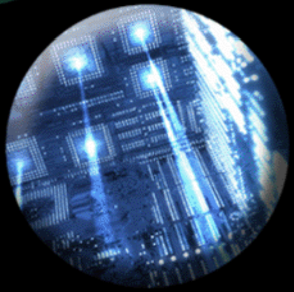
ManTech
International Corporation

The Convergence of
National Security and Technology

Secure Systems
and Infrastructure
Solutions


Information
Technology
Solutions

Systems
Engineering
Solutions

ManTech Security
& Mission Assurance

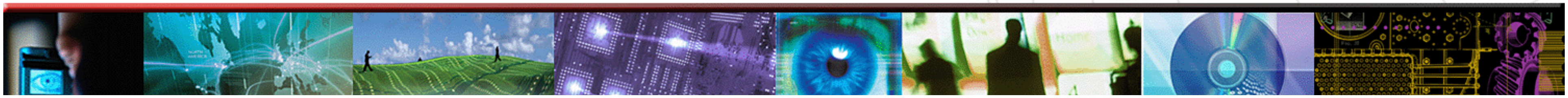
Computer Forensics & Intrusion Analysis Group

ManTech
International Corporation

Vulnerability Assessment & Penetration Testing

GREAT SEAL
LIBERTY AND UNION NOW AND FOREVER ONE AND INSEPARABLE
OCTOBER 1st 1889
STATE OF NORTH DAKOTA

Project Outbrief

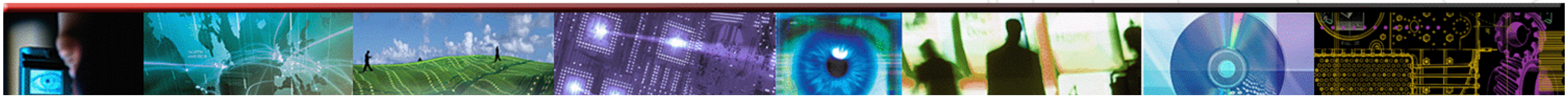


Introduction

- ManTech SMA Project Manager

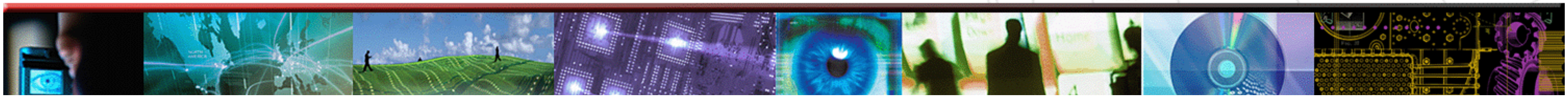
Mark Shaw
Principal Forensics and Intrusion Engineer
CFIA Cyber Defense Division
mark.shaw@mantech.com
(703)610-9326

CFIA
MANTECH SMA
COMPUTER FORENSICS & INTRUSION ANALYSIS



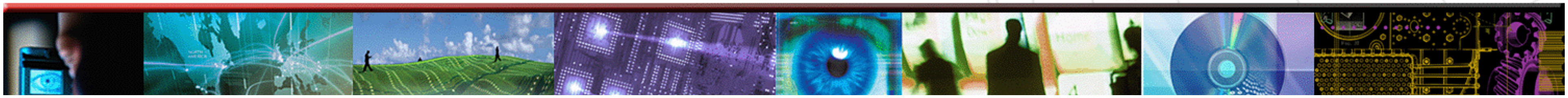
Project Overview

- Security Assessment conducted August-September 2007
- 4 Project Tasks
  - External Vulnerability Assessment
  - Internal Vulnerability Assessment
  - Penetration Test
  - Application Security Assessment



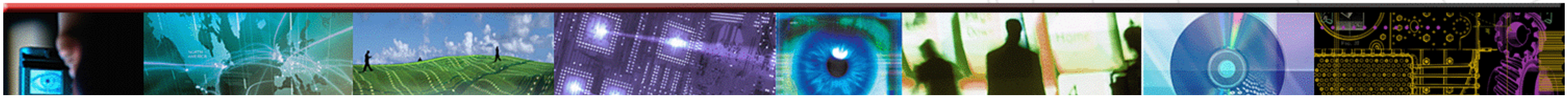
External Vulnerability Assessment-Overview

