



Windows Security Analysis
Computer Science E-Commerce Security '2005'

Matthew Cook

<http://escarpment.net/>

Introduction

Senior IT Security Specialist

Loughborough University

<http://www.lboro.ac.uk/computing/>

Windows Security Analysis



- Introduction
- Step-by-step Machine Compromise
- Preventing Attack
- Incident Response
- Further Reading



Introduction

Basic Security Overview

Physical Security



- Secure Location
- BIOS restrictions
- Password Protection
- Boot Devices
- Case Locks
- Case Panels

Why bother?

Why bother?

- Keeping control and service availability
- Spreading infection
- Data Integrity (DPA)
- Legal Liability
- Reactive Work Loads
- Bad Public Relations
- Personal Responsibility

Why bother?

- Computing has changed...
- Ten years ago the Internet was very small, few connections, mainly dialup users.
- JANET connected UK Universities from the early 90s.
- ISDN links at 64Kb/sec for industry.
- Advent of broadband brings many, many more users on a fast connection.

The Easiest Security Improvement

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about your chosen password. This leaves them no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation.

The Easiest Security Improvement

- Do not use your login name in any form
- Do not use your first or last name
- Do not use your spouse's or child's name
- Do not use your Car Registration etc.
- Do not use a dictionary based password
- Do not use a password shorter than 8 chars
- Do not write it on 'post-it' notes

The Easiest Security Improvement

- Use a password with mixed-case characters
- Use a password with a mix of alpha- numerics and punctuation
- Use a password that is easy to type to avoid ‘Shoulder Surfers’
- Use the first letters from song titles, song lyrics or film quotations



Step-by-step Machine Compromise

Why, where, how?

Background

Reasons for Attack:

- Personal Attacks
- Information theft and modification
- Experimentation
- Bandwidth theft
- DoS Botnets
- Warez servers
- Distribute Viruses, Worms and Trojans

Gathering Information

- Companies House
- Internet Search
URL: <http://www.google.co.uk>
- Whois
URL: <http://www.netsol.com/cgi-bin/whois/whois>
- A Whois query can provide:
 - The Registrant
 - The Domain Names Registered
 - The Administrative, Technical and Billing Contact
 - Record updated and created date stamps
 - DNS Servers for the Domain

Gathering Information...

- Use Nslookup or dig
- dig @<dns server> <machine address>
- Different query type available:
 - A – Network address
 - Any – All or Any Information available
 - Mx – Mail exchange records
 - Soa – Zone of Authority
 - Hinfo – Host information
 - Axfr – Zone Transfer
 - Txt – Additional strings

Identifying System Weakness



Many products available:

- Nmap
- Nessus
- L0pht Crack

Nmap

- Port Scanning Tool
- Stealth scanning, OS Fingerprinting
- Open Source
- Runs under Unix based OS
- Port development for Win32
- URL: <http://www.insure.org/nmap/>

Nmap

```
ccmsc@escarpment.lut.ac.uk: /home/ccmsc
Password:
[root@escarpment ccmsc]# nmap -sS -O -p1-65535 gemini

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on gemini.lut.ac.uk (131.231.82.218):
(The 65526 ports scanned but not shown below are in state: closed)
Port      State      Service
135/tcp   open      loc-srv
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
1025/tcp  open      listen
1026/tcp  open      nterm
1029/tcp  open      unknown
3306/tcp  open      mysql
3372/tcp  open      unknown
3389/tcp  open      msrdp

Remote OS guesses: Windows Me or Windows 2000 RC1 through final release, MS Wind
ows2000 Professional RC1/W2K Advance Server Beta3, Windows Millenium Edition v4.
90.3000

Nmap run completed -- 1 IP address (1 host up) scanned in 32 seconds
[root@escarpment ccmsc]#
[root@escarpment ccmsc]#
```

Nessus



- Remote security scanner
- Very comprehensive
- Frequently updated modules
- Testing of DoS attacks
- Open Source
- Win32 and Java Client
- URL: <http://nessus.org/>

L0pht Crack

- Password Auditing and Recovery
- Crack Passwords from many sources
- Registration from \$249
- URL: <http://www.atstake.com/>

L0pht Crack



Crack Passwords from:

