



Protecting your Windows Web Infrastructure

Daniel Dorr

Hewlett Packard

Internet Security Division



Agenda

- review of threats
 - example violations
 - tools available
 - overall issues
- review of protection
 - best practices
 - tools available
- conclusion



The Customer Problem

Recent targets:

HP

Microsoft

CD Universe

Yahoo

Amazon.com

Nasdaq.com

New York

Times

Western Union

March 8, 2001 — The federal government's central computer-crime bureau reported today that **there is an ongoing and organized series of hacker attacks against e-commerce Web sites** that has resulted in the theft of more than 1 million individual credit card numbers.

—*By Dennis Fisher, EWEEK*



Attack Examples

- **#EXEC Exploit**

Risk of an intruder causing a DOS and stealing company's valuable information as a result of a random and potentially malicious attack via #EXEC command on CGI scripts and ASP/ISAPI applications

- **Script Debugging Exploits**

Risk of an intruder extracting from client/server debugging scripts vital information such as directory names, user names and passwords

- **.asa (or .asp, .ini, etc.) file Exploit**

Microsoft IIS 4.0 and 5.0 can be made to disclose fragments of source code that should otherwise be inaccessible



Example Windows Exposure

May 1, 2001 - MS races to fill in serious security hole

The announcement of the vulnerability comes at a bad time, as Chinese and American online vandals have apparently started cooperating for a weeklong string of attacks on government and corporate servers to protest the actions of each other's governments.



Largest Credit Card Theft

MSNBC - March 17, 2000

“In the largest known case of cybertheft, a computer intruder stole information on more than **485,000** credit cards from an e-commerce site...”