- **Conducted August 13-22 2007**
- **Passive Mapping**
  - **Internet searches**
    - **Personnel (emails, phone numbers, key personnel)**
    - **Documents**
    - **Network Assets**
    - **WHOIS & DNS queries**
  - **Open source research is virtually undetectable by target**
  - **Information gathered is available to anyone**



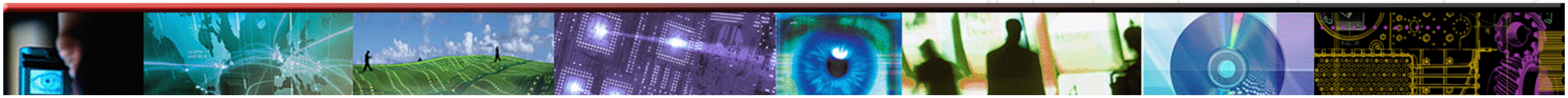
External Vulnerability Assessment-Overview

- Active Mapping
  - Port scanning
    - Identify available systems and services
  - Automated scanners and manual checks
    - Identify vulnerabilities



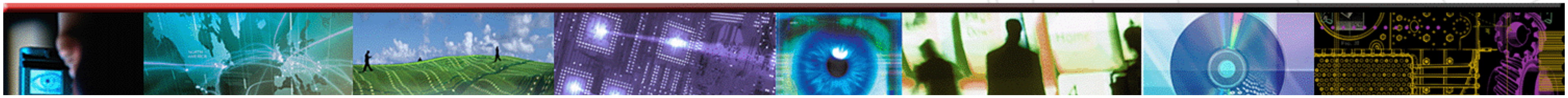
External Vulnerability Assessment-Results

- Vulnerability Findings
  - Great improvement over 2005 results
  - K12/EDU scanned but results not fully analyzed
  - 313 systems State Agencies or organizations found to have at least one vulnerability
  - 10 high risk/2 medium risk/4 low risk
  - Vulnerabilities could be classified as:
    - Missing OS or Application Patches
    - Architectural Design
    - Misconfigured Systems or Applications



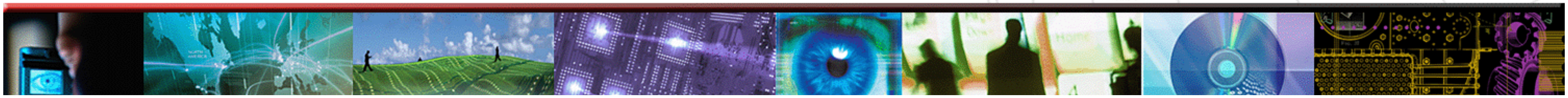
External Vulnerability Assessment-Results

- General Recommendations
  - Review Content Available on Publicly Accessible Servers
  - Filter Inbound Access to All State Systems
  - Ensure Segregation Between K12/EDU and State Networks



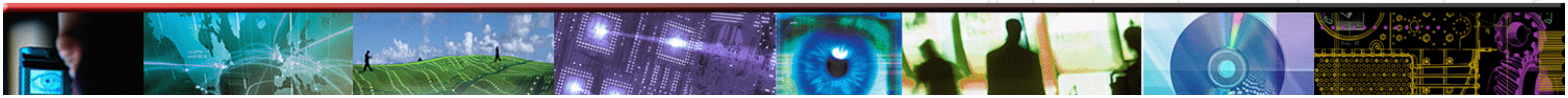
Internal Vulnerability Assessment-Overview

- Conducted August 27-September 5 2007
- Similar Methodology to External Assessment
- Identify vulnerabilities and security misconfigurations
- Automated scanners and manual checks
  - Identify risks to systems and data



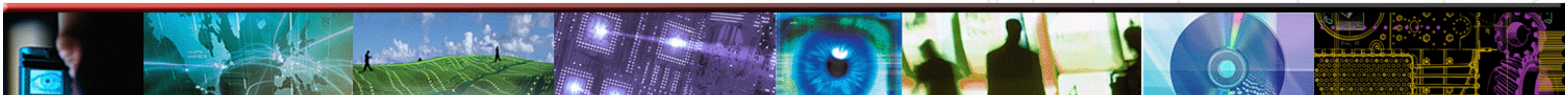
Internal Vulnerability Assessment- Results

