1 **HOW DO THEY DO IT?**

Part 1: Cyber-Graffiti

2

"You know, I don't know what I hate more, wearing your face, or wearing your body. Look, why don't we just give them back to each other and call it even, okay?"

Castor Troy (Nicolas Cage, wearing John Travolta's face) from the movie, *Face/Off*

3 **Introduction**

- What is *cyber-graffiti*?
  - Web site defacement
  - Hackers using known techniques to gain administrative control and replace the Web site with their own version
- This chapter is rather like a case study
  - We'll follow a hacker as he hacks a travel agency Web site
  - We'll suggest precautions against such an attack

4 **Defacing Acme Travel's Web Site**

- Acme Travel…
  - Small Houston-based company
  - Bought their own domain
  - Company's "computer guy" also the Web site manager
  - Set up a Linux-based system:
    - Proxy server for employee sharing of the DSL connection
    - Apache Web server
    - "Staging" area for Web site design
  - Small site: 8 static Web pages and several images

5 **Defacing Acme Travel's Web Site**

- Basically, the Web pages are an "Electronic" brochure
- Also provides employee's with email accounts
  - SMTP (Simple mail transfer protocol)
  - Fetchmail
  - POP3 (Post office protocol version 3)
- Disgruntled customer decides to "teach Acme a lesson"
- IP trace & port scan of acmetravel.com revealed that the site was hosted elsewhere

6 **Defacing Acme Travel's Web Site**

- But, the email from Acme revealed its IP address in "Received from"

Received:from [10.3.2.1] by acmetravel.com (8.8.8/8.8.5) with ESMTP id RAA08342 for <jsmith@netmail.com>

- Now, run a port scan on 10.3.2.1 to show the open or listening ports

7 **Defacing Acme Travel's Web Site**

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
110/tcp	open	pop-3
8001/tcp	open	http-proxy

- Usually, ports other than 80, 443 and 8001 are "wrapped" in some way.
- The only attack points are ports 80 and 8001

8 **Mapping the Target Network**

9 **Throwing Proxy Servers in Reverse**

- Attempts to connect to ports 80 & 8001 through an HTTP request via a browser results in "Forbidden" – access denied
- Could the proxy server be misconfigured? Might the server let HTTP proxy requests in?
- Using netcat, the hacker sends a "GET http://127.0.0.1:80/ HTTP/1.0" to port 8001
- This request asks the proxy server on port 8001 to open an HTTP connection to 127.0.0.1 on port 80, retrieve the response and data and send it back to the client

10 **Throwing Proxy Servers in Reverse**

- The HTTP response shows that the trick worked!
- The attacker did not get a "Forbidden" but an "Authorization Required" – a step in the right direction!
- The response comes from the Apache server running on port 80, not 8001
- How did this attack work?
-

11 **Throwing Proxy Servers in Reverse**

12 **Throwing Proxy Servers in Reverse**

- How the hack works:
  - Employee browsers are configured to make HTTP requests to 10.0.1.1:8001 (the proxy server)
  - The proxy server sends the request and forwards the response to the local system
  - The proxy acts as a "go between"
  - The proxy server system is dual-homed:
    - 10.0.1.1 – intranet (proxy)
    - 10.3.2.1 – external intranet

13 **Throwing Proxy Servers in Reverse**

- How the hack works: (cont)
  - Directly accessing 10.3.2.1 on port 80 or port 8001 results in "Forbidden"
    - Server configured to reject *incoming* IPs from other than 10.0.1.1–254 and 127.0.0.1 (local loopback)
  - However, misconfiguration allows any IP to *send* a proxy request
  - Thus, sending an HTTP proxy request for 127.0.0.1 to 10.0.1.1:8001 results in a valid response: a 401 Authorization Required
-

14 **A Bit About The 3 A's**

- Q: When a request for a resource is made, will the request result in that resource actually being returned?
- Three criteria to answer this Q:
  - *Authorization*
  - *Authentication*
  - *Access control*
- All 3 criteria are closely related
- In a "real world" app., sometimes the 3 are highly coupled