- Site was an NT web server
- Had not been updated in 2 years

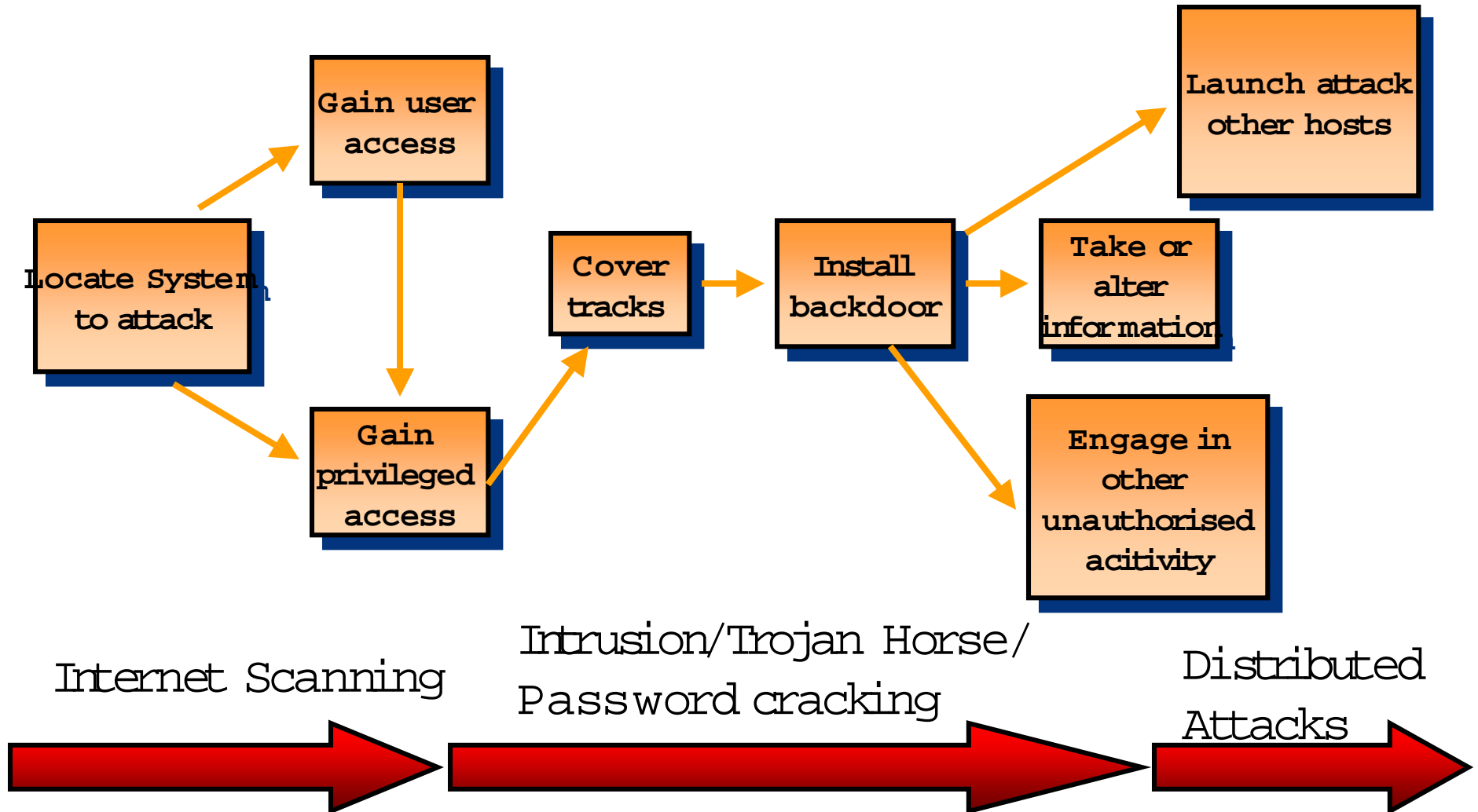


“Hacker puts Nasdaq on warning”

- Hacker found holes in finance web site security
 - Nasdaq.com
 - CBS.MarketWatch.com
 - BigCharts.com
 - FTMarketWatch.com
- Known security hole for 3 months
 - .asa (or .asp, .ini, etc.) file, Microsoft IIS 4.0 and 5.0 can be made to disclose fragments of source code that should otherwise be inaccessible
 - Got administrative password and used to take over web server



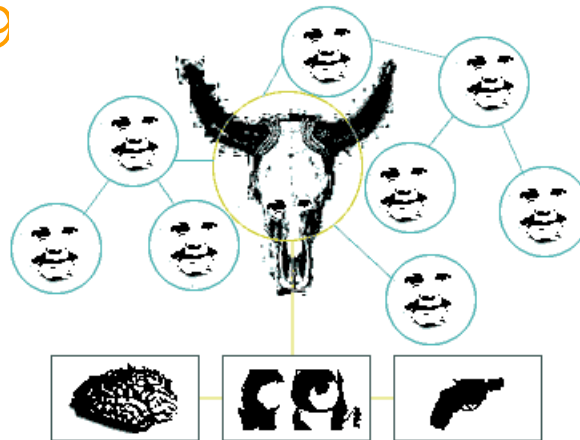
Typical Internet Attack





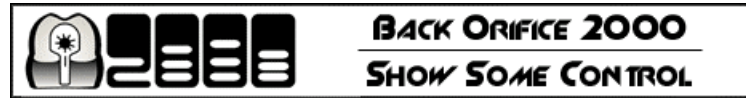
Back Orifice 2000

- Back Orifice originally came out in August 1998 by Cult of the Dead Cow (cDc)
- B02K (Back Orifice 2000) introduced in July 19





Back Orifice 2000



- Allows for remote control of Windows 95/98/NT/2000 machines across network
- Open Source
- Server installed on victim's machine
- Client runs on attacker's machine
- Very compact code – 200K for server and 500K for client



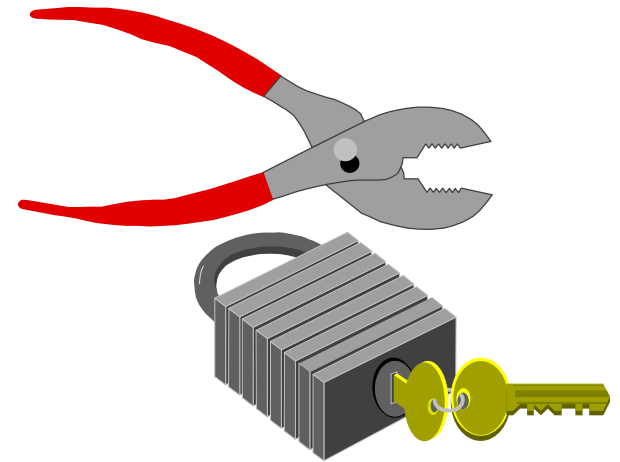
BO2K Capabilities

- System Control
- Gather passwords cached by user
- File System Control
- Process Control
- Registry Control
- Network Control
- and more...



Password Cracking

- Brute Force Attack
- *Crack, John the Ripper* for UNIX
- *L0phtCrack* for NT
- Commercial password cracking utilities available for ZIP, Word, Excel, Access!





