November 1997
Volume 1, Issue 11

The Insider

Your Knowledgebase on Computer Security

Inside this Issue

Coming Up

Dec '97 **Who's There?**
Remote Access Systems and Virtual Private Networks

Jan '98 **Forget Steroids - Eat more Rice!**
Beefing up the Security within Your Networks

Feb '98 **Who Watches The Watchers?**
Intrusion Detection Systems to Protect Your Network

Mar '98 **Spy Stuff**
Protecting your Mobile Data with Encryption

Can't Wait for the Info?
Contact our Senior Security Consultant Now
041 4411 149

Technical Incursion Countermeasures Pty. Ltd.
ACN 080 068 891

Phone (08) 9429 8898
Fax (08) 9429 8800
Secure Fax (08) 9454 6042 (bus hrs)

1 Havelock Street
West Perth, WA, 6005
Australia

So all you need is a firewall to protect your business from attacks, right? And a Firewall is a Firewall isn't it? Wrong!

Think of a firewall as the security guard checking everyone leaves the shopping centre. A good guard will check everyone's bag to make sure that they are not stealing something. A bad guard will just look at what they are carrying, or worse still - what they look like.

For a corner store a bad guard will probably be OK, after all stealing the lollies won't put the corner store out of business - they can only carry so much before being noticed. However, having each person steal something in a large supermarket would not be good and for a jewlerry store, disastrous.

The point here is that the more valuable your data is, the stronger the firewall you should use to protect it.

What is Available?

Packet Filters

The cheapest and weakest are the Packet Filtering Firewalls. These firewalls simply look at each packet of data as it flows though and checks it against a simple table before allowing it or denying it.

These firewalls are good for small offices or home offices where the value of the data is low and the connection to the outside world (either by the Internet or by dial-up) is in the form of a modem. A good example is the Phoenix Firewall from iinet Technologies. This firewall also offers all that a small business needs to present a permanent presence on the Internet - mail server, web server and other services all in one box.

Stateful Inspection

The next weakest is the Stateful Inspection Packet Filtering Firewall - sometimes known as a Dynamic Filtering Firewall. These firewalls know how a particular protocol should work. In other words the firewall has seen the person enter the store, it knows that they picked up something and it is expecting them to pay for it - if they do not it stops them leaving. Note: the guard did not check the contents of the bag.

These types of firewalls are very good for ISPs wanting to provide a moderate level of protection for their clients web servers, mail, etc. A good example of this technology is the SPF200 system from Sun Computers or the Cisco PIX. It is available from Technical Incursion Countermeasures or Alphawest.

Application Proxies

For a stronger system, we need to go to a different technology - Application Proxies. These firewalls work something like the cashier at the Casino. You ask the person for some gambling chips and they take your money and hand them to you. In other words, a Proxy Firewall does not let data through it, it fetches the data on the client's behalf.

Unlike Packet filters, Proxy servers are made up of many small applications; each application is effectively a client and a server. So when you use a web browser to surf the web the firewall appears as a server to you browser and a browser to the rest of the world. In this way it can inspect the contents of each packet and determine what is safe and what is not.

Interestingly, all the Certified

firewalls are Application Proxy types.

Certification is currently done by the NSA in the US and ITSEC in Europe. Certification is a lengthy and expensive process, but it gives a good indication of the strength of the firewall and the commitment of the company behind it. Uncertified firewalls might be as strong, but they have not been tested.

NOTE the NCSA tests firewalls by a very simple procedure. Full certification involves not just testing the firewall, but inspecting the source code.

An example of an uncertified Proxy Server is the Technologic Interceptor. This relatively cheap firewall is good for companies with valuable data but a low budget. It is a Firewall Appliance - that is, it is delivered as a single working unit; most firewalls require you to purchase the software and the hardware separately.

There are only two certified Firewalls at this date, these are the TIS Gauntlet and the Cyberguard Firewall. These systems are ideal for companies where money or valuable data is involved. These systems run on certified secure operating systems and have had the firewall applications certified as well.

What is Technical Incursion Countermeasures?

Technical Incursion Countermeasures is the science of defending a facility from attempts to enter by technological means - as opposed to using a sledgehammer.

As a company, Technical Incursion Countermeasures (TICM for short) provide specialist consultation and devices to improve the security of your computer systems. TICM can be visualised as a System Integrator for security systems. We are able to provide almost any firewall and security device or software, ranging from disk encryption systems for laptops to E3 certified Firewalls and strong Authentication Systems. We also provide security auditing and training.

TICM is based in Perth, Western Australia, but is able to supply services over the entire ASEAN and Oceania regions.

Subscriptions

Did you receive this from a friend? Perhaps you would like to receive it direct? Please fill in the Following and fax it to (08) 9429 8800.

All data will be classified “Confidential” and will not under any cirumstances be released to a third party, it will be destroyed after five years of disuse.

Name: _____

Company: _____

Department _____ Position _____

Phone _____ Fax _____

Email _____

Company URL _____

Note:
The following are optional but will assist us greatly in tailoring the newsletter to our readers. If you are a current subscriber, but have not filled in this section we would also appreciate it.

External Connections

Remote Dial-up ☐

Internet ☐

Speed of line _____

Firewall _____

Mail Filter _____

Authentication _____

Internal Networks

TCP/IP	NetWare	MS NT	Other
☐	☐	☐	☐

Comments:

Current Security Advisories

Source: Best of Security Mailing List

Windows NT SNMP agent exploits.

This first exploit demonstrates the ability via SNMP to dump a list of all usernames in an NT domain (assuming the target box is a Domain Contoller) or on an NT Server.

“snmputil walk victim.com.au public .1.3.6.1.4.1.77.1.2.25” is the attack.

The second exploit permits the attacker, via SNMP, to delete all of the records in a WINS database remotely, bypassing all NT security. Knowledge of SNMP community strings would allow an attacker to effectively shut down any large NT infrastructure.

The only suggested solution is to deny access to the SNMP port, either by a firewall or by removing the agent.

The Latest in Denial of Service Attacks: “Smurfing”.

Description:

The "smurf" attack, named after its exploit program, is the most recent in the category of network-level attacks against hosts. A perpetrator sends a large amount of “Ping” traffic broadcast to a third party’s ‘C’ class address, all of it having a false source address of the victim machine. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast, then most hosts on the third party IP network will take the ping request and reply to it with a ping reply, multiplying the traffic by the number of hosts responding. On a large network, there could potentially be hundreds of machines replying to each packet. All these ping replies arrive at the target machine, overloading it.