- Vulnerability Findings
  - Great improvement over 2005 results
  - 427 systems at State Agencies or organizations found to have at least one vulnerability
  - 29 high risk/8 medium risk/4 low risk
  - Vulnerabilities could be classified as:
    - Missing OS or Application Patches
    - Architectural Design
    - Misconfigured Systems or Applications



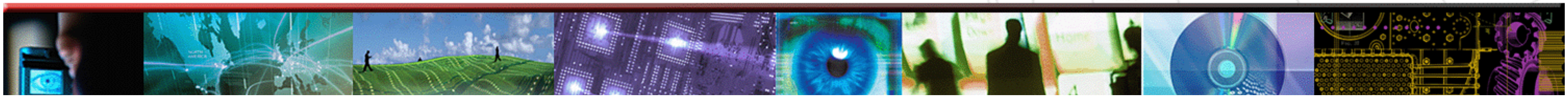
Internal Vulnerability Assessment- Results

- General Recommendations
  - Segment Public Facing Servers from Internal Network
  - Internal Segregation of Critical Servers and Development Systems
  - Include Applications in Formal Patch Management Program
  - Implement Outbound Access Control
  - Require use of Encrypted Protocols for Remote Management



Penetration Test- Overview

- Conducted September 5-10 2007
- Emulate realistic & current threats
  - Gain access to systems
    - Technical means & social engineering
- Exploit discovered vulnerabilities
  - Find legitimate vulnerabilities not identified by conventional methods
  - Fully Validate findings
- Test Response Procedures

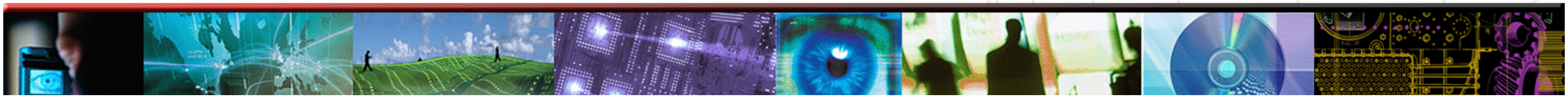


Penetration Test- Overview

- Social Engineering
  - Gain access to systems and/or information
  - Sensitize user population and administrators to hacker techniques
    - Phishing
    - Client-side exploits
    - Pretexting

Penetration Test- Results

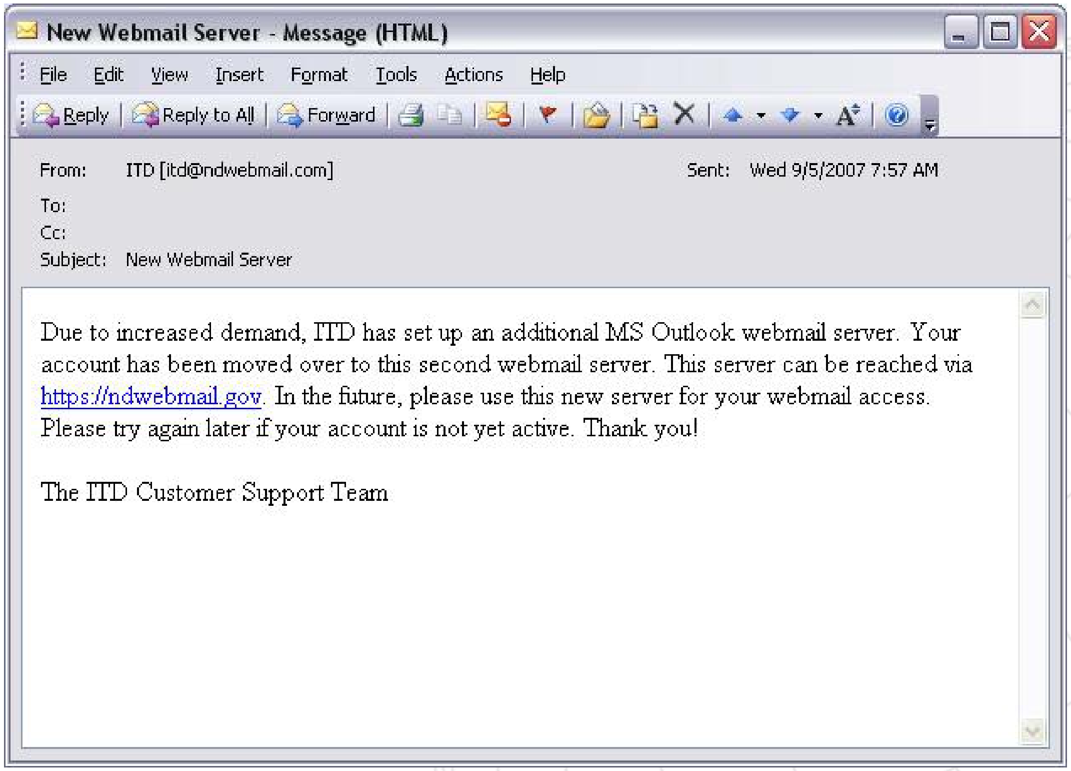
- Direct Exploitation
  - Identified 9 systems to target based on vulnerability assessment results
  - Unsuccessful in exploiting 8 of the systems
  - Successfully exploited one system and created an account with administrator privileges