L0phtCrack 2.5

- Doesn't have to run on the target host
- Guess the password based on
 - user id and name variations
 - dictionary entries (supply your own or download)
 - brute force (try every possible combination)
- Integrated sniffer for SMB authentication
- Crack all alphanumeric passwords in 24 hours with 450MHz Pentium II



Organization Security Issues


FBI / DOJ issue list of worst Internet threats

1. Opening unsolicited e-mail attachments without verifying their source or checking their content
2. Failing to install security patches
3. Assigning untrained people to maintain security;
4. Failing to see the consequences of poor security;
5. Failing to make fixes or follow up on them;
6. Relying primarily on a firewall for security;
7. Failing to realize how much money their "information and organizational reputations are worth";
8. Authorizing short-term fixes and pretending that problems will go away if they are ignored.



IT Security Issues

FBI / DOJ issue list of worst Internet threats

1. Connect systems to the Internet before hardening them
2. Connect test systems to the Internet with default accounts or passwords
3. Fail to update systems when security holes are found
4. Use Telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKIs (public key infrastructures)
5. Give out passwords to users over the phone or change passwords without verifying the legitimacy of the request
6. Fail to maintain and test backups
7. Implement firewalls that do not stop malicious or dangerous traffic
8. Fail to educate users about security problems
9.  Untrained users responsible for securing important systems



Security Study Findings Overview

- "A few software vulnerabilities account for the majority of successful attacks..."
 - Attackers are opportunistic-taking the easiest and most convenient route
 - Attackers count on organizations not fixing the problems
 - Attack indiscriminately by scanning the Internet for vulnerable systems
- System administrators typically say they are too busy
 - They do not know which of more than 500 potential problems are the most dangerous





Security is Insurance – WRONG!

- In a recent FBI survey of US businesses...
 - **85 % experienced security breaches** in the last 12 months
 - **64 % suffered losses** as a result
 - **lost \$377.8 million** (up from \$265.5 million last year)
 - 70 % identified Internet-connected systems as a frequent target of attacks



Out of the box security holes

- Insecure IIS samples
- Unnecessary services enabled
 - Indexing Service
 - Telnet
 - Net Meeting Remote Desktop Sharing
 - Internet printing
- Unnecessary network shares
 - ADMIN\$, C\$, etc.
- NetBIOS Over TCP/IP
- Vulnerable versions of MDAC installed
- Weak default permissions on files, folders, and registry entries



Security 101: Policies

- Set organizational security policies
- Audit the system to understand the current security settings
- Lock down system to meet with security policy
- Continually audit system to ensure consistency with policies



Example Policies

- Least privilege enforced
- Obscure resources
- Protect customer data from Internet access
- Define user policies
 - user names, password changes, education
- All new deployments must have corp. security review
- Define regular audit policies

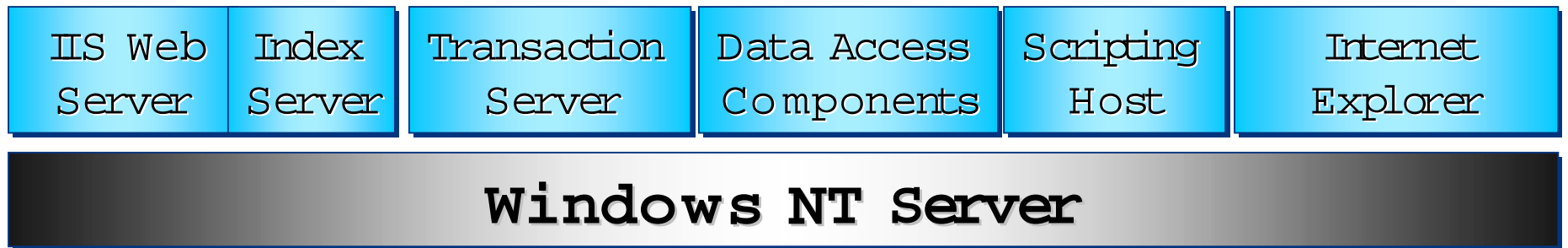
FYI – this can all be automated



Windows Web Server Environment

It all needs protection!

