The Catman's Lair

Hacker Resource Files

http://www.pryde-lands.com/catman/

WARNING - Contents of this file are for educational purposes only. It is strongly suggested that you do not use this knowledge for illegal purposes!

Techniques Adopted By 'System Crackers' When Attempting To Break Into Corporate or Sensitive Private Networks.

By the consultants of the Network Security Solutions Ltd.
Front-line Information Security Team (FIST), December 1998.

fist@ns2.co.uk http://www.ns2.co.uk

0 Table Of Contents

1.0 Introduction

This white paper was written to help give systems administrators and network operations staff an insight into the tactics and methodologies adopted by typical system crackers when targeting large networks.

This document is not a guide about how to secure your networks, although it should help you identify security risks in your networked environment and maybe help point out any accidents that are waiting to happen.

We hope you enjoy reading this paper, and hopefully learn a little about how crackers operate in the meantime!

The Network Security Solutions Ltd. FIST staff (fist@ns2.co.uk)

1.1 Just who is vulnerable anyway?

Networked computer environments are used everyday by corporations and various organisations. Networks of computers allow users to share vast amounts of data very efficiently.

Usually corporate networks are not designed and implemented with security in mind, merely functionality and efficiency, although this is good from a business standpoint in the short-term, security problems usually arise later, which can cost millions to solve in larger environments.

Most corporate and sensitive private networks work on a client-server principle, where employees use workstations to connect to servers in order to share information. In this paper we will concentrate on server security, as most crackers will always target servers first, the server is much like a 'hub' where all the information is stored. If a cracker can gain unauthorised access to such a server, the rest of his work is easy.

Vulnerable parties to large-scale network probes usually include :

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various goverment agencies
- Multinational corporations

Although many of these attacks take place internally (by users who have authorised access to parts of the corporate or sensitive networks already), we will be concentrating on the techniques used when breaking into such networks entirely from the outside.

Financial institutions and banks are probed and attacked in attempts to commit fraud. Many banks have been targeted in this way, risking vast monetary funds. Banks make it policy not to admit to being victims of such external attacks because they will certainly lose customers and

trust if attacks are publically known.

Internet service providers are a common target by crackers, as ISP servers are easily accessible from the internet, and ISP's have access to large fibre optic connections which can be used by crackers to move large amounts of data across the internet. The larger ISP's also have customer databases, which usually contain confidential user information such as credit card numbers, names and addresses.

Pharmaceutical companies are victims of mainly industrial espionage attempts, where a team of crackers will be paid large amounts in exchange for stolen pharmaceutical data, such drug companies often spend millions on research and development, and a lot can be lost as a result of such an attack.

Over the last 6 years, Government and defence agencies in the United States have been victim to literally millions of attacks originating from the internet. Due to the low information security budgets and the weak security policies of such agencies, information security has become an uphill battle, as government and military servers are constantly being probed and attacked by crackers.

Defence contractors, although security conscious, are targets to crackers seeking classified or sensitive military data. Such data can then be 'sold on' by crackers to foreign groups. Although only a handful of these cases have been publically known, such activities can occur at an alarming rate.

Multinational corporations are prime examples of victims of industrial espionage attempts. Multinational corporations have offices based all around the world, and large corporate networks are installed in order for employees to be able to share information efficiently. NSS staff have performed penetration tests for multinational corporations, and our findings in most cases have shown that many can be compromised.

Like pharmaceutical companies, multinational corporations operating in electronics, software or computer-related industries, spend millions on research and development of new technologies. It is very tempting for a competitor of such a corporation, to employ a team of 'system crackers' to steal data from a target corporation. Such data can then be used to quickly and easily improve the competitors knowledge of key technologies, and result in financial losses of the target corporation.

Another form of attack adopted by competitors of corporations, is to 'take down' a corporate network for a certain amount of time, this results in loss of earnings for the target corporation. In most cases it is extremely difficult to locate the source of such an attack. Depending on the internal network segmentation in place, this kind of attack can be hugely effective and result in massive financial losses.

Such 'foul play' is commonplace in today's networked society, and should be taken very seriously.

