Protecting Your Business Online

David Papp, P.Eng.
CISA, CISSP, CWNA, MCSE, CCDA, CCNP

Last Modified
20 minutes ago ☺

The Business Link

April 27, 2004

A bit of history

The Rogue Gallery of Hackers…

Rogue Gallery of Hackers

- CIRCA 1971
  - John Draper, a Vietnam vet, discovers that a Cap'n Crunch whistle produces a tone activating AT&T's free calling.
- CIRCA 1983
  - A Milwaukee hacking group called the 414's break into computers at Los Alamos Labs and the Memorial Sloan-Kettering Cancer Center.

Rogue Gallery of Hackers

- 1984
  - The Legion of Doom (LOD) hacking group formed by "Lex Luthor" targets telecommunications companies and 911 emergency telephone services.
- 1988
  - Student Robert Morris unleashes a worm on the Internet that crashes 6,000 computers. Morris becomes the first person convicted under the US Computer Fraud and Abuse Act.

Rogue Gallery of Hackers

- 1990
  - Kevin Poulsen takes over all the phone lines going into KIIS-FM in Los Angeles to guarentee that he'd be the 102nd caller and win a Porsche. Poulsen is later convicted.
- 1992
  - Four members of MOD are convicted of various computer crimes, Phiber Optik, a.k.a. Mark Abene, is sentenced to a year in prison.

Rogue Gallery of Hackers

- 1994
  - Russian mathematician Vladimir Levin leads a break-in of Citibank computers to steal $10 million. All but $400,000 was recovered and Levin was later arrested.
- 1995
  - Kevin Mitnick, also known as Condor, is arrested again, this time for illegal use of stolen cellular telephone numbers. He spends five years in jail.

Rogue Gallery of Hackers

- 1988
  - Kevin Mitnick is arrested and convicted. At the time, Mitnick had broken into Digital Equipment Corp.'s computer systems.
- 1990
  - The "Great Hacker War" begins as LOD and Masters of Deception (MOD) cyberwar jams many phone lines and results in multiple break-ins of computers.

Rogue Gallery of Hackers

- 1999
  - The Melissa Virus is released by David L. Smith. It replicates by sending itself to people listed in the victim's address books.
- 2000
  - DDoS attacks all but shut down Web sites, including Amazon, CNN, eBay, and Yahoo. A recorded online chat session later fingers a Montreal teenage hacker.

Rogue Gallery of Hackers

- 2000
  - A variant of Melissa called the Love bug or ILoveYou virus is traced to a Phillipine computer science student. The estimated damage caused by the virus: $6.7 billion.
- 2000
  - Wireless phones in Europe are targeted by a cell phone virus called Timofonica, signalling what may be a new capability for hackers.

Recently

Today we have a proliferation of email spam, viruses, and many more computer users & devices connected to the Internet.

Anatomy of a “Hack”

(Basis for Network Security Audits)

1) Footprinting
2) Scanning
3) Enumeration
4) Gaining Access
5) Escalating Privilege
6) Pilfering
7) Covering Tracks
8) Creating Back Doors
9) Denial of Service

Categorizing Security

- Exploits
  - Audits, penetration tests
- Methodologies
  - Certifications, documentation/reports, experience
- Countermeasures
  - Firewalls, VPNs, Encryption, Disaster Recovery Plans

Email Headers

- Outlook (right click on email subject line in Inbox, then Options, then read the Internet Headers)
- Read from bottom up
- Excellent information about reading email headers at

  http: / / www.stopspam.org / email / headers / headers.html

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com [22.22.22.22]) by
mailhost.company.com (8.8.5/8.7.2) with ESMTP id LAA20869
for ; Tue, 18 Mar 2003 14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-host.isp.com
[11.11.11.11]) by mail.isp.com (8.8.5) id 004A21; Tue, Mar
18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003
14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5)
id 004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003
14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5)
id 004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Sample Email Header

```
Received: from mail.isp.com (mail.isp.com
[22.22.22.22]) by mailhost.company.com (8.8.5/8.7.2)
with ESMTP id LAA20869 for ; Tue, 18 Mar 2003
14:39:24 -0800 (PST)
Received: from mycomputername.bogus.com (ip-
host.isp.com [11.11.11.11]) by mail.isp.com (8.8.5)
id 004A21; Tue, Mar 18 2003 14:36:17 -0800 (PST)
From: jane.doe@isp.com (Jane Doe)
To: someperson@company.com
Date: Tue, Mar 18 2003 14:36:14 PST
Message-Id: <rth031897143614-00000298@mail.isp.com>
X-Mailer: Loris v2.32
Subject: Lunch today?
```