Typical IIS Web Server Environment



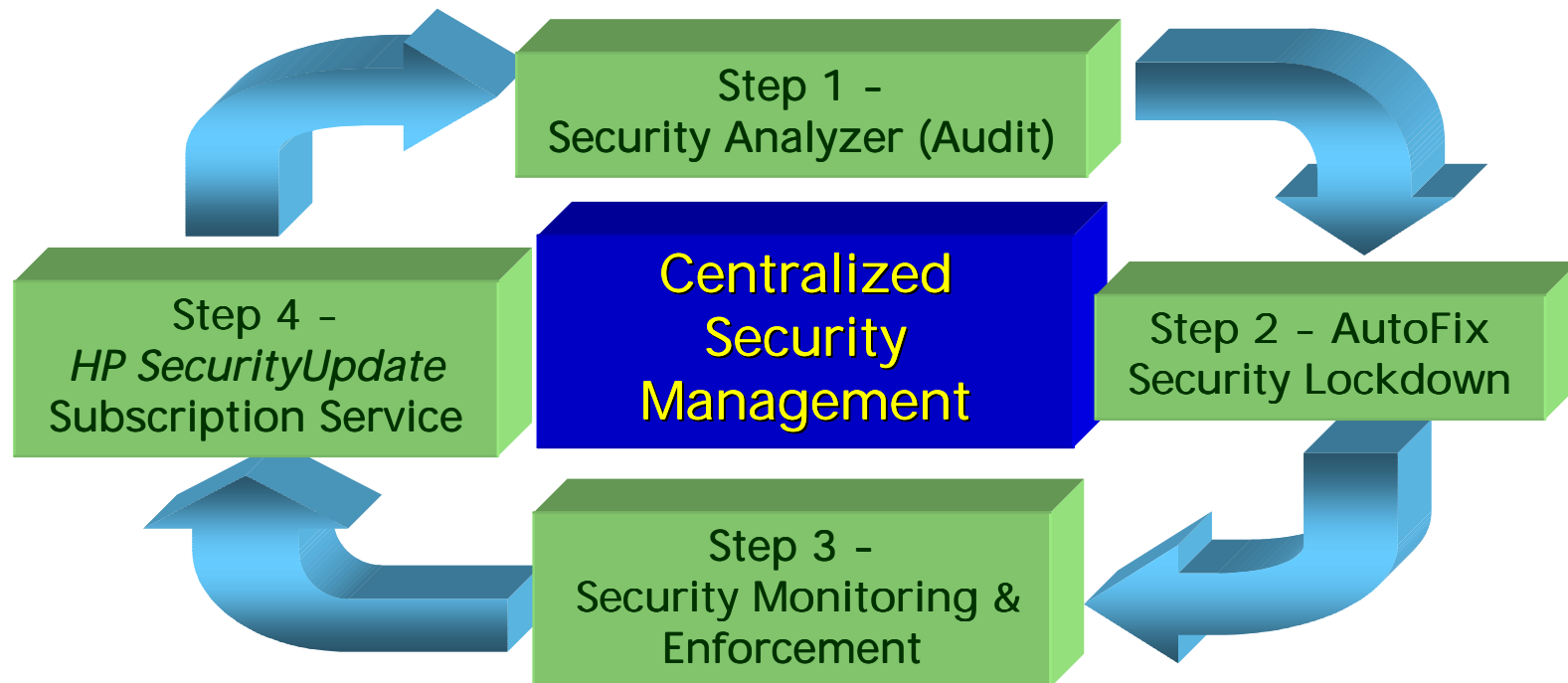
HP Webenforcer

Secure Web Server Environment

The safest place for deploying Windows NT Web-server applications

Secure your NT infrastructure

- Weeks of security consulting in a simple software solution
- Automatic, secure configuration of NT systems ensuring lower total cost of ownership
- Constant security updates ensure continual security without the need for personal vigilance





Product Features

- System scanning
 - Pre-defined and Custom Security Profiles
- Automated enforcement
 - Fix all or just specific problems
 - Immediately roll-back to last configuration
- Constant security monitoring
 - Flexible Time Increments
 - Alerts & Event Logging
- Ensure security over time
 - *SecureUpdate* Subscription Service



Web Enforcer Management

Intuitive
Windows "look
& feel" GUI

The screenshot shows the HPLDLockdown console interface. The left pane displays a tree view of the security profile structure, including folders for NT Security Lockdown Administration, Security Profile for the Mercury Web Server, BackOffice, Transaction Server, Index Server, Data Access Components, system32, IE, IIS, Application Security, Access Control, Web Server Security, Installed Software, Windows NT, Access Control, Workstation Lockdown, System Security, Installed Software, and Networking Security. The right pane shows a table of security rules:

Rule Name	Description
Enforce Administrative Security	Enforce Administrative Security
Secure the Web Application Manager Account	Secure the Web Application Manager Account

Below the table, there is an 'Overview' tab selected, showing a detailed description of the 'Secure the Web Application Manager Account' rule:

Overview:

Microsoft Transaction Server (MTS) provides a platform from which programmers can create three-tier server-centered (ASP and ISAPI) applications by making use of Component Object Model (COM) and Distributed Component Object Model (DCOM) technologies.