Penetration Test- Results

Phishing email #1

- ndwebmail.com domain
- Sent ~110 emails from "ITD"
- Directs users to "new" web mail site


New Webmail Server - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply | Reply to All | Forward

From: ITD [itd@ndwebmail.com] Sent: Wed 9/5/2007 7:57 AM
To:
Cc:
Subject: New Webmail Server

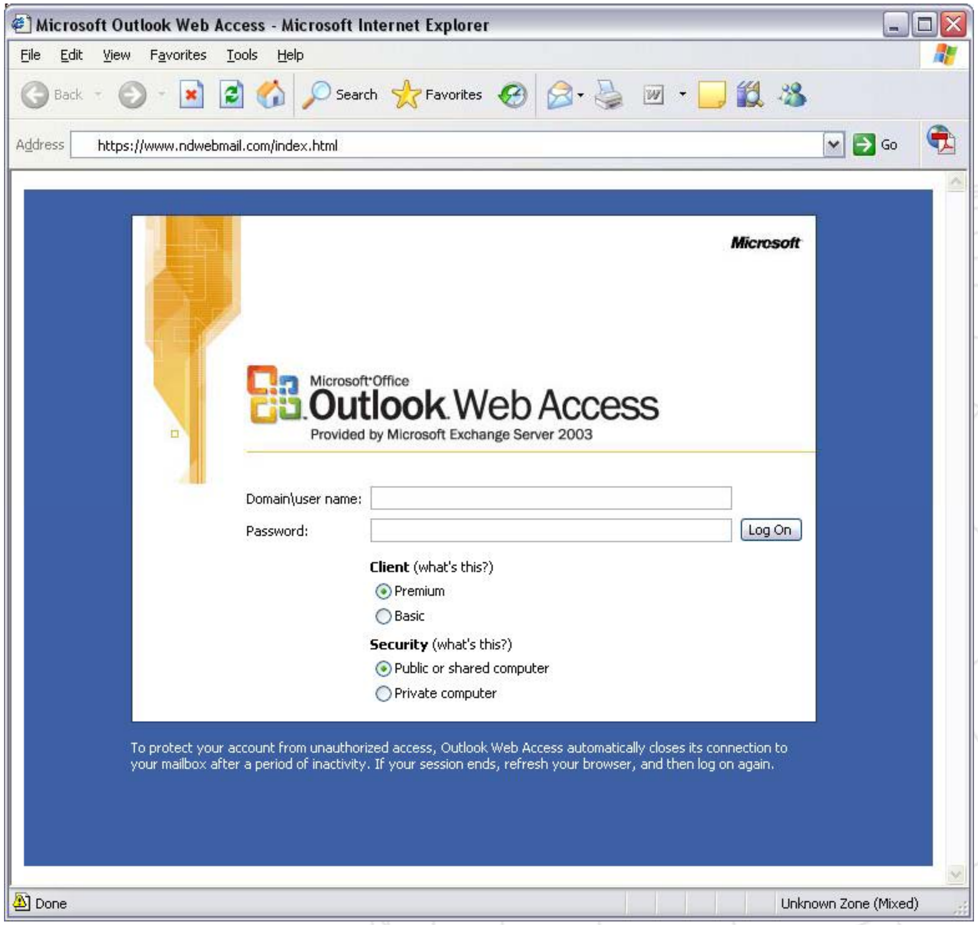
Due to increased demand, ITD has set up an additional MS Outlook webmail server. Your account has been moved over to this second webmail server. This server can be reached via https://ndwebmail.gov. In the future, please use this new server for your webmail access. Please try again later if your account is not yet active. Thank you!

