Techniques used for bypassing firewall systems

presented by

Adam Gowdiak

POL34CERT
COMPUTER SECURITY INCIDENTS RESPONSE TEAM OF POL34 NATIONAL NETWORK

9th TF-CSIRT Meeting, 29-30th May 2003, Warsaw
About POL34-CERT

Who we are?

- POL34-CERT is part of Poznan Supercomputing and Networking Center, the operator of the Polish Scientific Broadband Network POL34/155
- It has been established in 2000 to provide effective incident response service to members and users of the POL34/155 network
- The primary goal was to provide active incident handling with high quality technical support which can be guaranteed by seven years of experience acquired by the Security Team of PSNC
About POL34-CERT

Mission statement

- An adequate technical support while handling security incidents and recovering from their consequences
- Complex co-ordination of all responses to an incident with special emphasis on exchanging information between various interested parties
- Valuable educational materials aimed at increasing the awareness of security as well as improving the overall knowledge of security techniques among the members of the constituency
About POL34-CERT
Constituency

The declared constituency of POL34-CERT contains all those systems connected to POL34/155 network i.e. networks of most academic and scientific institutions in Poland.
PSNC Security Team

Our experience

- Security administration of the POL34/155 network infrastructure and PSNC’s supercomputing resources
- Performing real-life, large scale penetration tests for third parties (both commercial and educational ones)
- Participation as security consultants in research projects founded by Polish Academy of Sciences and EC
- Extensive knowledge of attack methodologies and techniques
- Continuous security vulnerability research
Introduction

Presentation motivations

- Practical security is based both on knowledge about protection as well as about threats.
- If one wants to attack a computer system, he needs knowledge about its protection mechanisms and their possible limitations.
- If one wants to defend his system, he should be aware of attack techniques, their real capabilities and their possible impact.
Introduction

Presentation thesis

- The difficulty of securing a given network infrastructure goes along with its size and complexity
- Securing a network infrastructure is a continuous process, that should have its beginning in the design phase
- *Security is not a product, (Bruce Schneier)*
- Firewalls are not the end-all, be-all solution to information security
- You can never feel 100% secure...
Firewall systems
Introduction

- They got particularly popular around 1996 - the time where some new attack techniques emerged (*buffer overflows*, remote exploits)
- Their primary goal was to provide traffic control and monitoring
- They enforce the security policy represented by a set of rules, specifying what is explicitly permitted/denied
- They usually interconnect two or more logical networks - public and a private ones
Firewall systems
Evolution

Diagram:

A. Internet to corporate network

B. Internet to Bastion to corporate network

C. Internet to Bastion to demilitarised zone (DMZ) to corporate network
Firewall systems
Types and operation

Packet level filtering

Application level filtering
Firewall systems
State of the art

- They run as part of the OS kernel (KLM)
- They use some advanced algorithms for stateful traffic analysis (*Adaptive Security Analysis, Stateful Inspection*)
- They can hide information from the outside about the internal logic of the protected network (NAT, PAT, DNS Proxy)
- They can authenticate users with the use of different authentication methods (*SecureID*, RADIUS, AXENT, TACACS, Vasco, S/Key)
- They can do some limited content filtering (*Java*, ActiveX)
Firewall systems
State of the art (2)

- They can be extended by 3rd party products (OSPF)
- They can transparently proxy some common application services (FTP, telnet)
- They provide support for:
  - SNMP (Simple Network Management Protocol),
  - LDAP (Lightweight Directory Access Protocol),
  - ODBC (integration with relational databases),
  - X.509 (certificates exchange)
- They also include support for implementing VPN (DES, RC-4, MD5, SHA-1, SKIP, IPSec, IKE)
Firewall systems
State of the art (3)

They are able to analyze most of the common:

- applications protocols:
  - dns, echo, finger, ftp, irc, NetBeui, ras, rexec, rlogin, rsh, smb, snmp, syslog, telnet, tftp, time, uucp, X11, smtp, pop2, pop3, Microsoft Exchange, gopher, http, nntp, wais, egp, ggp, grp, ospf, rip