When an MTS package is created for an ASP or ISAPI application, its process identity is set to a special [Web Application Manager account](#) called IWAM_computername.

By default, IWAM_computername account has access to very few resources beyond

Detailed, easy-to-understand
description of each security rule





Webenforcer Security Report

WebEnforcer has found 60 classes of vulnerabilities in this Web Server environment.

Pass

Fail

!

i

Analyze Report

- Enable Logging
- Property 'Enable Logging' passed validation.
- Enable Warnings for Remote Browsing
- Enforce Administrative Security
- Establish Account Lockout Policy
- Establish Password Policies
 - Invalid, the password policy Password Age is 42, but it should be 62.
 - Invalid, the password policy Password Age is 0, but it should be 7.
 - Invalid, the password policy Maximum Password Length is 0, but it should be 8.
 - Invalid, the password policy Password Uniqueness is 0, but it should be 5.
 - Invalid, the password policy Password Length Minimum to log on to change password is not set, but it should be set.
- Force Pagefile to be Cleared
- Hide the Last User Name
- Obscure the Administrator Account
- Isolate ISAPI and ASP Applications
- Remove .REG Associations with Regedit
- Remove Network Shares
- Remove Password Change Interface
- Remove Password File from BackOffice Installation
- Valid, file Reboot.ini in this path Program Files\Microsoft BackOffice\Reboot.ini doesn't exist.

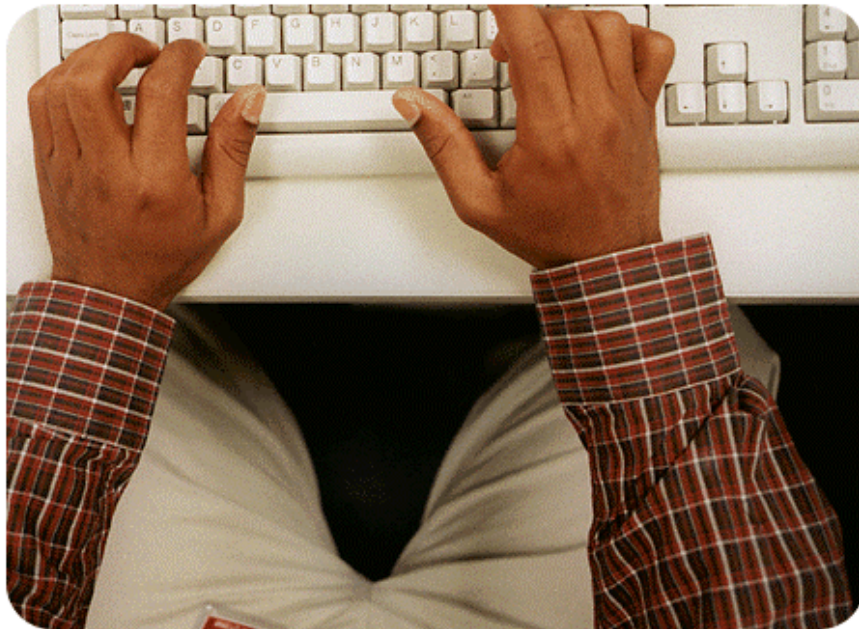
Fix Rule Fix All Rules Details... Print Report Delete Report Close Report

20 Vulnerabilities are critical to the system security.

Hackers
continue to
openly share
information



toward a secure
infrastructure ...



- create an always-on infrastructure that correctly executes business strategy
- e-tool security policies for next generation interactions
- develop worldwide accepted standards and definitions
- share information across the industry



Thank you

Daniel Dorr

daniel_dorr@hp.com

408-447-4682



Reference Web Sites

- www.hp.com/security
- www.cert.org
- www.securityportal.com
- www.securityfocus.com
- www.itsecurity.com
- www.gocsi.com
- www.antonline.com
- www.hackernews.com