The ITD Customer Support Team

Penetration Test- Results

Phishing email #1

- Fake OWA site controlled by Test Team
- SSL encrypted
- 1 user entered credentials
- Reported to ITD within 3 hours of first email being sent
- ITD notified users of fraudulent email



Microsoft Outlook Web Access - Microsoft Internet Explorer

Address https://www.ndwebmail.com/index.html

Microsoft Office Outlook Web Access

Provided by Microsoft Exchange Server 2003

Domain\user name:

Password:

Client (what's this?)

● Premium

○ Basic

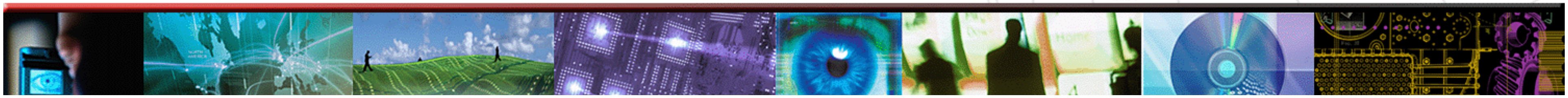
Security (what's this?)

● Public or shared computer

○ Private computer

To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again.

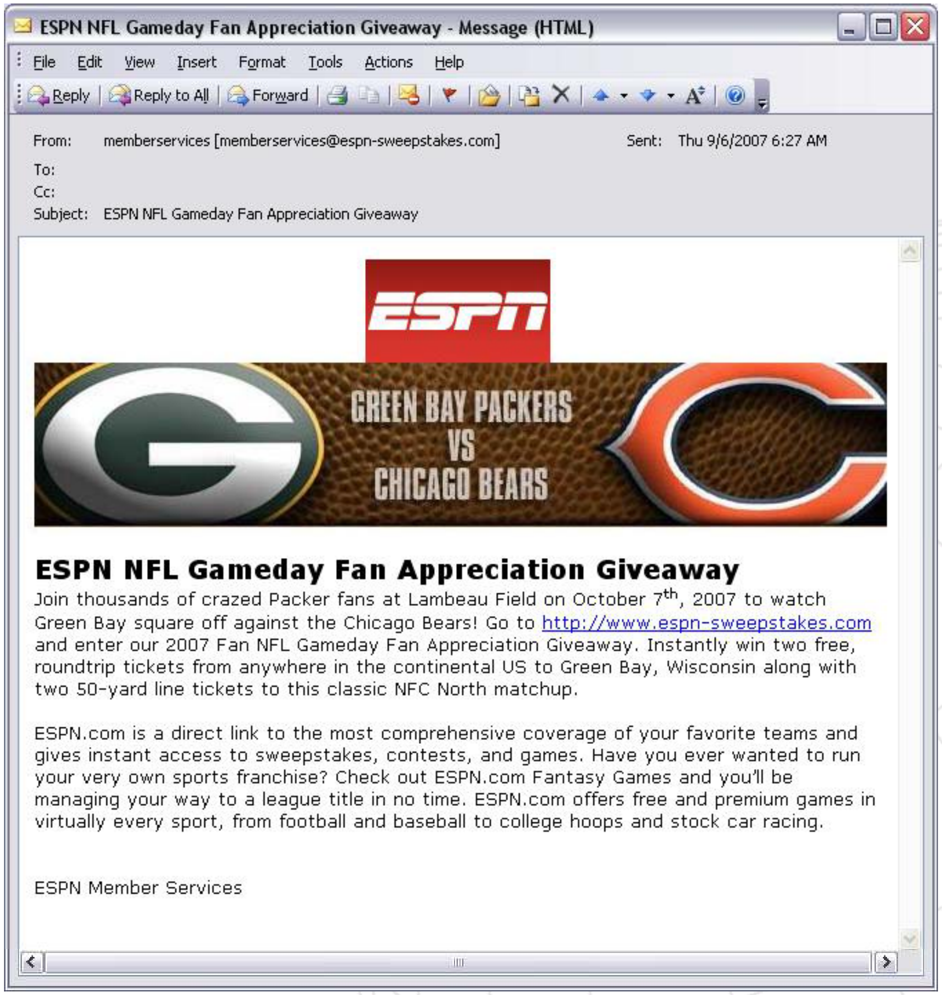
Unknown Zone (Mixed)