- Local Machine
- Remote Machine
- SAM File
- SMB Sniffer
- PWDump file

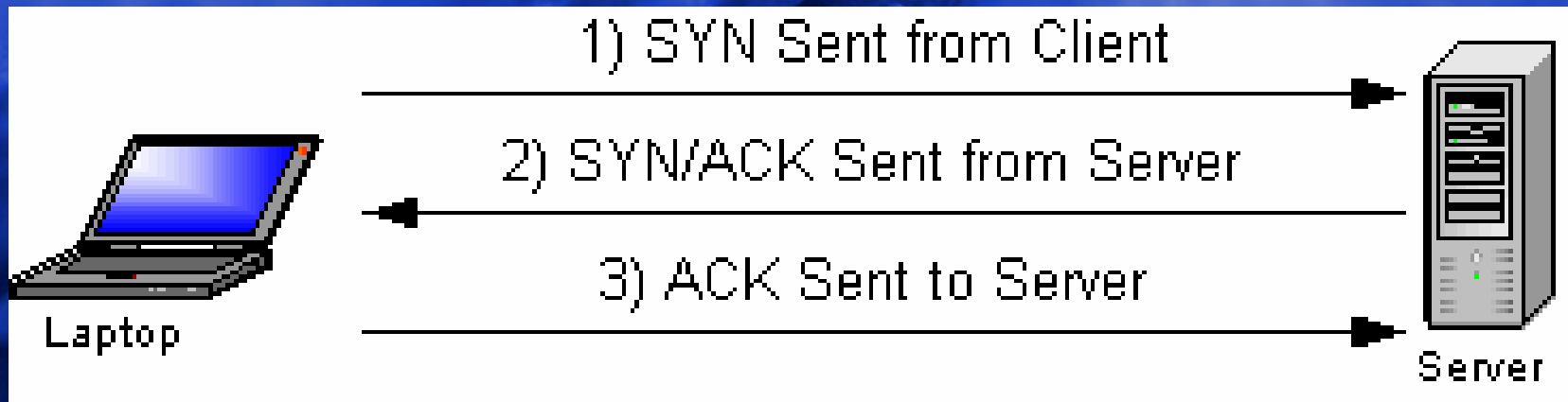
Nmap Analysis

- `nmap -sP 158.125.0.0/16`
 - Ping scan!

- `nmap -sS 158.125.0.0/16`
 - Stealth scan

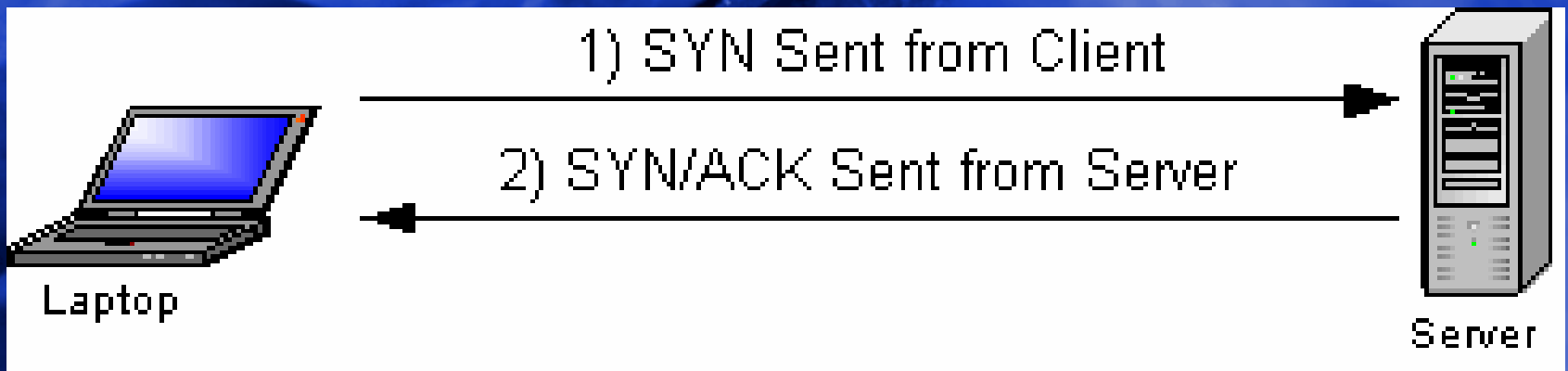
Nmap Analysis...

- TCP Connect Scan
- Completes a 'Three Way Handshake'
- Very noisy (Detection by IDS)



Nmap Analysis...

- TCP SYN Scan
- Half open scanning (Full port TCP connection not made)
- Less noisy than the TCP Connect Scan



Nmap Analysis...

