



Newsletter #2

Table of Contents

Editorial by Ennisp. 3

Editorial by MsMittensp. 5

What is a Trojan? Part 1 by Rip7p. 6

Unix Tutorial #2 by MsMittensp. 10

Security Auditing by Remote_Access_p.12

To Enter or Not To Enter by Andrew Matheson..p13

Default Password Paths compiled by s0nicp.15

Default Passwords compiled by s0nicp.15

Editorial

AntiOnline Newsletter #2
March/April 2002

By Ennis

The AntiOnline Newsletter is property of AntiOnline.com and all the copyright info.

Special thanks to Ennis, Rip7, Remote_Access_, Andrew and sOnic for their submissions.

Special thanks to JP for allowing us this venue.

Any errors in submissions are the fault of the authors.

Submissions are always welcomed. You can send them to MsMittens via PM (Private Message) or via email to msmittens@msmittens.com.

When sending via email include your submission as a Word document or an RTF file.

The AntiOnline Addicts Manifesto

The following is a tale of how I came to love a little site and join a community I grew to love {cue tears! }

It was a delightful Autumn afternoon and as usual I was just looking through my Favourites. Anyway I was getting tiresome of this dreary routine and needed a virtual home, somewhere I could just layabout, contribute and find a gathering of people who know their security inside out.

So I typed in the address which always provides the required results [Google](#), and proceeded to enter, *security*. As you should know in nearly every search engine one particular site always pops up first when you enter security and rightfully so, produced before me was AntiOnline. I had never taken much notice of this site, it had an awful colour scheme {sorry JP } and well that turned me off. Today however I was willing to try anything so I clicked the damn link and arrived at a site that I have since failed to disagree with. My first objective was to join the forums; I knocked in all the details, filled out my profile and headed to Discussion Forums.

I was quite honestly shocked at the sheer amount of forums and how they were maintained so well. I had a look around and read what I could. I was soon gathering the social hierarchy of the place and the list of Top 10 posters seemed daunting to a virtual newbie such as myself. I didn't post for a long time, for the next month or so I itched to get involved but my fear was soon quashed when somebody made an odd reference to the RAT we all love to hate, Sub7. My first post! I attempted to phrase it well, and to my best ability I checked in various titbits of information that came to mind.

I returned the next day to see the reaction, to my surprise people had agreed with my point of view and well I felt that maybe I should contribute more.

This I tried, looking for subjects I knew about and helping where I could, all the time learning more from the respected members. I noted one particular user Terr as truly helpful and I owe a lot of the info I have accumulated to his presence. My first unsavoury moment in the forums came with my lackadaisical

use of grammar.

The General Chit Chat forum has many flaws for a newbie, firstly it contains a vast array of topics and well when you get into the swing of things you can start posting meaninglessly. Secondly having an open opinion leaves you wide open for a well deserved flaming at times. My first flame came at the hands of a user called Negative. For those of you not familiar with Negative, this man has the ability to flame to an electrifying degree and in a spectacular manner which leaves you often in awe!

Not knowing what to do as my grammar came under fire I decided to flame him back...

This I did with an unexpected result, I gave it my all trying to gain recognition and attacking his post in any manner I could. Of course I failed to arouse a reaction and quite rightly so, it did however get me an invitation to the IRC channel that I did not fully enjoy until later.

Here I was after a while, I had been flamed, I had learned, I had tried to help and I still wasn't bored. This meant something to me, after all many a forum had quite simply bored me to the point where my eyes began turning inward so as to find inspiration!

I now had a reasonable amount of posts and found that replies came quickly at AntiOnline, sometimes too fast for me to keep up! I ventured on and soon found joy in the infamous IRC chatroom neither man nor woman should miss out on! To understand what goes in AntiOnline's IRC chat one must be prepared for odd conversations and to be saturated with constant security information. If you need help join the chatroom and look for MsMittens and you will be pleasantly surprised by the sheer knowledge that can be mustered by actively partaking in the chat.

The main change that occurred halfway through my time at AntiOnline was the introduction of AntiPoints, this idea is like no other rating system that can be found on the net. No longer would you be defined by peoples memory concerning your past posts but by little red and green dots that hover quaintly under your screen name. I was glad to see that antipoints promoted quality posting and stopped flaming to some degree { a subject I try to demote! } .

It has not all been rosy during my time at AntiOnline, two events forced me out of the scene for a short time, and both concerned flaming. Each time I came back after a short stint boring myself with other forums. I always came back to AntiOnline proving my addiction. They served a purpose, each time I returned I had a renewed hunger to pacify the forums but well the AntiOnline custom flame could not be stopped by one man and his mission but hey it was fun!

I have since reconciled with members who have badly flamed me and like most people I have my little enemies but the friends far outweigh their presence. The friendly but firm atmosphere of AO is emphasised by the real presence of its Webmaster, constantly conjuring up new and fresh ideas to improve the community JP can only be described as a hard working individual who has gained my utmost respect.

I have enjoyed my time overall, putting together the first issue of the newsletter helped me get to know a lot of people at AO on a more personal level and I hope this lets them get to know me a little better!

Take this for what you will, it is just a small piece of literature for you to pass the time but I hope it shows that us AntiOnline Addicts are addicted to something that is truly a good experience, both for learning and having a good time on the net.

I offer you the *AntiOnline Addicts Manifesto!*

Ennis.

Editorial:

Rant about Not Thinking Securely by MsMittens

While the thought of Internet-wide computing, sometimes referred to as distributed computing, has appeal, largely due to the redundancy it can create, I suspect that there may be inherent pitfalls to this system. In a recent issue of Scientific American, it was suggested that one day we will have what is referred to as “Internet-Scale Operating System”. Basically, this would be a peer-to-peer network OS. Everything you download won’t come from one location but rather from multiple locations, ensuring redundancy and reliability.