1.2 Profile of a typical 'system cracker'

Studies have shown that typical a 'system cracker' is usually male, aged between 16 and 25. Such crackers usually become interested in breaking into machines and networks in order to improve their cracking skills, or to use network resources for their own purposes. Most crackers are quite persistent in their attacks, this is due to the amount of spare time an average cracker has.

A high percentage of crackers are opportunists, and run scanners to check massive numbers of hosts for remote system vulnerabilities. Upon identifying hosts or networks that are vulnerable to remote attacks, the cracker will usually gain root access to the host, then install a backdoor and patch the host from common remote vulnerabilities, this prevents other crackers from being able to use the same popular techniques to gain access to the host.

Opportunists operate on primarily two domains, the first being the internet, the second being telephone networks.

To scan internet hosts for common remote vulnerabilities, the cracker will usually launch a scanning operation from a host that he has access to with a fast connection to the internet, usually on a fibre-optic connection.

To scan for machines operating on telephone networks, being terminal servers, bulletin board systems, or voice mail systems. The cracker will use a wardialling program, this will automatically scan large amounts of telephone numbers for 'carriers', thus identifying such systems.

A very small percentage of crackers actually define targets and attempt to attack them, such crackers are far more skilled, and adopt 'cutting-edge' techniques to compromise networks. It is known for these types of crackers to attack corporate networks that are firewalled from the internet by exploiting non-published vulnerabilities and 'features' in firewalls.

The networks and hosts targeted by these crackers usually have sensitive data contained within them, such as research and development notes, or other data that will prove useful to the cracker.

Such crackers are also known to have access to exploits and tools used by security consultants and large security companies, and then use them to scan defined targets for all known remote vulnerabilities. Crackers that are attacking specific hosts are also usually very patient, and have been known to spend many months gathering data before attempting to gain access to a host or network.

2.1 Networking methodologies adopted by many companies

A typical corporation will have an internet presence for the following purposes :

The hosting of corporate webservers
E-mail and other global communications via. the internet
To give employees internet access

Of the corporations NSS has performed network penetration tests from the internet for, a networked environment is adopted where the corporate network and the internet are seperated by firewalls and application proxies.

In such environments, the corporate webservers and mailservers are usually kept on the 'outside' of the corporate network, and then information is passed via. trusted channels onto the corporate network.

In the case of trust present between external mailservers and hosts on the corporate network, a well-thought filtering policy has to be put into effect, as usually the external mailservers should only be able to connect to port 25 of a single 'secure' mailserver on the corporate network, as this will massively minimise the probability of unauthorised access, even if the external mailserver is compromised.

One of the corporate networks NSS has performed penetration test on also had a handful of 'dual-homed' hosts, these hosts had network interfaces active on both the internet and the corporate network. From a security standpoint, such hosts that operate on multiple networks can pose a massive threat to network security, as upon compromising a host, it then acts as a simple 'bridge' between networks.

2.2 Understanding vulnerabilities in such networked systems

On the internet, a corporation may have 5 external webservers, 2 external mailservers, and a firewall or filtering system implemented.

Webservers are usually not attacked by crackers wanting to gain access to the corporate network, unless the firewall is misconfigured in some way that will allow the cracker access to the corporate network upon compromising the webserver. Although it is always good practise to secure your webservers and run TCP wrappers to allow only trusted parties to connect to the telnet and ftp ports.

Mailservers are commonly targeted by crackers wanting to gain access to the corporate network, as a mailserver must have access to mailservers on the corporate network in order to distribute and exchange mail between the internet and the corporate network. Again, depending on the filtering in place, this tactic may or may not be effective on the cracker's part.

Filtering routers are also commonly targeted by crackers with agressive-SNMP scanners and community string brute-force programs, if such an attack is effective, the router can easily be turned into a bridge, thus allowing unauthorised access to the corporate network.

In this kind of situation the cracker will evaluate exactly which external

hosts he has access to, and then attempt to identify any kinds of trust between the corporate network and the external hosts. Therefore if you install TCP wrappers on all your external hosts, which define that only trusted parties can connect to the critical ports of your hosts, which are usually :

```
ftp  (21),   ssh  (22),   telnet (23),   smtp   (25),   named (53),
pop3 (110),  imap (143),  rsh    (514),  rlogin (513),  lpd   (515).
```

SMTP, named and portmapper should be filtered accordingly depending on the host's role is on the network.

