and sum up the risks. Beside the client's signed declaration of consent, the safety specialist needs only the IP address area that is to be analysed.

The penetration test then consists of several steps:

- Passive procurement of information: foot printing
- Active procurement of information: scanning
- Entering the system, "gain root": enumeration

First step: foot printing

Before the tester makes contact with the computers to be examined, he or she should collect as much information about the client as possible. A good source for this are the "Whois" databases; these supply the domain (of the appropriate IP address), the email and postal addresses, the provider, technical partners and their telephone numbers, as well as the assigned IP address space.

The data so found may be out of date already. Even if it was correct at the time of log-on, the IP addresses may well have changed in the meantime. The date of the last change helps to measure the probability that the information is correct.

The client's Web site gives the first impression of the client's safety philosophy: does it give across a professional impression or does it resemble a playground for the latest in animation? Are the pages even readable with safety-conscious browser settings?

Every now and then, a Web site can be a veritable treasure chest of data. A search system for all employees of a company with their direct-dial numbers and email addresses may appear a good idea at the time, but at the same time it leaves the door to the social club wide open.

Second step: scanning

Following this rather passive step comes the active scanning phase. Its purpose is likewise the procurement of information, but in contrast to foot printing, the target system is contacted directly. The different methods used here have varying levels of conspicuousness – some can even completely hide themselves in the normal communication.

Other, less sophisticated procedures will quickly set off the alarm bells in the target network. Not all machines will tolerate a port scan, even if they look like they are the latest and greatest. Some older IBM machines even react to this by crashing. Apart from this, many system administrators may not like being put under the microscope in this obtrusive manner.

In scanning, the tester's attention focuses on the operating system that the target computer uses, as well as the offered services (open TCP and UDP ports) and the patch level of the programs. The tester will also try to look behind the firewall: some of the network topology is often visible, and in many cases there isn't even any firewall.

Through security holes in the offered services, an intruder can, despite the firewall, get to the root rights. These services therefore represent one of the greatest risks, and their role is accordingly important in the vulnerability assessment.

The test is usually over after the scanning phase. The tester gathers the identified weaknesses and the usable information and analyses this. On top of this, the tester will suggest possible measures to eliminate the gaps.

Third step: enumeration

Not all jobs end with the scanning. The tester will often try to actually attain root rights on the target system. At this is point, he or she differs from a genuine intruder: the tester will not install any rootkits and won't read or modify any internal data. A genuine intruder would cover his tracks and in many cases use the computer as a launching pad for further attacks.

Weak passwords are frequently the path to root; especially with databases. Not every administrator goes to the trouble of modifying the standard password. The second largest path uses server services, which often contain security gaps.

The cheapest method, in view of time and necessary knowledge, is the "Script Kiddie method": completed exploits, i.e. programs that use a certain weak point, save a lot of work for the intruder and the tester. A vulnerable computer needs to be found (by scanning), whereupon the exploit is released. More sophisticated attacks are accordingly possible with more know-how, time and money.

Tools

Many of the steps in a vulnerability assessment can be easily automated – above all, port scanners and full-blown security scanners are frequently used for this purpose. Some products even give suggestions as to how the ascertained weak spots can be plugged.

The port scanner of choice is often Fyodor's Nmap. Available free of charge and well documented, it offers a broad palette of options and is an almost ideal starting point into the field. The Security

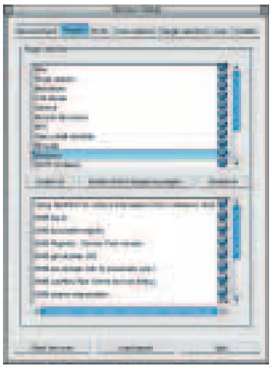


Figure 1: Nessus uses plug-ins for the different scans. Individual tests can therefore be re-tooled at any time