This first and foremost is the concept of trust between users. While there are many individuals that will happily go along with the status quo there are many who will challenge it. Of concern is that fact that, as presented in the article in the March 2002 Scientific American, packet malformation is ignored. When new systems are designed and created, especially in this day and age – that is, post September 11th – security needs to be at the forefront.

That is definitely lacking in this proposal. It assumes that the worse security flaw would be clients not telling the “payers” that they have in fact done what is expected of them or telling them they have done more than that. What it doesn’t pay attention to is the fact that this kind of system is truly open, and that anyone can get into anyone else’s system. For most users, the common answer – even in today’s present Internet is – “I don’t have anything worthwhile to steal”. We often forget that we do – our identity.

Second to this is the trustworthiness of the “Internet-Scale Operating System” or ISOS, as well as hardware issues. The issue of trustworthiness is similar to the issue found within the clients. Given the lack of protection of consumers by Internet predators it is truly foolish to plan and develop systems that cannot be supported or governed. The temptation to “rip-off” clients is too easy. How will users be protected when they participate but aren’t paid accordingly.

Further to this is the issue of hardware. Whatever the OS is to be one thing it cannot be: hardware or platform specific. We did not do as IBM once predicted: be a society with only 5 computer manufacturers. We have thousands of different products, types, levels, etc. Additionally, the overhead required to run the OS should be minimal, otherwise many pockets of the PC environment may be inadvertently excluded.

It should be perferrable that more though is put into many of our great concepts before they are presented to the public as a possible future.

Have a rant? want to write a letter to the editor? Just send a PM to MsMittens for submission to the next issue of AntiOnline Newsletter

What is a Trojan...?

And what is the code for programming it... (part1) by Rip7

A Trojan is a program witch has 2 sides a server side and a client side. The server side you must install by your victim, the client side is for controlling the server (the victim). Easy not. But how works such a program and what is the code.

How does it work

First of all you need an example code for such a program, we keep it simple and we chose only for the server code. This server code search for passwords, username's and so on and send this information to you (in this example with an e-mail). This code can you find at the download section of antionline (the name of the program is atomica2).

This is a large program so I will only explain the basics later I will explain some advanced programming techniques like Winsock.

(The program is coded in c++ (Microsoft visual c++))

In this part you can change some basic things like names (nothing special) but read it careful.

```
#define RSP_SIMPLE_SERVICE 1 // registers app as a service
#define RSP_UNREGISTER_SERVICE 0 // unregisters app as a service
#define DEF_MSGTITLE "NOOP" // message box title
#define DEF_MESSAGE "Are you sure you want to apply this patch ?"
// message box text

#define DEF_REGKEY "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
// the registry key under wich the
// registry value is stored
#define DEF_REGVALUE "DialUpSecurity" // the registry value where exe_path
// is stored
#define DEF_CHECKFILE "rasxnfo.dll" // this file is used to check if the
// ras informations have changed
#define DEF_SAVEFILE "rasxnft.dll" // this file is used for saving ras
// informations even if there is no
// connection to the internet.
// it is useful if you have access to
// the victim's system directory.
#define DEF_EXENAME "dialupsc.exe" // this will be set when the program
```


Data - <http://www.hideaway.net/data.html>
ANTIONLINE - <http://www.antionline.com>

go to this site and read the information about security exploits it can help you making your own trojans.

2. Configuring a Trojan (like subseven) (for newbies)

First of all you must understand some basic words

-Ports = this are the ports were a program will listen to (server side) and make connection (client side) to. (There are 65536 ports)

-A destination address (ip or host name) = the victims address ->(this must be the internet address and not the LAN address!!)<-

-Smtp = the ISP who gives you the e-mail service with mail or smtp for it and the country code after it (like: smtp.skynet.be). This is needed when your program must send e-mails to you. The name of your smtp server can you find in the manual of your isp server. you must not use the smtp of your server it may also be another when like hotmail

And now for the configuring

First of all we must configure the server. Open the window where you can configure the server (the configuring is on all servers the (\pm) same), when you see a label with port on it fill in a port number (in some programs like winchcrash you mustn't configure the server you must only know the Ip address for connecting to the server).

After that we can enter a protect password this password is needed when you are scared other people will change the server and re-configuring it. In subseven you can also fill in another pass, this pass is used for? Security ;-)? When you will connect to the server subseven ask this password.

in some caches you can chose for a random port, random file name's and random victim's name (this victim name is used for identification, you never know when you are in the ronge computer except with this J).

Now for the start-up methods, this is simple use the registry run and one other of you choice.

Notifications:

1. SIN notification = when you activate this the server will send a signal to the client every time he will start (this is good for the people with cable). The sin will also tell on witch port the server is listening and on witch Ip address.

2. E-mail notify = this option will send E-mail to the destination address (sometimes you must fill in your smtp server)

3. others like: irc notify (self explaining)

some very good trojans:

bionet and Progenic (in the next part a whole article over the best trojans)

That's all

in the next part:

- an article about the best trojans <—
- the winsock code (by rip7) <—

any comments,tips,questions,... can you mail at sterewb@crosswinds.net

So.. do you like what you see? If you do, how about submitting your article, tutorial or rant about security related issues or computing in general? Are you a budding cartoonist or artist? We could use some graphics! Here's a list of some things we are looking for:

- cartoons/pictures
- articles, howtos, rants
- book reviews
- anything else that might help someone else better protect themselves online

Send them to me via PM or to msmittens@msmittens.com

Unix Tutorial #2:

Grep is your friend...