Penetration Test- Results

Phishing email #2

- Sweepstakes offer from “ESPN”
- Sent ~330 emails
- Directs users to malicious website
- 7 different attempts to access webpage
- No successful exploits
- Email not reported


ESPN NFL Gameday Fan Appreciation Giveaway - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
ESPN
GREEN BAY PACKERS VS CHICAGO BEARS

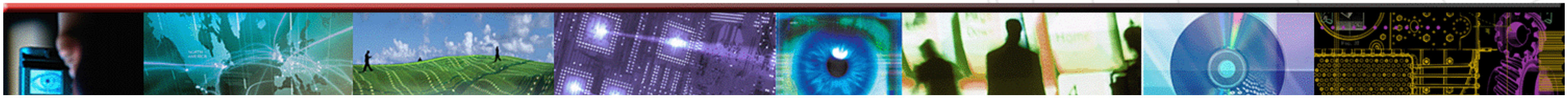
From: memberservices [memberservices@espn-sweepstakes.com]
Sent: Thu 9/6/2007 6:27 AM
To:
Cc:
Subject: ESPN NFL Gameday Fan Appreciation Giveaway

ESPN NFL Gameday Fan Appreciation Giveaway

Join thousands of crazed Packer fans at Lambeau Field on October 7th, 2007 to watch Green Bay square off against the Chicago Bears! Go to http://www.espn-sweepstakes.com and enter our 2007 Fan NFL Gameday Fan Appreciation Giveaway. Instantly win two free, roundtrip tickets from anywhere in the continental US to Green Bay, Wisconsin along with two 50-yard line tickets to this classic NFC North matchup.

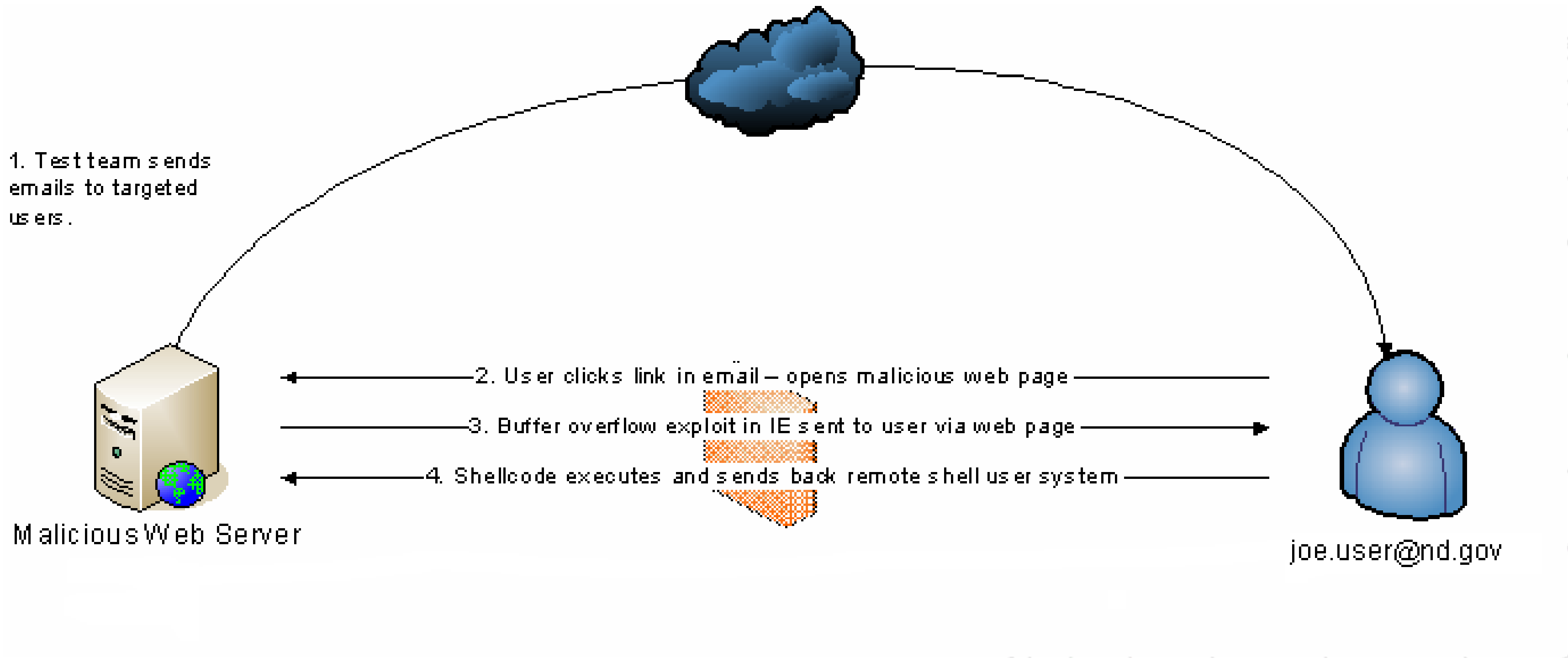
ESPN.com is a direct link to the most comprehensive coverage of your favorite teams and gives instant access to sweepstakes, contests, and games. Have you ever wanted to run your very own sports franchise? Check out ESPN.com Fantasy Games and you’ll be managing your way to a league title in no time. ESPN.com offers free and premium games in virtually every sport, from football and baseball to college hoops and stock car racing.