- multimedia protocols:
  - Cooltalk, Partners, CU-SeeMe, FreeTel, H.323, Internet Phone, NetMeeting, NetShow, RealAudio/Video, StreamWorks, Vosaic, Web Theater

- database protocols:
  - Cooltalk, Partners, CU-SeeMe, FreeTel, H.323, Internet Phone, NetMeeting, Lotus Notes, MS SQL Server, SQLNet* by Oracle, SQL Server by Sybase
Firewall systems
The risks

- They are pretty complex piece of software!!! (the Linux KLM binary of Checkpoint FW 1 NW is 1.2 MB bytes long)
- Commercial firewall systems are closed software, which means that no one has really put them under the glass in a search for security problems...
- Over the last couple of years there has been just several bugs found in them...
- Do you still believe they are bug free ??
Firewall systems
The risks (2)

- They just filter traffic coming from/to your network
- They can handle dozens of application protocols, but unfortunately cannot protect you against malicious content
- Security level of a network protected by a firewall system depends on many factors (DNS, routing infrastructure, security of client software...)
- There is always a great risk associated with the so-called „human error”
Introduction to attack techniques
The usual firewall deployment model
Introduction to attack techniques
The rules people usually forget about

- “The weakest point” rule - your network is as secure as its weakest point

- “The defense in depth” rule - the security of your network should not rely on the efficacy of a one and a given security mechanism

- “Choke points” rule - any security mechanism is completely useless if there exist a way to bypass it
Introduction to attack techniques
The myths people usually believe

- I am not going to be the target of a hack attack
- Even if so, attackers are not skilled enough to get into my network (NEVER, but NEVER UNDERESTIMATE YOUR OPPONENT)
- My 10k$ worth firewall system is unbeatable, I have put it at my front door and I am sure that it provides me with a high level of security

If you believe any of the above, sooner or later YOU WILL BE LOST!
Firewall attack techniques

Attackers goals

To be able to communicate with/access services of systems located in a corporate network.

To run code of attackers choice at some workstation/server located inside the attacked corporate network.
Firewall attack techniques

Attackers goals (2)

- Backward connection to attackers host through HTTP (port 80)
Firewall attack techniques
The past

- Packet fragmentation
- Source porting (can be still used occasionally)
- Source routing
- Vulnerabilities in TCP/IP stack
- FTP PASV related application proxy vulnerabilities (dynamic rules were created without properly assuring that the PASV response string was part of a legitimate FTP connection)
Firewall attack techniques
The present

- **Attacks through external systems**
  The goal: to use some trust relationship between the internal network’s systems and systems from the outside in order to get access to the internal network.

- **Attacks through content** (passive attacks)
  The goal: to provide user with a content that when dealt with (opened) will execute attacker’s provided code

- **Man in the middle attacks**
  The goal: to inject content into user traffic in such a way so that attack through content will occur
Firewall attack techniques

Attacks through external systems

Getting in through trusted external systems can be accomplished by first compromising the machines from which access to the internal network is permitted.

This might include:

- home machine of the workers of the company
- the network of the 3rd party that does remote administration/outsourcing for the attacked company
- the network of the company’s office in some other location/country
Firewall attack techniques
Attacks through external systems (2)

Getting in through non trusted external systems can be accomplished in several ways:

- throughout the exploitation of a vulnerability in a client software (SecureCRT, ftp, ...)
- by obtaining user credential information/other sensitive data from the user X screen grabbing
- throughout the combination of the above, Netscape /Mozilla remote control capabilities and a JVM vulnerability
Firewall attack techniques
Attacks through external systems (case study)

User works (SSH session, Xforward) with some external system
Firewall attack techniques
Attacks through external systems
(case study)

Intranet servers

Database servers

Corporate network

Demilitarised zone (DMZ)

Communication server

WWW

INTERNET

compromised system

Attacker steals user’s X-MIT-MAGIC-COOKIE
Firewall attack techniques
Attacks through external systems (case study)
Firewall attack techniques
Attacks through external systems (case study)

Attacker finds WindowID of the running Netscape 4.x/Mozilla process on user’s system
Firewall attack techniques
Attacks through external systems
(case study)