Ok. The long awaited second part to the Unix Tutorial. `grep`. A wonderful tool. Something we should forget about and how powerful it can be. `grep` is actually an acronym command which means Global Regular Expression Printer. Fancy, eh?

I'm going to make a distinction between the command `grep` and the `find` command. `grep` is used to find or locate patterns inside of something. `find` is used to find files or directories. `find` can run other commands against the results it found. Ok. Let's start with `grep`. Look at the example below and state what the command pattern is:

1. Excavate elongate aggetate tidewater
2. 23237294 092339452 56489723474 8437254323 9348823458734

Ok. Have you found them. The first row is easy: `ate` appears through all the words. In the second row, if you look carefully you will see `23` appearing. Our patterns if you will. `grep` is used to find patterns in files (remember, when you do an `ls` command it is nothing more than a file).

So one thing you might `grep` for is to see if there is a root account in the shadow file (do you know where your shadow file is or an equivalent file is?). Simply type:

```
grep root /etc/shadow
```

You are telling the system that you are looking for the pattern `root` in the file `/etc/shadow`. I can combine it with a pipe `|` to help filter items out. For example, if I wanted to find a file that begins with a capital `M` but don't remember the name of it and it's somewhere on my file system I can type:

```
ls -Ra / | grep ^M
```

The little "hat", referred to as a caret (pronounced ca-rayt), means at the beginning of a line. I can search at the end of a line by putting a `$` after the pattern I'm looking for. Now the only downside to this is that it will return all files that begin with a capital `M`. I can narrow it down a bit by doing this:

```
ls -IRa / | grep mittens | grep M
```

Now, this example has me filter all the files found under root (`/`) for the pattern `mittens`

(hopefully I haven't called any files mittens) and that have a capital M. Now why did I use my "hat"? Well, notice I did a long listing this time. That means the listing will begin with the permissions. The name of the file is actually found at the end of the listing.

And like *nix as a whole, it is a case-sensitive command. It will look for that pattern exactly as its typed. If however you were looking for the name mittens in an /etc/passwd file but that it might be spelt as mittens or Mittens or msmittens or MsMittens, then we need to add another option to the command. grep has a case-insentive option which means that it can "turn-off" the case-sensitive normally found in the command.

grep -i mittens /etc/passwd

Other things to keep in mind about grep:

- the "." or dot will match any single character. As an example,
grep m...ens /etc/passwd would match exactly 3 characters between m and e in the pattern, any 3 characters.
- a combination of the dot and asterisk metacharacter ".*" means any number of characters
grep m.*ens /etc/passwd would match any number of characters between the m and e in the pattern.
- in some cases you might need to search for metacharacters (* ./\ \$ ^, etc.). We can do pattern searches using grep and \. The backslash is called an escape character in grep.
grep www\.\antionline\.com /etc/hosts if I wanted to search for the pattern of www.antionline.com
- lastly, if a pattern has spaces or tabs, the entire pattern must be included in between single quotes.

The best way to practise grep is to create some files and do searches for items.

Next newsletter: Unix Tutorial 3: Have you found your find yet?

Note from author: all mistakes are mine and Microsoft Word with it's stupid autocorrect feature. Remember that all commands should be lowercase. Options may be lowercase or uppercase. Do not forget to use the man pages to help find information about commands or go and buy the wonderful book: Unix in a Nutshell by O'Reilly Press.

As we go through the basics of *nix I will start to add in *nix security tips (probably this summer as it looks like I will be teaching it for the summer.)

Security Auditing by Remote_Access_

Security auditing should be a requirement for everyone that is connected to the Internet. There are many tools and programs available to help you test your network or PC at home. A few topics you should read about and have a good general knowledge are:

Firewalls - what they are, how to use one, where to get one, etc.

IDS - Intrusion Detection System

Sniffers - to find out where that DoS attack came from, who sent what packet, etc.

Buffer overflow protection - Keep your box safe from this common vulnerability

Honey pots - creates virtual systems to trap scanners and hackers

Proxy – to help you remain anonymous on the web

SOCKS chain - work through a chain of SOCKS or HTTP proxies to conceal the actual IP-address.

Security auditing can be done for a fee from various companies or done by you to save a few dollars and get more of a hand on experience with testing your network or your box at home. Here are a few things to look for when testing the security of your box:

Vulnerabilities

Malware – Trojans & viruses

NFS - way of sharing files

Network monitoring tools – PC Anywhere, Remote admin, etc.

Physical Security - most overlooked vulnerability

Wingate - allows a Win95 PC to act as a gateway.

CGI Scripts - poorly written CGI (Common Gateway Interface) programs are vulnerable to intruders.

For a more detailed list of vulnerabilities visit [Http://www.CERT.org](http://www.CERT.org)

Ports

You should monitor what ports and services are running on your machine. Especially the ones that you don't recognize. You can find a list of ports and what services run on those ports on any of your favorite search engines. To remove the risk of being attacked, close any application that you find suspicious and view the file's properties.

To Enter or not To Enter...

By Andrew Matheson

So you have your CISCO PIX firewall, you have your password files all set, you have your virus scanning all up to date...but hold on a second...you don't lock your office door???

Well...you have failed at the first rule of total network security...PHYSICAL SECURITY.

You can password, port block and lock down a network all you want, but if the public has free physical access to the network, then all your efforts are futile.

To begin designing proper physical security, one needs to look no further than their own backyard. Does the guy in the mail room have access to the server room, or only the network technicians? Is your server closet on the main floor next to the main entrance, or is it on a floor all on its own? Form lockable server cabinets, pass cards, retinal scans and security patrols, there are many ways to physically ensure that your data and network are safe.