Whois

- Domain Names and IP Addresses
- www.abc.com = hostname
- abc.com = domain name
- 216.239.57.99 = IP Address (www.arin.net)
  - www.samspade.org
  - www.network-tools.com
    (goto www.network-tools.com/help/ for good info)

Worms

- August 2003 - **Blaster** worm
  - *300,000 to 350,000 infected*
- January 2003 – **Slammer** worm
  - *200,000 to 250,000 infected*
- September 2001 – **Nimda** worm
  - *150,000 to 200,000 infected*
- July 2001 – **Code Red** worm
  - *350,000 to 400,000 infected*

Blaster Worm

- Software patch to prevent Blaster was out more than 1 month before the worm struck.

Slammer Worm

-Fastest computer worm in history. As it began spreading, it DOUBLED IN SIZE EVERY 8.5 SECONDS!

-It achieved full scanning rate of over 55 million scans per second after only 3 minutes.

-It infected more than 90% of vulnerable hosts within 10 minutes. Code Red was 14 hours.

-Two orders of magnitude faster than Code Red which has a “leisurely” doubling time of 37 minutes.

-Slammer was so aggressive that it quickly interfered with its own growth due to completely using up all the bandwidth of many Internet connections.

-The weakness was discovered and a patch was released on July 24/02. The worm broke out Jan25/03, 6 months later!!

Why?

- Lack of people applying Microsoft updates
- Lack of AntiVirus software present
- Lack of updating AntiVirus definitions
- Lack of firewalls in place

- Your computer is not a “toaster”. You cannot just plug it in and take it for granted that it works. Regular maintenance must be performed. Just like a car with oil & filter changes, break pads, etc.

Trivia

There is no industry standard for an acceptable number of bugs, but a sometimes-quoted figure is one bug per 10,000 lines of code – a lot of bugs when you consider than Windows 2000 reportedly contains some 40 million lines of code. XP has even more…

Protect You and Your Computer

(see handout)

- Apply Windows and Office Updates
- Software firewall
- Hardware firewall
- AntiVirus
- Encryption
- VPN
- Passwords
- Backups
- Surge Protection, UPS
- Destroy deleted files
- Wipe hard drives
- Protect Internet privacy
- Spyware blocker
- Spam blocker
- Be skeptical

Wireless Network Security

(see handout)

- Select appropriate hardware
- Manage SSIDs
- Change default usernames and passwords
- Use large WEP keys
- Provide VPN service
- Require user authentication
- Filter by MAC address and/or IP address
- Secure the wireless clients

Trivia

Average Time for Exhaustive Key Search

At 1,000,000 encryptions per second:

32-bit key length requires ~ 2 milliseconds
56-bit key length requires ~ 10 hours
128-bit key length requires
~5,000,000,000,000,000,000 years

Trivia

- The American Dialect Society voted the verb Google the “most useful” word for 2002.
- The term itself is a play on googol – same pronunciation – which is the number 1 followed by 100 zeroes. It was coined in 1938 by nine-year-old Milton Sirotta, after his uncle, mathematician Edward Kasner, asked him for a word to describe a really big number. ☺

Security Certifications

- **CISSP** – Certified Information Systems Security Professional, www.isc2.org
- **SSCP** – Systems Security Certified Practitioner, www.isc2.org
- **CISA** – Certified Information Systems Auditor, www.isaca.org
- **CPP** – Certified Protection Professional, www.asisonline.org
- **GIAC** – Global Information Assurance Certification, www.giac.org
- **Security Certified Program** – www.securitycertified.net
- **Cisco certifications** – www.cisco.com
- **Microsoft certifications** – www.microsoft.com

Questions to ask a security consultant

- Is this your day job?
- How long have you been doing this?
- What certifications/training do you have?
- Do you or any of your staff have a criminal record?
- Do you have any ties or associations with a particular vendor?
- Do you offer any guarantees?
- Do you offer support for emergency situations?
- Do you have any references or a client list?

Relevant Websites

- www.grc.com
- www.infosecnews.com
- slashdot.org
- www.securityfocus.com
- www.antionline.com
- www.google.com
- www.cert.org
- www.sans.org
- www.ciac.org
- www.cerias.purdue.edu /hotlist
- www.cnet.com
- www.secinf.net
- www.operationsecurity.com

Show and Tell

- Linksys
- iButton
- USB Flash
- USB / Parallel Key
- SecurID Token
- Cryptocard
- KeyGhost

Q & A

David Papp
david@remote.net
780.951.4869