15 **A Bit About The 3 A's: Authentication**

- *Authentication* is any process by which you verify that someone is who they claim they are
- This usually involves a username and a password, but can include any other method

of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints
- Authentication is equivalent to showing your drivers license at the ticket counter at the airport

16 **A Bit About The 3 A's: Authorization**
- *Authorization* is finding out if the person, once identified, is permitted to have the resource
- This is usually determined by finding out if that person is a part of a particular group, if that person has paid admission, or has a particular level of security clearance
- Authorization is equivalent to checking the guest list at an exclusive party, or checking for your ticket when you go to the symphony

17 **A Bit About The 3 A's: Access Control**
- *Access control* is a much more general way of talking about controlling access to a web resource
- Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, the time of day, the phase of the moon, or the browser which the visitor is using
- Access control is analogous to locking the gate at closing time, or only letting people onto the ride who are more than 48 inches tall
- It's controlling entrance by some arbitrary condition which may or may not have anything to do with the attributes of the particular visitor

18 **Brute Forcing HTTP Authentication**
- There are 3 types of HTTP authentication: Basic, Digest & NTLM
- Basic Authentication:
  - When a browser gets a 401 response, it pops up a dialog for the user to enter a username and password
  - Credentials are encoded by the Base64 encoding scheme and sent to the server for the same resource in a new HTTP request
  - Server decodes Base64 credentials and verifies against its credentials.
  - Match ? 200 OK response : 401 response

19 **Brute Forcing HTTP Authentication**
- Other 2 are not used too often because of their limits:
  - Digest Authentication: only supported by Opera
  - NTLM Authentication: used to with IIS to authenticate Microsoft NT users
- To brute force basic authentication, you simply need a program that generates passwords!
  - You can write your own
  - You can find them on the internet!

20 **The Final Defacing…**
- Once into the server, the hacker pokes around looking for pages to modify
- Even though the Web site is staged (a copy kept locally), modifying pages in the staging directory results in the main server being changed when the stage is uploaded to the off-site server
- Hacker modifies pages and waits for the scheduled update

21 **What went wrong?!?**
- It seemed that the administrator had taken some precautions, but, some areas were left exposed:
  - The HTTP Proxy port 8001 allowed tunneling of HTTP requests inside the internal

network
- Basic authentication is easily cracked with a brute force program
- Directory browsing had not been disabled on the proxy server
- Leaving admin scripts in the document root
- Automatic replication of the Web site on the external Web server

22 **HTTP Brute-forcing Tools**
- HTTP is the easiest protocol to brute force because Web servers are designed to handle a large volume of HTTP requests
- Basically, you can fire loads of username / password combo's at the server
- Programs to brute force HTTP authentication:
  - Home made
  - Brutus
  - WebCracker

23 **Countermeasures…**
- Successfully countering the Acme Travel Hack requires:
  - Addressing the ability of external clients to use the server as a reverse proxy
  - Obtain usernames and passwords through HTTP authentication brute forcing
  - Browser directories on a Web server
- Turning off Reverse Proxying
  - This is a matter of server configuration
  - Each server has a different way to do this
  - In Apache, the configuration file httpd.conf is used.

24 **Countermeasures…**
- Using Stronger Passwords
  - Nothing can be done about strengthening HTTP authentication mechanisms…
  - Enforce better passwords:
    - Longer minimum length
    - Use symbols and punctuation
    - Uppercase / lowercase
  - As the administrator, look for many multiple requests for protected resources in the log file

25 **Countermeasures…**
- Turn off Directory Browsing
  - Directory browsing should always be turned off unless there is a concrete reason for having it on
  - This can be configured in Apache or IIS

26 **Summary**
- Seemingly trivial oversights can lead to disaster!
- Defacement is usually a goal of the hacker
- The hacker usually takes advantage of a known security vulnerability