One extreme case of physical security is Rack Space® their data centre is like Fort Knox as you will see from the following URL:

<http://www.rackspace.com/infrastruc...ctid=0104-99999>

"Physical Security

The data center is physically isolated from everyone but level three technicians. Public access is strictly forbidden. Access to the floor the data center resides on is restricted to those holding Rackspace military-grade passcards. Furthermore, access to the data center itself is restricted by Biometric hand scanners." (quote from www.rackspace.com)

This is an extreme case of physical security. Only have 15 employees? Then by using locking server cabinets, and using a keycode door lock on the server room, you can secure your network from most intruders.

Do you run a mission critical network for millions of users? Then hand scanners, retinal scans, systems that require two different unlocking mechanisms and military level access and keycode doors are for you.

All in all, physical security can be as easy as a lock, or as complex as an FBlesque system.

Whatever you choose, remember that your network isn't secure until it is physically secure.

Enjoy!

Default Password Paths

Compiled by s0nic

As administrators it's good to know where these are so we can better protect those locations. Where can Unix or Windows password files usually be found?

| Windows System Type | Path | Token |
|---|---|-------|
| Windows9x | \\windows\user.pwl | |
| Windows 2000 | \\WINNT\system32\config\SAM or | |
| \\WINNT\repair\SAM | | |
| UNIX System Type | Path | Token |
| AIX 3 | /etc/security/passwd | |
| or | | |
| /tcb/auth/files/<first letter of username>/<username> | | ! |
| or | | |
| # | | |
| A/UX 3.Os | /tcb/files/auth/* | * |
| BSD4.3-Reno | /etc/master.passwd | * |
| ConvexOS 10 | /etc/shadpw | * |
| ConvexOS 11 | /etc/shadow | * |
| DG/UX | /etc/tcb/aa/user | * |
| EP/IX | /etc/shadow | X |
| HP-UX | /.secure/etc/passwd | * |
| IRIX 5 | /etc/shadow | X |
| Linux 1.1 | /etc/shadow | * |
| OSF/1 | /etc/passwd[.dir .pag] | * |
| SCO UNIX #.2.x | /tcb/auth/files/<first letter of username>/<username> | * |
| SunOS 4.1+c2 | /etc/security/passwd.adjunct | ## |
| SunOS 5.0 | /etc/shadow | |
| System V 4.0 | /etc/shadow | X |
| System V 4.2 | /etc/security/* database | |
| Ultrix 4 | /etc/auth[.dir .pag] | * |
| UNICOS | /etc/udb | * |

Default Passwords

compiled by s0nic

NOTE: This listing is only provided as a resource to network administrators and security professionals. It is also meant to remind people that a serious problem exists when people configure a network or a computer system and do not change these passwords. The manufacturers of the listed devices, software or systems are not to blame for this problem, and we are not trying to discredit them or their products. A default login is a means for an end user of a product to complete the initial setup of the device or system. Most manufacturers strongly recommend their end users change these logins and passwords for security reasons.

SNMP / Notes are only available on <http://security.nerdnet>.

| Manufacturer | Model | OS Version | Login | Password |
|--------------|------------------------------|--------------------|----------|--------------|
| 3Com | - | 1.25 | root | letmein |
| 3Com | Super Stack 2 Switch | Any | manager | manager |
| 3Com | AccessBuilder® 7000 BRI | Any | - | - |
| 3Com | CoreBuilder 2500 | - | - | - |
| 3Com | Switch 3000/3300 | - | manager | manager |
| 3Com | Switch 3000/3300 | - | admin | admin |
| 3Com | Switch 3000/3300 | - | security | security |
| 3com | Cable Management System | SQL Database (DOS) | CIC DHCP | Win2000 & MS |
| DOCSIS_APP | 3com | | | |
| 3Com | NAC (Network Access Card) | - | - | adm |
| none | | | | |
| 3Com | HiPer ARC Card | v4.1.x of HA | adm | none |
| 3Com | CoreBuilder 6000 | - | debug | tech |
| 3Com | CoreBuilder 7000 | - | tech | tech |
| 3Com | SuperStack II Switch 2200- | | debug | synnet |
| 3Com | SuperStack II Switch 2700- | | tech | tech |
| 3Com | SuperStack / CoreBuilder | - | admin | - |
| 3Com | SuperStack / CoreBuilder | - | read | - |
| 3Com | SuperStack / CoreBuilder | - | write | - |
| 3Com | LinkSwitch and CellPlex | - | tech | tech |
| 3Com | LinkSwitch and CellPlex | - | debug | synnet |
| 3com | Superstack II 3300FX | - | admin | - |
| 3com | Switch 3000/3300 | - | Admin | 3com |
| 3com | 3comCellPlex7000 | - | tech | tech |
| 3Com | Switch 3000/3300 | - | monitor | monitor |
| 3Com | AirConnect Access Point | n/a | - | comcomcom |
| 3com | Superstack II Dual Speed 500 | | - | security |
| curity | | | | se- |
| 3Com | OfficeConnect 5x1 | at least 5.x | - | PASSWORD |
| 3Com | SuperStack 3 Switch 3300XM | | - | admin |
| 3com | Super Stack 2 Switch | Any | manager | manager |
| 3Com | SuperStack II Switch 1100- | | manager | manager |
| 3Com | SuperStack II Switch 1100- | | security | security |
| 3com | super stack 2 switch | any | manager | manager |
| 3Com | Office Connect Remote 812 | | - | root |
| lroot | | | | |
| 3Com | Switch 3000/3300 | - | admin | admin |