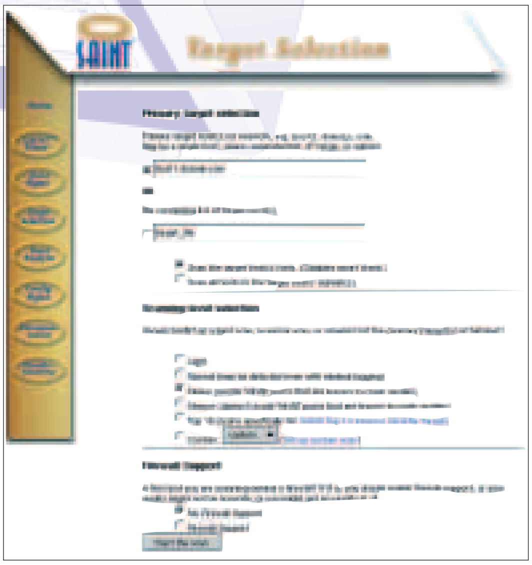


Figure 2: As a successor of Satan, Saint is also locally installed and operated through a browser. The level of detail and ruthlessness Saint uses to examine its targets can be adjusted

Security scanners

Free tools

Nmap from Fyodor: *http://www.insecure.org/nmap*
Nemesis: *http://www.packetfactory.net/Projects/Nemesis*
Satan (Security Administration Tool for Analysing Networks): *http://www.fish.com/satan*
Sara (Security Auditor's Research Assistant): *http://www-arc.com/sara*
Saint (Security Administrators Integrated Network Tool): *http://www.wwdsi.com/saint*
Whisker: *http://www.wiretrip.net/rfp/p/doc.asp/i2/d21.htm*
Nessus: *http://www.nessus.org*

Commercial scanners

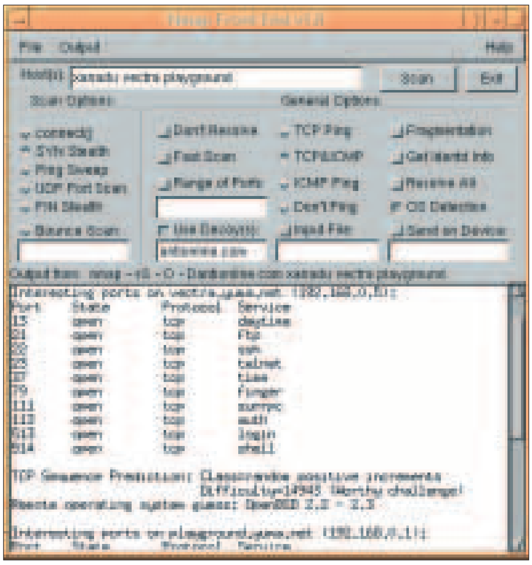
ISS Internet Scanner: *http://www.iss.net/eval/specs3.html*
QualysGuard: *http://www.qualys.com/services*
Cisco Secure Scanner (was NetSonar): *http://www.cisco.com/warp/public/cc/pd/sqsw/nesn*
Symantec NetRecon: *http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46*

scanners boxout lists even more tools, which are suitable for penetration tests. It should be emphasised here that the free security scanner Nessus is just as powerful as the commercially available tools. With two or three free tools on your laptop, a good toolbox of UNIX commands under your arm and the necessary expertise in your head, you are already quite well equipped.

As well as the free tools, there is also a handful of commercial security scanners. The advantage of these is usually in the support, maintenance, updates, training and warranty obligations. They are also frequently faster and easier to use. Their most serious disadvantage (apart from the price) is that the source text is not made public. You can thus never be certain what the program is exactly doing. This is particularly irksome with a penetration test, as you want to be able to produce a real picture of the planned procedure for your client.

ISS Internet scanner

The ISS Internet scanner manages to mark potentially dangerous functions with a small bomb. The tool, which comes from the Internet Security Systems (ISS) company, can be set to five different function levels. Levels one and two determine the operating system of the scanned computers. Level three tests the system's sensitivity (or robustness) against simple attacks. Level four and five simulate automatic intrusion tools and the procedure of a qualified attack.



```
Interesting ports on vectra.yuma.net (192.168.0.5):
Port    State      Protocol   Service
13      open       tcp        daytime
21      open       tcp        ftp
22      open       tcp        ssh
23      open       tcp        telnet
37      open       tcp        time
79      open       tcp        finger
111     open       tcp        sunrpc
113     open       tcp        auth
513     open       tcp        login
514     open       tcp        shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14985 (Worthy challenge!)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net (192.168.0.1):
Port    State      Protocol   Service
```

Figure 3: The powerful port scanner Nmap has several graphical front-ends, for example NmapFE (now included in Nmap)

The free security scanner Nessus is just as powerful as the commercially available tools

Security scanners made illegal?