- TCP FIN Scan
 - FIN Packet sent to target port
 - RST returned for all closed ports
 - Mostly works UNIX based TCP/IP Stacks
- TCP Xmas Tree Scan
 - Sends a FIN, URG and PUSH packet
 - RST returned for all closed ports
- TCP Null Scan
 - Turns off all flags
 - RST returned for all closed ports
- UDP Scan
 - UDP Packet sent to target port
 - “ICMP Port Unreachable” for closed ports

Exploiting the Security Hole

Common Fingerprints:

- Directory Traversal

`http://host/cgi-bin/lame.cgi?file=../../../../etc/motd`

- Unicode Requests

`http://host/cgi-bin/lame.cgi?page=dir%20/a`

`http://host/cgi-bin/lame.cgi?page=../etc/motd%00html`

- Redirection Requests

`http://host/cgi-bin/lame.cgi?page=echo"733t">../msg.html`

`http://host/something.php=Hi%20I'm%20Bold!`

Backdoor Access

- Create several user accounts
- Net user iisservice <pass> /ADD
- Net localgroup administrators iisservice /ADD
- Add root shells on high end ports
- Tiri is 3Kb in size
- Add backdoors to 'Run' registry keys

System Alteration



- Web page alteration
- Information Theft
- Enable services
- Add VNC

- Creating a Warez Server
- Net start msftpsvc
- Check access
- Upload file 1Mb in size, then 10Mb, then 100Mb
- Advertise as a warez server

Audit Trail Removal

- Many machines have auditing disabled
- Main problems are IIS logs
- DoS IIS before logs sync to disc
- Erase logs from hard disc
- Erasing Eventlog harder

- IDS Systems
- Network Monitoring at firewall

Preventing Attack

How to stop the attack from happening and how to limit the damage from crackers!

NetBIOS/SMB Services

- NetBIOS Browsing Request [UDP 137]
- NetBIOS Browsing Response [UDP 138]
- NetBIOS Communications [TCP 135]
- CIFS [TCP 139, 445 UDP 445]
- Port 445 Windows 2000 only
- Block ports at firewall
- Netstat -A

Windows Updates

- Automatic Updates
 - My Computer > Select Properties > Select Automatic Updates tab.
 - We do NOT recommend Automatic or Turning Automatic Updates off.
 - Either; Download updates for me, but let me choose when to install them.
 - OR Notify me but don't automatically download or install them.

Baseline Security Analyser



- Microsoft Baseline Security Analyser
- Freely available from Microsoft
- Provides advice on
 - Security best practices
 - Strong passwords
 - Security mis-configurations
 - Application configurations

Operating System Patching

- Operating Systems do contain bugs, and patches are a common method of distributing these fixes.
- A patch or hot fix usually contains a fix for one discovered bug.
- Service packs contain multiple patches or hotfixes. There are well over 200 hot fixes in most service packs.

Operating System Patching...

- Its not just the Operating System!
 - Software needs patching too
 - Lots of vulnerabilities are discovered in software.
 - MS Office, GDI+ JPEG Module, IIS, MS SQL, Oracle etc

Incident Response

What to do when something does
go wrong!

Incident Response...

- Don't Panic!
- Unplug the network
- Get a notebook
- Back-up the system and keep the Back-ups
- Restrict use of email
- Look for information
- Investigate the cause

- Request help and assistance.

Incident Response...

- Important to return to service swiftly
 - Do not jeopardize security
 - If in doubt, re-build
 - Perform forensics on a backup
- Keep documentation and evidence
- Contact local CERT if investigation proves non worm/script kiddie activity.

Further Reading

- Garfinkel, S. *Web Security & Commerce* *O'Reilly* [ISBN 1-56592-269-7]
- Hassler, V. *Security Fundamentals for E-Commerce* *Artech House* [ISBN 1-58053-108-3]
- Huth, M R A. *Secure Communicating Systems* *Cambridge Uni Press* [ISBN 0-52180-731-X]
- Schneier, B. *Secrets & Lies (Digital Security in a Networked World)* [ISBN 0-47125-311-1]

Useful Books, Tools and URLs

- Securing Windows NT/2000 Servers for the Internet. (Stefan Norberg.)
- Incident Response. (Kenneth R. van Wyk, Richard Forno.)
- Hacking Exposed: Network Security Secrets & Solutions. (Stuart McClure et al)
- Hacking Exposed Windows 2000: Network Security Secrets and Solutions. (Scambray.)

Useful Books, Tools and URLs

- Microsoft Security Website
<http://www.microsoft.com/security/>
- Computer Security Incident Response Team
http://www.cert.org/csirts/csirt_faq.html
- JANET CERT
<http://www.ja.net/cert/>
- Computing Services – Security Service
<http://www.lboro.ac.uk/computing/security>

Questions

Slides available at:
<http://escarpment.net/>