Such filtering has been proven to massively reduce the risk of an attack on the corporate network.

In the cases of networks with no clear 'corporate to internet' network security policy, multiple-homed hosts and misconfigured routers will exist. A lack of internal network segmentation will also usually exist, this makes it a lot easier for an cracker based on the internet to gain unauthorised access to the corporate network.

Corporate network mapping can easily occur if external DNS servers are misconfigured, as NSS has performed penetration tests where we have been able to map the corporate network via. such a misconfigured DNS server, because of this, it is very important that DNS doesn't exist between hosts on the corporate network and external hosts, it is far safer to simply use IP addresses to connect to external machines from the corporate network and vice-versa.

Insecure hosts with network interfaces active on multiple networks can be abused to gain access to the corporate network very easily.
The insecure host doesn't even have to be compromised. It is very easy to abuse a finger daemon on such a host that allows forwarding.. as users, hosts and other network information can be collected to identify easily exploitable hosts on the corporate network, the operating system of a host can even be determined in many cases by issuing a finger request for root@host, bin@host and daemon@host.

Some crackers are now starting to adopt techniques regarding the 'wardialling' of corporate locations, such as buildings and network operation centres.

If a cracker was to find and then compromise a corporate terminal server, he would usually have a degree of access to the corporate network, thus totally bypassing any firewalls or filters that seperate the corporate network from the internet. It is therefore very important to identify and ensure the security of your terminal servers, logging of connections to such servers is also strongly advised.

When trying to understand vulnerabilities in networked systems, a key point to remember, is trust between hosts on your network. Either through the use of TCP wrappers, hosts.equiv files, .rhosts or .shosts files, many larger networks are commonly attacked by exploiting the

trust between hosts.

For example, if an attacker uses a CGI exploit to view your hosts.allow file, he may find that you all connections to your ftp and telnet ports from *.trusted.com. Of course, the attacker can then gain access to any host at trusted.com, and gain access to your hosts easily.

For these reasons, it is always a good idea to ensure that trusted hosts are equally secure from remote attack.

One other attack that should be mentioned, is the installation of trojans and backdoors on corporate hosts (such as Windows 95/98 machines), if the employees have internet access through using an application proxy and a firewall, then they will sometimes visit 'warez' sites to download pirated software.

Such 'warez' sites usually have screesaver software, and other utilities on offer, which in some cases contain trojan horse programs, such as the Cult of the Dead Cow's 'Back Orifice' trojan. Upon the installation of the screensaver, the trojan infests itself within the machine's registry and is run every time the machine boots.

In the case of the BO trojan, plugins can be applied to the trojan to make the machine perform certain operations automatically, such as connect to IRC servers and join channels, and the like. This can prove very dangerous, as a trojaned machine on your corporate network could easily be controlled by someone on the internet.

The BO trojan is infinitely more effective if the cracker already has access to the corporate network, either because he is an employee or has unauthorised access to corporate hosts. The BO trojan could be installed on every single Windows 95/98 machine in a matter of weeks if the cracker uses the correct strategy, after which he will have total remote control over the machines in question, including being able to manipulate files, reboot machines and even format drives, entirely remotely.

3.1 Techniques used to 'cloak' the attackers location

Typical crackers will usually use the following techniques to hide their true IP address :

- Bouncing through previously compromised hosts via. telnet or rsh.
- Bouncing through windows hosts via. Wingates.
- Bouncing through hosts using misconfigured proxies.

If such a cracker has a pattern of always scanning your hosts from previously compromised machines, wingates or proxies, then it is advisable to contact the administrator of the machine by telephone, and notify him of the problems in hand. Never e-mail an administrator in such a case, because the cracker can simply intercept the e-mail beforehand.

The more talented crackers who are skilled in breaking into hosts via. telephone exchanges, may use the following techniques :

- Bouncing through '800-number' private telephone exchanges before connecting to an ISP using a 'cracked', 'phished' or 'carded' account.