| | | | | |
|----------------------------|----------------------------|---------------------|------------------------|------------|
| 3COM | OCR-812 | - | root | !root |
| 3com | - | - | - | - |
| 3com | NBX100 | 2.8 | administrator | 0000 |
| 3com | Home Connect | - | User | Password |
| 3Com | OfficeConnect 5x1 | at least 5.x | estheralatruey | - |
| 3Com | SuperStack II Switch 3300- | - | manager | manager |
| 3Com | Superstack | - | - | - |
| ACC | Routers | - | netman | netman |
| Acc/Newbridge | Congo/Amazon/Tigris | All versions | netman | netman |
| Acc/Newbridge | Congo/Amazon/Tigris | All versions | netman | netman |
| adaptec | - | - | - | - |
| Adaptec RAID | Storage Manager Pro | All | Administrator | adaptec |
| adtran | tsu 600 ethernet module | - | 18364 | - |
| Adtran | TSU 120 e | - | - | ADTRAN |
| Adtran | TSU 120 e | - | - | ADTRAN |
| Aironet | All | - | - | - |
| alcatel | - | - | - | - |
| Alcatel | 1000 ANT | Win98 | - | - |
| alcatel | speed touch home | - | - | - |
| Alcatel/Newbridge/Timestep | VPN Gateway 15xx/45xx/7xxx | - | Any | root |
| permit | - | - | - | - |
| Alcatel/Newbridge/Timestep | VPN Gateway 15xx/ | Any | root | permit |
| Alcatel/Newbridge/Timestep | VPN Gateway 15xx/ | Any | root | permit |
| Allied Tensin | R130 | - | Manager | friend |
| Alteon | ACEswitch 180e (telnet) | - | admin | blank |
| Alteon Web Systems | All hardware releases | Web OS 5.2 | none | admin |
| APC | MasterSwitches | - | apc | apc |
| APC | Any | Firmware Priapcuser | - | apc |
| Apple | Network Assistant | 3.X | None | xyzzzy |
| Apple | Airport | 1.1 | none | public |
| Arrowpoint | any? | - | admin | system |
| Ascend | All TAOS models | all | admin | Ascend |
| Ascend | Pipeline Terminal Server | - | answer | - |
| Ascom | Timeplex Routers | Any | See notes | - |
| AT&T | Starlan SmartHUB | 9.9 | N/A | manager |
| AWARD | Any BIOS | - | AWARD_SW | - |
| Axent | NetProwler manager | WinNT | administrator | admin |
| Axis | NPS 530 | 5.02 | root | pass |
| AXIS | StorPoint CD100 | 4.28 | root | pass |
| AXIS | 200 V1.32 | - | admin | - |
| Axis | 2100 Network Camera | Linux (ETRAX | - | root |
| pass | - | - | - | - |
| bay | cv1001003 | - | - | - |
| bay | - | - | - | - |
| Bay | - | - | - | - |
| Bay / Nortel | ARN | 13.20 | Manager (caps count !) | - |
| Bay Network Routers | All | - | User | - |
| Bay Networks | ASN / ARN Routers | Any | Manager | Manager |
| Bay Networks | Baystack | - | - | NetICs |
| Bay/Nortel Networks | Accelar 1xxx switches | Any | rwa | rwa |
| Bay/Nortel Networks | Remote Annex 2000 | Any | admin | IP address |
| BEA | Weblogic | 5.1 | system | weblogic |
| BEA | - | - | - | - |

| | | | | | |
|---|----------------------------------|------------------------------|--------------------------|---------------------|-----|
| bewan | - | - | - | - | |
| Bintec | all Routers | Any | admin | bintec | |
| Bintec | - | - | - | - | |
| Biodata | BIGfire & BIGfire+ | all | - | biodata | |
| Biodata | all Babylon-Boxes | all | - | Babylon | |
| Black Box terminal server / telnet auf ports 2001-2016 LES2700A-422 | | LES2700A-16, LES2700A-32 and | SYSTEM (admin rights) | | |
| Borland | interbase | - | - | - | |
| Borland | Interbase | Any | politically | correct | |
| Borland/Inprise | Interbase | any | SYSDBA | masterkey | |
| BreezeCom | AP10, SA10 | BreezeNET | PR | - | - |
| BreezeCOM | Station Adapter and Access Point | | 4.x | - | Su- |
| per | | | | | |
| BreezeCOM | - | 3.x | - | Master | |
| BreezeCOM | Station Adapter and Access Point | | 2.x | - | |
| laflaf | | | | | |
| Brocade | Silkworm | - | admin | password | |
| Buffalo/MELCO default) | AirStation WLA-L11 | - | root (cannot be changed) | (no password by | |
| Cabletron | any | any | — | — | |
| Cabletron | NB Series | Any | - | inuvik49 | |
| Cabletron routers and switches | | * | * | blank | |
| blank | | | | | |
| Cayman | 3220-H DSL Router | GatorSurf 5. | Any | - | |
| celerity | - | - | - | - | |
| Chase Research | Iolan+ | - | - | Iolan | |
| Cisco | Any Router and Switch | 10 thru 12 | cisco | cisco | |
| Cisco | ConfigMaker Software | any? | n/a | cmaker | |
| CISCO | Network Registrar | 3.0 | ADMIN | changeme | |
| CISCO | N/A | N/A | pixadmin | pixadmin | |
| Cisco | routers | Not sure...j | - | san-fran | |
| Cisco | VPN 3000 Concentrator | - | admin | admin | |
| Cisco | Net Ranger 2.2.1 | Sol 5.6 | root | attack | |
| cisco | 1600 | 12.05 | - | - | |
| cisco | 1601 | - | - | - | |
| cisco | - | - | - | - | |
| cisco | - | - | - | - | |
| Cisco | MGX | * | superuser | superuser | |
| cisco | 1601 | - | - | - | |
| cisco | - | - | - | - | |
| Cisco | - | - | - | - | |
| cisco | - | - | - | - | |
| Cisco | any | aany IOS | no default login | no default password | |
| CISCO | arrowpoint | - | - | - | |
| cisco | - | - | - | - | |
| cisco | - | - | - | - | |
| cisco | - | - | - | - | |
| Cisco | 2503 | - | - | - | |
| Cisco | - | - | - | - | |
| cisco | - | - | - | - | |
| Cisco | IDS (netranger) | - | root | attack | |
| cisco | - | - | - | - | |