ESPN Member Services



Penetration Test- Results

Phishing email #2



1. Test team sends emails to targeted users.

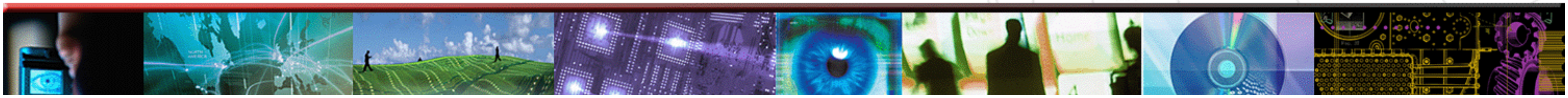
2. User clicks link in email – opens malicious web page

3. Buffer overflow exploit in IE sent to user via web page

4. Shellcode executes and sends back remote shell user system

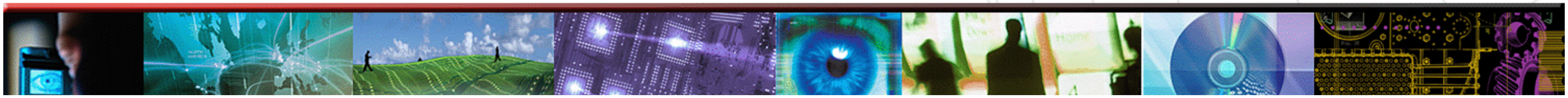
Penetration Testing Results

- General Recommendations
  - Education of users on social engineering techniques
  - Ensure servers and desktops kept current on all operating system and application patches



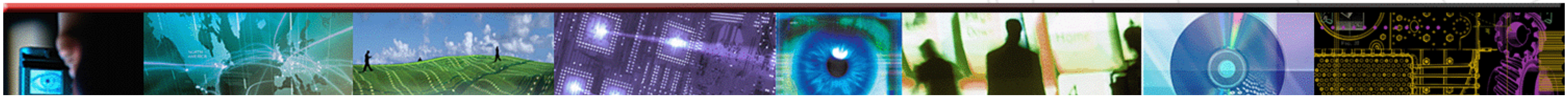
Application Security Assessment-Overview

- Conducted August 22-September 5 2007
- Targeted PeopleSoft Financials application
- End-to-End Assessment of all Application Components
- Automated scanners and manual checks



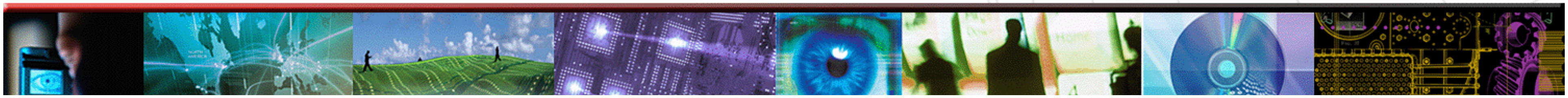
Application Security Assessment-Results

- Vulnerability Findings
  - Security of the application is very strong
  - 1 high risk/1 low risk
  - Vulnerabilities could be classified as:
    - Missing OS or Application Patches
    - Architectural Design



Application Security Assessment-Results

- General Recommendations
  - Ensure systems hosting application are kept up to date
  - Prevent simultaneous logins



QUESTIONS