- Connecting to a host by telephone, that is in turn connected to the internet.

Crackers adopting the techniques of bouncing through telephone networks before connecting to the internet are extremely hard to track down, because they could be literally anywhere in the world. If a cracker was to use an '800-number' dialup, he could dial into machines globally without having to worry about the cost.

3.2 Network probing and information gathering

Before setting out to attack a corporate network from the internet, a typical cracker will perform some preliminary probes of your networks external hosts present on the internet. A cracker will attempt to gain external and internal hostnames by using the following techniques :

- Using nslookup to perform 'ls <domain or network>' requests.
- View the HTML on your webservers to identify any other hosts.
- View the documents on your FTP servers.
- Connect to your mailservers and perform 'expn <user>' requests.
- Finger users on your external hosts.

Crackers usually attempt to gather information about the layout of your network itself first as opposed to identifying specific vulnerabilities.

By looking at results from the queries listed above, it is usually easy for a cracker to build a list of hosts and start to understand the relationships that exist between them.

When performing these preliminary probes, a typical cracker will make very small mistakes and sometimes use his own IP to connect to ports of your machines to check operating system versions and other small details.

If your hosts are compromised, it is a good idea to check your FTP and HTTPD logs for the presence of any strange requests.

3.3 Identifying trusted network components

Crackers look for trusted network components to attack, a trusted network component is usually an administrators machine, or a server that is regarded as secure.

A cracker will start out by checking the NFS exports of any of your machines running nfsd or mountd, the case being that critical directories on some of your hosts (such as /usr/bin, /etc and /home for example) may be mountable by such a trusted host.

The finger daemon is often abused to identify trusted hosts and users, being users who often log into the machine from specific hosts.

The cracker will then check your machines for other forms of trust, if he can exploit a machine using a CGI vulnerability, he may gain access to a hosts /etc/hosts.allow file, for example.

After analysing the data from the above checks, the cracker will start to identify trust between hosts. The next step for the cracker is to identify any trusted hosts that are vulnerable to a remote compromise.

3.4 Identifying vulnerable network components

If a cracker can build lists of your external and internal hosts, he will use Linux programs such as ADMhack, mscan, nmap and many smaller scanners to scan for specific remote vulnerabilities.

Usuaully such scans of your external hosts will be launched from machines on fast fibre-optic connections, ADMhack requires to be run as root on a Linux machine, so a cracker will probably use a Linux machine that he has gained unauthorised access to and properly installed a 'rootkit' on. Such a 'rootkit' is used to backdoor critical system binaries to allow unauthorised and undetectable access to the host.

The systems administrators of the hosts that are used to scan external corporate hosts usually have no idea that scans are being launched from their machines, as binaries such as 'ps' and 'netstat' are trojaned to hide scanning processes.

Other programs such as mscan and nmap don't require to be run as root, and so can be launched from Linux (or other platforms in the case of nmap) hosts to effectively identify remote vulnerabilities, although these scans are slower, and cannot usually be hidden very well (as the attacker doesn't need root access to the host as with ADMhack).

Both ADMhack and mscan perform the following types of checks on remote hosts :

- A TCP portscan of a host.

- A dump of the RPC services running via. portmapper.
- A listing of exports present via. nfsd.
- A listing of shares present via. samba or netbios.
- Multiple finger requests to identify default accounts.
- CGI vulnerability scanning.
- Identification of vulnerable versions of server daemons, including Sendmail, IMAP, POP3, RPC status and RPC mountd.

Programs such as SATAN are rarely used by crackers nowadays, as they are slow.. and scan for outdated vulnerabilities.

After running ADMhack or mscan on the external hosts, the cracker will have a good idea of vulnerable or secure hosts.

If routers are present that are SNMP capable, the more advanced crackers will adopt agressive-SNMP scanning techniques to try and 'brute force' the public and private community strings of such devices.

3.5 Taking advantage of vulnerable network components

So the cracker has identified any trusted external hosts, and also identified any vulnerabilities in external hosts. If any vulnerable network components were identified, then he will attempt to compromise your hosts.