| | | | | |
|------------------------------|-----------------------------------|--------------|----------------------------|---------------|
| cisco | 1600 | - | - | - |
| CMOS BIOS | - | - | - | ESSEX or IPC |
| Cobalt | RaQ * Qube* | Any | admin | admin |
| Com21 | - | - | - | - |
| Comersus Shopping Cart | 3.2 | Win 95/98/NT | | admin |
| dmr99 | | | | |
| Compaq | Insight Manager | - | Administrator | administrator |
| Compaq | Insight Manager | - | operator | operator |
| Compaq | Management Agents | All | administrator | none |
| compaq | - | - | - | - |
| copper mountain | - | - | - | - |
| Coppercom | - | - | - | - |
| Coyote-Point | Equaliser 4 | Free BSD | eqadmin - Serial port only | equalizer |
| Coyote-Point | Equaliser 4 | Free BSD | root - Serial port only | - |
| Coyote-Point | Equaliser 4 | Free BSD | look - Web Browser only | (Read a |
| look | | | | |
| Coyote-Point | Equaliser 4 | Free BSD | touch - Web Browser only | (Write |
| touch | | | | |
| Cyclades | MP/RT | - | super | surt |
| D-Link | DI-704 | - | - | admin |
| D-Link | DI-701 | 2.22 (?) | - | - |
| Dell | PowerVault 50F | WindRiver (E | | root |
| calvin | | | | |
| Dell | PowerVault 35F | - | root | calvin |
| Dell | Powerapp Web 100 Linux | RedHat 6.2 | root | powerapp |
| dell | - | - | - | - |
| Digiboard | Portserver 8 & 16 | any | root | dbps |
| DLink | DI-206 ISDN router | 1.* | Admin | Admin |
| Dlink | DI-106 ISDN router | - | - | 1234 |
| DLink | DL-701 Cable/DSL Gateway/Firewall | - | - | - |
| year2000 | | | | |
| Dlink | DFE-538TX 10/100 Adapter | | Windows 98 | - |
| dlink | di704 | - | - | admin |
| DLink | DI 106 | winnt | administrator | @*nigU^D.ha,; |
| Dupont Digital Water Proofer | Sun Sparc | any | root | par0t |
| eci | - | - | - | - |
| Efficient | - | - | - | - |
| Elron | Firewall | 2.5c | hostname/ip address | sysadmin |
| emai | hotmail | - | - | - |
| Ericsson | ACC | - | netman | netman |
| Ericsson (formerly ACC) | Any router | all | netman | netman |
| Extended Systems | ExtendNet 4000 / Firewall | all Versions | admin | admin |
| Extended Systems | Print Servers | - | admin | extendnet |
| Extreme | All Summits | - | admin | - |
| extreme | black diamond | - | - | - |
| Extreme | All | All | Admin | - |
| Flowpoint | 144, 2200 DSL Routers | ALL | - | password |
| FlowPoint | 144, 2200 DSL Routers | ALL | - | admin |
| Flowpoint | 2200 | - | - | Serial Num |
| Flowpoint | 2200 | - | - | Serial Num |
| fore | - | - | - | - |
| Fore Systems | ASX 1000/1200 | 6.x | ami | - |
| Foundry Networks | ServerIronXL | Any | - | - |