Attacker issues openURL() command to the found window
Firewall attack techniques
Attacks through external systems
(case study)

User’s web browser connects with the attacker’s WWW server

INTERNET

compromised system

Copyright @ 2003 Poznan Supercomputing and Networking Center, POL34-CERT
Firewall attack techniques
Attacks through external systems
(case study)

Attacker inserts malicious payload into the requested web page (Java applet)
Firewall attack techniques
Attacks through external systems
(case study)
Firewall attack techniques
Attacks through content

Sending mail to the victim user containing:
- an executable file
- Microsoft Office document exploiting the *macro bypass* vulnerability
- HTML mail body exploiting a flaw in Internet Explorer/Outlook Express or Netscape leading to the code execution

DEMONSTRATION
Firewall attack techniques

File formats vulnerable to the “infection”

There are many file formats used for holding text, graphics or multimedia data that can be used as a carrier of a malicious content.

EXE, COM, BAT, PS, PDF
DVB, DWG (AutoCad)
DOC, DOT, CNV, ASD (MS Word)
ADP, MDA, MDB, MDE, MDN, MDZ (MS Access)
MPP, MPT (MS Project)
MSG, OTM (MS Outlook)

CDR (Corel Draw)
SMM (AMI Pro)
XLS, XLB, XLT (MS Excel)
VSD (Visio)
PPT, PPS, POT (MS PowerPoint)
WPD, WPT (WordPerfect)
Firewall attack techniques
Attacks through content (2)

Hacking some highly popular WWW/FTP server and putting a *trojan horse* file on it

- software installation files (RealPlayer, Winamp, web browsers, ...)
- software for mobile phones
- screen savers
- „funny” content in an executable form

*Backdooring* source code of some very popular and critical Internet service (apache, bind, sendmail, ...)

Firewall attack techniques

*Man in the middle* attacks

You cannot look at the security of your network only from the LAN/firewall perspective.

There are also many other things you should take into account because they may influence the security of your network:

- DNS service
- Routing/security of routes
Firewall attack techniques

*Man in the middle* attacks

(case study)
Firewall attack techniques

*Man in the middle* attacks

(case study)

User enters `www.yahoo.com` address in his web browser.
Firewall attack techniques

*Man in the middle* attacks

(case study)

Web browser requests the name of www.yahoo.com from the corporate DNS server
Firewall attack techniques

*Man in the middle* attacks

(case study)
Firewall attack techniques

*Man in the middle* attacks

(case study)
Firewall attack techniques

*Man in the middle* attacks

(case study)
Firewall attack techniques

*Man in the middle* attacks

(case study)

Attacker inserts malicious payload into the requested web page (Java applet)
Firewall attack techniques

*Man in the middle* attacks

(case study)
Firewall attack techniques
DNS attacks are still the real threat

DNS can be quite successfully manipulated through the use of DNS spoofing ("birthday attack" in particular)
Firewall attack techniques
DNS attacks are still the real threat (2)

Although the CERT® Advisory CA-2002-31 from November 2002 (Multiple Vulnerabilities in BIND) was issued there are still many BIND servers that are vulnerable to the "cached SIG record" buffer overflow attack.

As of February 2003, there were more than 40% of them...

Why ?? Do we have such a situation because there was no official exploit code published for this issue ??

THE CODE FOR THIS ISSUE EXIST
Firewall attack techniques
Short digression

Which Web Browser is in your opinion the most secure?

Which one do you use:
- Internet Explorer
- Netscape
- Mozilla
- Opera
- any other?
Firewall attack techniques
Short digression (2)

This page contained information about not-yet disclosed security vulnerability.

Vendor has been provided with technical details of the bug on June 2nd 2003.

DEMONSTRATION
Firewall attack techniques

Final words

- Attacker needs to find only one weakness in your security infrastructure
- You are required to have none of them/all of them patched
- Your security depends on the security of many, many components...
- Skilled, motivated attackers are the real threat and they are really out there...
Finally
The End

Thank you for your attention!

adam.gowdiak@man.poznan.pl

Poznan Supercomputing and Networking Center
http://www.man.poznan.pl

CERT-POL34
http://cert.pol34.pl