A patient cracker won't compromise your hosts during normal hours, he will usually launch an attack between 9pm in the evening and 6am the next morning, this will reduce the likelyhood of anyone knowing about the attack, and give the cracker ample time to install backdoors and sniffers on your hosts without having to worry about the presence of Systems Administrators.

Most crackers have a great deal of spare time over weekends, and attacks are usually launched then.

The cracker will compromise an external trusted host that can be used as a point from which to launch an attack on the corporate network. Depending on the filtering between the corporate network and the external corporate hosts, this technique may or may not work.

If the cracker compromises an external mailserver, which in turn has total access to a segment of the internal corporate network, then he can start work on embedding himself deeply into your network.

To compromise most networked components, crackers will use programs to remotely exploit vulnerable versions of server daemons running on external hosts, such examples include vulnerable versions of Sendmail, IMAP, POP3 and RPC services such as statd, mountd and pcnfsd.

Most remote exploits used by crackers are launched from previously compromised hosts, as in some cases they need to be compiled on the same platform as the host they are to be used to exploit.

Upon executing such a program remotely to exploit a vulnerable server daemon running on your external host, the cracker will usually gain root access to your host, which in turn can be abused to gain access to other hosts and the corporate network.

3.6 Upon gain access to vulnerable network components

After exploiting a server daemon, the cracker will start a 'clean-up' operation of doctoring your hosts logs and 'backdooring' service binaries so he can access the host undetected later.

First he will start to implement backdoors, so he can later access the host. Most backdoors that crackers use are precompiled, and techniques are adopted to change the date and the permissions of the binary that has been backdoored, in some cases, even the filesize of the new binary is the same as the original binary. Attackers conscious of FTP transfer logs may use the 'rcp' program to copy backdoored programs to hosts.

It is unlikely that such a cracker breaking into a corporate network will start to patch your hosts from vulnerabilities, he will usually only install backdoors and trojan critical system binaries such as 'ps' and 'netstat' to hide any connections he may make to and from the host.

The following critical binaries are usually backdoored on Solaris 2.x machines :

```
/usr/bin/login
/usr/sbin/ping
/usr/sbin/in.telnetd
/usr/sbin/in.rshd
/usr/sbin/in.rlogind
```

Some crackers have also been known to place an .rhosts file in the /usr/bin directory to allow remote bin access to the host via. rsh and csh in interactive mode.

The next thing that most crackers do is to check the host for any presence of logging systems that may have logged his connections to the host, he will then proceed to edit such connections out of any logs found on the host. It is advisable to log to a lineprinter if the machine is very likely to be a prime target of an attack, as this makes it extremely difficult for the cracker to edit himself from the logs.

Upon ensuring that his presence has not been logged in any way, the cracker will proceed to invade the corporate network. Most crackers won't bother exploiting vulnerabilities in other external hosts if they have access to the internal network.

4.1 Downloading sensitive information

If the cracker's goal is to download sensitive information from FTP servers or webservers on the internal corporate network, he can do so from the external host that is acting as a 'bridge' between the internet and corporate network.

However, if the cracker's goal is to download sensitive information held within internally networked hosts, he will proceed to attempt to gain access to them by abusing the trust with the external host he already has access to.

4.2 Cracking other trusted hosts and networks

Most crackers will simply repeat the steps taken in sections 3.2, 3.3, 3.4 and 3.5 to probe and gain access to hosts on the internal corporate network, depending on what the cracker is attempting to achieve, trojans and backdoors may or may not be installed on your internal hosts.

If the cracker wishes to achieve total network access to the hosts on the internal network, he will install trojans and backdoors and remove logs as in section 3.6. Crackers will also install sniffers on your hosts, these are explained in section 4.3.

If the cracker merely wishes to download data from key servers, he will take different approaches to gaining access to your hosts, such as identifying and attacking key hosts that are trusted by the target key servers.

4.3 Installing sniffers

An extremely effective way for crackers to quickly obtain large amounts of usernames and passwords for internally networked hosts is to use 'ethernet sniffer' programs. Because such 'sniffer' programs need to operate on the same ethernet as the hosts the cracker wants to gain access to, it would be ineffective to run a sniffer on the external host he is using as a bridge.