| | | | | | |
|---------------------|---|--------------|-------------|---------------|---|
| fujitsu | l460 | - | - | - | - |
| Future Networks | FN 110C Docsis cablemodem | | Any | - | - |
| gateway | solo9100 | win95 | - | - | - |
| General Instruments | SB2100D Cable Modem | - | test | test | |
| gonet | - | - | fast | abd234 | |
| Hewlett Packard | HP Jetdirect (All Models) | Any | none | none | |
| Hewlett Packard | MPE-XL | - | HELLO | MANAGER.SYS | |
| Hewlett Packard | MPE-XL | - | HELLO | MGR.SYS | |
| Hewlett Packard | MPE-XL | - | HELLO | FIELD.SUPPORT | |
| Hewlett Packard | MPE-XL | - | MGR | CAROLIAN | |
| Hewlett Packard | MPE-XL | - | MGR | CCC | |
| Hewlett Packard | MPE-XL | - | OPERATOR | COGNOS | |
| Hewlett Packard | MPE-XL | - | MANAGER | HPOFFICE | |
| hp | 4150 | - | - | - | |
| hp | - | - | - | - | |
| IBM | AS/400 | - | qsecofr | qsecofr | |
| IBM | AS/400 | - | qsysopr | qsysopr | |
| IBM | AS/400 | - | qpgmr | qpgmr | |
| IBM | NetCommerce PRO | 3.2 | ncadmin | ncadmin | |
| IBM | LAN Server / OS/2 | 2.1, 3.0, 4. | username | password | |
| IBM | 2210 | RIP | def | trade | |
| IBM | DB2 | WinNT | db2admin | db2admin | |
| IBM | Lotus Domino Go WebServer (net.commerce edition) | | | ANY ? | |
| webadmin | webibm | | | | |
| IBM | AS400 | Any | QSECOFR | QSECOFR | |
| IBM | RS/6000 | AIX | root | ibm | |
| IBM | - | OS/400 | QSECOFR | QSECOFR | |
| IBM | AS400 | - | QSRVBAS | QSRVBAS | |
| IBM | AS400 | - | QSRV | QSRV | |
| ibm | as400 | - | - | - | |
| IBM | AS/400 | OS/400 | QUSER | QUSER | |
| IBM | AS/400 | - | - | - | |
| IBM | ra6000 | AIX Unix | - | - | |
| IBM | AIX | - | - | - | |
| Imperia Software | Imperia Content Managment System | | Unix/NT | superuser | |
| superuser | | | | | |
| Intel | 510T | Any | - | admin | |
| Intel | All Routers | All Versions | - | babbit | |
| Intel | All Routers | All Versions | - | babbit | |
| Intel | Intel PRO/Wireless 2011 Wireless LAN Access Point | | | Any | - |
| Intel | | | | | |
| Intel | wireless lan access Point | - | - | comcomcom | |
| lpswitch | Whats up Gold 6.0 | Windows 9x | a | admin | |
| admin | | | | | |
| janta sales | 254 | compaq | janta sales | janta211 | |
| janta sales | 254 | compaq | janta sales | janta211 | |
| Jetform | Jetform_design | - | Jetform | - | |
| Kawa | - | - | - | - | |
| LANCAST | - | - | - | - | |
| Lantronix | LPS1-T Print Server | j11-16 | any | system | |
| Lantronix | MSS100, MSSVIA, UDS10 | | Any | - | |
| system | | | | | |
| Lantronix | LSB4 | any | any | system | |

| Printer and terminal servers | | | | |
|------------------------------|--------------------------|--------------|---------------|-------------|
| lantronix | | | - | - |
| system | | | | |
| LGIC | Goldstream | 2.5.1 | LR-ISDN | LR-ISDN |
| Linkou School | - | - | bill | bill |
| Linkou School | - | - | bill | bill |
| Linksys | Cable/DSL router | Any | - | admin |
| Linksys | BEFSR7(1) OR (4) | Standalone R | | blank |
| admin | | | | |
| linksys | - | - | - | - |
| Linksys | BEFSR41 | - | (blank) | admin |
| Livingston | Livingston_portmaster2/3 | - | !root | blank |
| Livingston | Livingston_officerouter | - | !root | blank |
| Lucent | Portmaster 2 | - | !root | none |
| Lucent | Cajun Family | - | root | root |
| lucent | Portmaster 3 | unknown | !root | !ishtar |
| Lucent | Packetstar (PSAX) | - | readwrite | lucenttech1 |
| Lucent | AP-1000 | - | public | public |
| lucent | dsl | - | - | - |
| lucent | - | - | - | - |
| macromedia | freehand | 9 | - | - |
| MacSense | X-Router Pro | - | admin | admin |
| mcafee | - | - | - | - |
| microcom | hdms | unknown | system | hdms |
| Micron | - | bios | - | - |
| Microrouter (Cisco) | Any | Any | - | letmein |
| Microrouter (Cisco) | Any | Any | - | letmein |
| Microsoft | Windows NT | All | Administrator | - |
| Microsoft | Windows NT | All | Guest | - |
| Microsoft | Windows NT | All | Mail | - |
| Microsoft | SQL Server | - | sa | - |
| Microsoft | Windows NT | 4.0 | pkoolt | pkooltPS |
| Microsoft | NT | - | - | start |
| MICROSOFT | NT | 4.0 | free user | user |
| Microsoft | Windows NT | 4.0 | admin | admin |
| MICROSOFT | NT | 4.0 | free user | user |
| Microsoft | - | - | - | - |
| microsoft | - | - | - | - |
| Microsoft | Ms proxy 2.0 | - | - | - |
| microsoft | - | - | - | - |
| mICROSOFT | - | - | - | - |
| Microsoft | Key Managment Server | Windows NT 4 | | - |
| password | | | | |
| Microsoft | - | - | - | - |
| Motorola | Motorola-Cablerouter | - | cablecom | router |
| Motorola | Motorola-Cablerouter | - | cablecom | router |
| motorola | cyber surfer | - | - | - |
| msdloto | msdloto | - | - | - |
| msdloto | - | - | - | - |
| Multi-Tech | RASExpress Server | 5.30a | guest | none |
| Nanoteq | NetSeq firewall | * | admin | NetSeq |
| NetApp | NetCache | any | admin | NetCache |
| Netgaer | RH328 | - | - | 1234 |
| Netgear | RH348 | - | - | 1234 |
| Netgear | ISDN-Router RH348 | - | - | 1234 |