That penetration testing cuts both ways is well known: programs that check computers for their security aren't solely used to protect one's own system. They can of course also be used as tool for breaking and entering into other computers. Administrators, advisors and crackers essentially use the same tools and know the same weak spots – the only difference is the intention behind the knowledge. It is substantially simpler to make use of a hole than to configure and administer a usable and nevertheless safe system.

The deadlock over these tools is endangered by a new law in the making – the intention of which is to provide more security in a quite different area. The European draft, almost amounts to a professional ban on security consultants who execute vulnerability assessments. It also outlaws the manufacturers of security scanners and decrees that administrators be blind-folded.

This problem is not new but with this proposed law, the limits are being pushed. One of the main reasons for this amendment was to find a way of eliminating the ways and means of not paying for Pay TV and similar services. This then additionally forbids the possession, distribution and development of tools, which enable this.

Now laws need to be wide enough so that they cannot be circumvented. In the widening of the law, the legislators have in this case shot way beyond the actual target, punishing activities for which the law is not at all meant. This mistake will then need to be corrected: a lengthy process examining the literature and the high court jurisdiction and determining how to alter the necessary wording and terms.

A question of access

The main term of conjecture in this case is "access control service", a description of what a set-top box does. This is to decode coded information only when the user has proved his authorisation. The law is to apply to television services, media services and broadcast presentations, which are broadcasted against payment. In the definition of this term, the train has already left the station. It is clear that individual information units are meant in this law, such as video streams or MP3 files, delivered for individual payment. The wording however encompasses much more, i.e. each and every Internet access. This also costs money and is "access controlled" by the user-identification. An "avoidance mechanism" is by definition any device or technical procedure that enables unauthorised use.

The wording thereby covers any unauthorised access onto server services. This culmination creates the following after effect: not only is the actual act of unlawful entry to be punished, but also preparatory

The scanner compares the version and patch level status of operating systems and applications with its database and thereby reports missing patches. The regular update of this database is therefore essential.

The scanner unfortunately only runs under Windows NT – as do many commercial tools. It contains an editor, in which individual test runs from different categories can be compiled. Not all tests are always really necessary, the selection however remains clear due to the grouping. The ISS Internet scanner is a quite complex and very useful tool.

QualysGuard

QualysGuard can be used from anywhere as a Web service (over HTTPS with password protection). The user doesn't have to worry about updates, as the scanner runs directly on Qualys' own servers. This tool also offers both port scans as well as a database with application-specific weak spots.

The relatively scant selection of options shortens the acquaintance period drastically, but it also makes it more difficult to estimate the function range. Alone, the report permits vague conclusions about the scan methods used.

QualysGuard supplies a quite useful first result with the minimum of time and energy. With its simple, easy operation it can even be used before your first cup of coffee in the morning.

Report analyses

A lot more is asked of the user in the analysis of automatically produced reports. Depending on the settings, commercial tools can supply reports big enough to fill half a filing cabinet – which of course no one wants to read. What is needed is a careful selection of the options and a gradual procedure, in which the configuration is refined step by step.