To 'sniff' data flowing across the internal network, the cracker must perform a remote root compromise of an internal host that is on the same ethernet as a number of other internal hosts. The techniques mentioned in sections 3.2, 3.3, 3.4, 3.5 and 3.6 are adopted here, as the cracker must compromise and backdoor the host successfully to ensure that the sniffer program can be installed and used effectively.

Upon compromising, installing a backdoor and installing trojaned 'ps' and 'netstat' programs, the cracker must then install the 'ethernet sniffer' program on the host. Such sniffer programs are usually installed in the /usr/bin or /dev directories under Solaris 2.x, and then modified to seem as if they were installed with all the other system binaries.

Most 'ethernet sniffers' run in the background and output to a log on the local machine, it is important to remember that the cracker will usually backdoor the 'ps' binary, so the process may not be noticeable.

Such 'ethernet sniffers' work by turning a network interface into 'promiscuous mode', the interface then listens and logs to the sniffer logfile, any useful usernames, passwords or other data that can be used by the cracker to gain access to other networked hosts.

Because 'ethernet sniffers' are installed on ethernets, literally any data travelling across that network can be sniffed, it doesn't have to be travelling to or from the host on which the sniffer is installed.

The cracker will usually return a week later and download the logfile created by the 'sniffer' program. In the case of a corporate network breach such as this, it is likely that the sniffer will be set up very well, and hardly detectable unless a good security policy is implemented.

A very good utility used by many security-conscious Administrators is Tripwire, which is available from COAST (see section 5.2). Tripwire makes an MD5 'fingerprint' of your filesystem, and will detect any modifications to your files made by malicious users or crackers.

To detect promiscuous network interfaces (a common sign of a sniffer installation), the 'cpm' tool available from CERT is very useful, see http://www.cert.org/ftp/tools/cpm/ for more information.

4.4 Taking down networks

If a cracker can compromise key servers running server applications such as databases, network operations systems or any other 'mission critical' functions, it is easy for him to take down your network for a period of time.

A crude, but not unusual technique adopted by crackers attempting to disable network functions, would be to delete all the files from the key servers by issuing an 'rm -rf / &' command on the server. Depending on the backup system implemented, the system could be for anything from hours, to months.

If a cracker was to gain access to your internal network, he could abuse vulnerabilities present in many routers such as in the Cisco, Bay and Ascend brands. In some cases the cracker could restart, or shut down routers entirely until an administrator was to reboot them.

This can cause big problems regarding network functionality,
as if the cracker was to assemble a list of vulnerable routers that
performed key networking roles (if they were used on the corporate
backbone for example), then he could easily disable the corporations
networking ability for some time.

For these reasons, it is very important that 'mission critical' routers
and servers are always patched and secure.

5.1 Suggested reading

There are many good papers available to help you maintain security of your
external and internal hosts and routers, we recommend you visit the following
websites and take a look at the following books if you wish to learn more
about securing large networks and hosts :

http://www.antionline.com/archives/documents/advanced/
http://www.rootshell.com/beta/documentation.html
http://seclab.cs.ucdavis.edu/papers.html
http://rhino9.ml.org/textware/

'Practical Unix & Internet Security'

A good introduction into Unix and Internet security if you really haven't
read much into the subject before.

Simson Garfinkel and Gene Spafford
O'Reilly & Associates, Inc.
ISBN 1-56592-148-8

US $39.95 CAN $56.95 (UK around 30 pounds)

5.2 Suggested tools and programs

There are many good free security programs available for common platforms
such as Solaris, IRIX, Linux, AIX, HP-UX and Windows NT, we recommend you
take a look at the following websites for information on such free security
tools :

ftp://coast.cs.purdue.edu/pub/tools/unix/
http://www.alw.nih.gov/Security/prog-full.html
http://rhino9.ml.org/software/

Network Security Solutions Ltd., is also currently developing a plethora of security tools for Unix and Windows based platforms, these will be available over the next few months, feel free to visit our site at http://www.ns2.co.uk , also look out for free 'lite' versions of our software!