| | | | | |
|--------------------------|------------------------------------|--------------|-------------------|-------------------|
| Netgear | RT311 | Any | Admin | 1234 |
| Netgear | RT314 | Any | Admin | 1234 |
| Netgear | RT338 | - | - | 1234 |
| Netgear | RT311/RT314 | - | admin | 1234 |
| netgear | - | - | - | - |
| netlink | rt314 | - | - | - |
| Netopia | R7100 | 4.6.2 | admin | admin |
| Netopia | 455 | v3.1 | | |
| Netscreen | NS-5, NS10, NS-100 | 2.0 | netscreen | netscreen |
| NeXT | - | NeXTStep 3.3 | | me |
| Nokia - Telecom NZ | M10 | - | Telecom | Telecom |
| Nortel | Meridian 1 PBX | OS Release 2 | | 0000 |
| 0000 | | | | |
| Nortel | Contivity Extranet Switches | | 2.x | admin |
| setup | | | | |
| Nortel | Norstar Modular ICS | Any | **ADMIN (**23646) | ADMIN (23646) |
| Nortel | Norstar Modular ICS | Any | **CONFIG (266344) | CONFIG (266344) |
| Nortel Networks (Bay) | Instant Internet | Any | - | - |
| Northern Telecom(Nortel) | Meridian 1 | - | - | m1link |
| Novell | NetWare | Any | guest | - |
| Novell | NetWare | any | PRINT | - |
| Novell | NetWare | Any | LASER | - |
| Novell | NetWare | Any | HPLASER | - |
| Novell | NetWare | Any | PRINTER | - |
| Novell | NetWare | Any | LASERWRITER | - |
| Novell | NetWare | Any | POST | - |
| Novell | NetWare | Any | MAIL | - |
| Novell | NetWare | Any | GATEWAY | - |
| Novell | NetWare | Any | GATE | - |
| Novell | NetWare | Any | ROUTER | - |
| Novell | NetWare | Any | BACKUP | - |
| Novell | NetWare | Arcserve | CHEY_ARCHSVR | WONDERLAND |
| Novell | NetWare | Any | WINDOWS_PASSTHRU | - |
| novell | - | - | - | - |
| ODS | 1094 IS Chassis | 4.x | ods | ods |
| Optivision | Nac 3000 & 4000 | any | root | mpegvideo |
| Oracle | 8i | 8.1.6 | sys | change_on_install |
| Oracle | Internet Directory Service | any | cn=orcladmin | welcome |
| Oracle | 7 or later | - | system | manager |
| Oracle | 7 or later | - | sys | change_on_install |
| Oracle | 7 or later | Any | Scott | Tiger |
| Oracle | 8i | all | internal | oracle |
| oracle | - | - | - | - |
| oracle | - | - | - | - |
| oracle co. | Database engines | every | sys | change_on_install |
| Osicom(Datacom) | Osicom(Datacom) | - | sysadm | sysadm |
| Pandatel | EMUX | all | admin | admin |
| PlainTree | Waveswitch 100 | - | - | default.password |
| RapidStream | RS4000-RS8000 | Linux | rsadmin | rsadmin |
| realtek | 8139 | - | - | - |
| Remedy | Any | Any | Demo | - |
| Research Machines | Classroom Assistant | Windows 95 | manager | changeme |
| Rodopi | Rodopi billing software 'AbacBill' | sql database | | - |

| | | | | |
|-------------------|----------------------------|-------------|--------------------------|---------------------|
| rodopi | rodopi | | | |
| ROLM | phones/phone mail | | | 111# |
| Samba | SWAT Package | Linux | Any Local User | Local User password |
| schoolgirl | member | - | ich | hci |
| Securicor3NET | Monet | any | manager | friend |
| Securicor3NET | Cezzanne | any | manager | friend |
| SGI | all | all | root | n/a |
| SGI | Embedded Support Partner | | IRIX 6.5.6 | Administrator |
| Partner | | | | |
| SGI | IRIX | ALL | lp | lp |
| SGI | IRIX | ALL | OutOfBox, demos, guest, | 4DGifts |
| (none by default) | | | | |
| SGI | IRIX | ALL | EZsetup | - |
| Shiva | LanRover | any? | root | - |
| Shiva | AccessPort | Any | hello | hello |
| Shiva | Any? | - | Guest | blank |
| SMC | Barricade | - | - | admin |
| soho | nbg800 | unknown | admin | 1234 |
| Solaris | - | - | - | - |
| sonic wall | any firewall device | admin | password | - |
| SonicWall | Any Firewall Device | - | admin | password |
| SpeedStream | - | - | - | - |
| Spider Systems | M250 / M250L | - | - | hello |
| Sprint PCS | SCH2000 | see notes | Menu - 8 - 0 (see notes) | 040793 |
| Ssangyoung | SR2501 | - | - | 2501 |
| Sun | - | SunOS 4.1.4 | | root |
| Sun | - | Solaris | - | - |
| surecom | ep3501/3506 | own os | admin | surecom |
| Symnatec | - | - | - | - |
| SysKonnnect | 6616 | - | default.password | - |
| SysKonnnect | 6616 | - | default.password | - |
| Tekelec | Eagle STP | - | eagle | eagle |
| Telebit | netblazer 3.* | - | setup/snmp | setup/nopasswd |
| Terayon | TeraLink Getaway | - | admin | password |
| Terayon | TeraLink 1000 Controller | - | admin | password |
| Terayon | TeraLink 1000 Controller | - | user | password |
| Terayon | TeraLink Getaway | - | user | password |
| terayon | - | 6.29 | admin | nms |
| Terrayon | - | - | - | - |
| Titbas | - | SCO | haasadm | lucy99 |
| TopLayer | AppSwitch 2500 | Any | siteadmin | toplayer |
| Toshiba | TR-650 | V2.01.00 | admin | tr650 |
| toshiba | 480cdt | - | - | - |
| toshiba | - | - | - | - |
| TrendMicro | ISVW (VirusWall) | any | admin | admin |
| Trintech | eAcquirer App/Data Servers | - | - | t3admin |
| Trintech | | | | |
| Ullu ka pattha | Gand mara | Gandoo | Bhosda | Lund |
| USR | TOTALswitch | Any | none | amber |
| Vina Technologies | ConnectReach | 3.6.2 | (none) | (none) |
| voy | - | - | - | - |
| WatchGuard | FireBox | 3-4.6 | - | wg (touch password) |