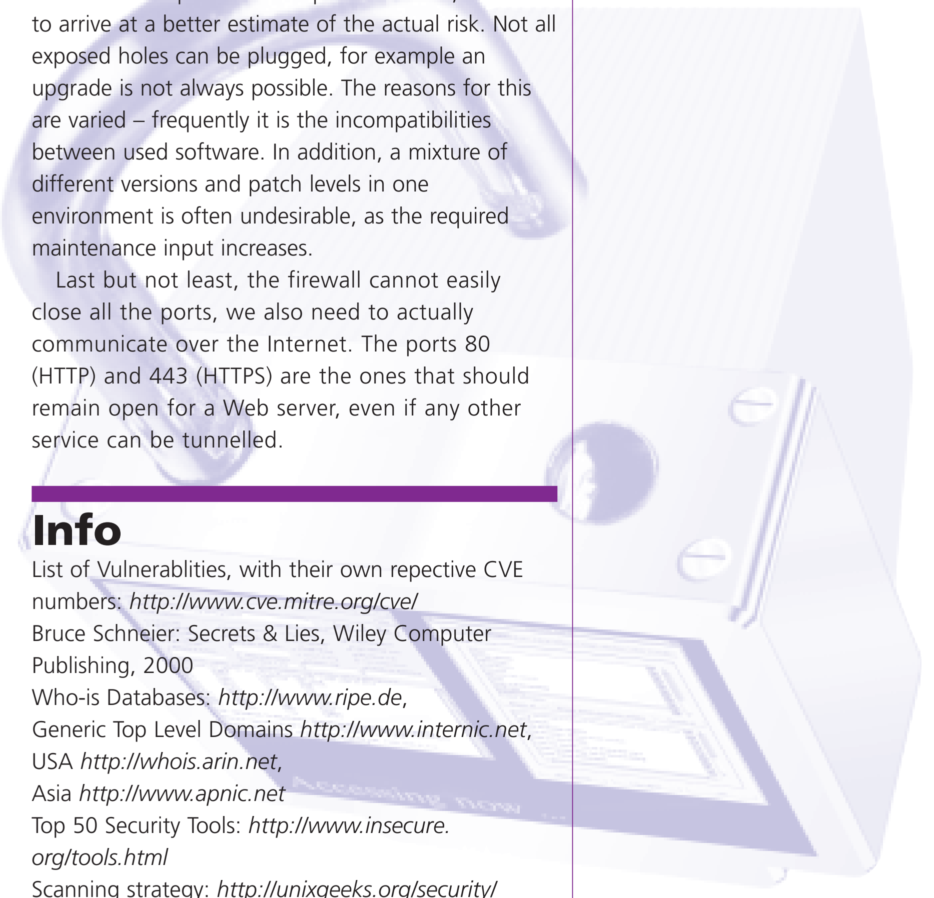
No less demanding is the estimate of the threat potential from the exposed weak spots. The generated bar and pie charts are often referred to as "management reports". They have however the main function of filling many pages with their key of: "If there's a lot of red on the page, it looks really bad." The estimate of the real situation becomes more accurate when one regards several weak points together as a combination and investigates their topicality and importance on the appropriate Web pages. The CVE list records the well-known software gaps, assigning each one its own, unique number.

Commercial tools can supply big reports big enough to fill half a filing cabinet

Result

A purpose of a vulnerability assessment is to point out the weak spots of a computer network, in order to arrive at a better estimate of the actual risk. Not all exposed holes can be plugged, for example an upgrade is not always possible. The reasons for this are varied – frequently it is the incompatibilities between used software. In addition, a mixture of different versions and patch levels in one environment is often undesirable, as the required maintenance input increases.

Last but not least, the firewall cannot easily close all the ports, we also need to actually communicate over the Internet. The ports 80 (HTTP) and 443 (HTTPS) are the ones that should remain open for a Web server, even if any other service can be tunnelled.



Info

List of Vulnerablities, with their own repective CVE numbers: *http://www.cve.mitre.org/cve/*

Bruce Schneier: Secrets & Lies, Wiley Computer Publishing, 2000

Who-is Databases: *http://www.ripe.de*,

Generic Top Level Domains *http://www.internic.net*,

USA *http://whois.arin.net*,

Asia *http://www.apnic.net*

Top 50 Security Tools: *http://www.insecure.org/tools.html*

Scanning strategy: *http://unixgeeks.org/security/newbie/pen/ssarh.html*

and support actions. The draft justifies this with the ease of distribution of hacker tools and a low threshold of inhibition. The model therefore also forbids the possession, manufacture, maintenance or exchange of such avoidance mechanisms or processes.

It goes on to say: "The law is formulated to be technically neutral and therefore applies independently of the concrete definition of the protection of the access control service or the avoidance mechanism."

An infringement against this law carries a maximum penalty of one year's imprisonment as well as a fine of up to 50,000 euros. This is therefore what faces someone in the possession of a port scanner – all because of this "technically neutral" formulation. It begs the question whether it is only the European Union guideline that has undergone such a particularly incompetent conversion. Perhaps the threat against corporate and financial order through the Internet will be fought preventatively by the sword of the justice system – present tendencies look this way. This will hardly be of concern to the real hackers out there. By breaking into foreign computer networks, they are infringing against the law anyway – it then doesn't really matter which law does it?

The draft was referred for further amendment by three specialised parliamentary committees in late 2001.