tracesecurity
Security Compliance Management

Social Networking

Good for Business or Security Nightmare

Get Compliant.
Get TraceSecurity.

d2 d3

Why social networks are popular

- **Easy to use**
- **Easy to learn**
- **Free or very low cost**
- **Large variety of sites to choose from**
  - **Face book, Twitter, LinkedIn, Orkut, MySpace plus hundreds more**
- **Everyone is using them to stay in touch, connect to others, meet new people**

tracesecurity
Security Compliance Management

Slide 2

d2 "mob mentality" - people go along with the crowd
dblazier, 10/1/2010

d3 Multimedia aspect has a psychological impact on the user...makes them actually feel connected with others.

This actually helps bring their guard down and share "too much information" which is what criminals are hoping for.
dblazier, 10/1/2010

d1

Why businesses benefit from social networks

- **Sales and Marketing tool**
- **Lead Generation Tool to attract potential customers**
- **Builds relationships with customers**
- **Creates an online presence of the business**
- **Screening tool for potential employees**
- **Many other great benefits**

tracesecurity
Security Compliance Management

Slide 3

d1 makes the relationship "sticky" - meaning that people VALUE RELATIONSHIPS and will stick to what they know
dblazier, 10/1/2010

Disadvantages from social networks

- Loss of employee productivity
- Privacy and security concerns
- Time consuming to maintain web presence
  - Dedicated Staff needed for maintenance and security
- Information not fully controlled by the business
  - Privacy policy is not a legal contract
- Once posted to the internet, the information Lives Forever!

tracesecurity
Security Compliance Management

Risks from social networks

- Unintentional or intentional information disclosure
- Reputational Risks
- Compromise of corporate network by introducing malware
  - Multiple vulnerabilities published recently
  - Outdated web browsers, unpatched systems, minimal technical security controls
- Legal and compliance issues
  - Regulations such as GLBA, NCUA, FDIC, HIPPA, etc
- Social Engineering nightmare

tracesecurity
Security Compliance Management

d5

Security Problems

- Controlling the information
- Lack of training for social network users
- Perception of trust that the site is safe
- Primary target of malicious hackers
- Well known malware, trojans, viruses still exist
  - Zeus (can be purchases for around $700)
  - Koobface
  - Conficker

tracesecurity
Security Compliance Management

Slide 6

d5 Because the users can link the content or repost to their own portals, it causes the company to lose any control over where the content appears

dblazier, 10/1/2010

WEB 2.0

- **Most social networks are based on WEB 2.0**
- **Web Content is retrieved from different applications, servers, tc without involvement of the user (AJAX) example is Google maps**
- **The website is only as secure as the other websites that provide information to the application**
- **If a vulnerability such as (XSS), exists on a web server that provides information to the website any visitor to the site is put at risk and unknowingly compromised**

tracesecurity
Security Compliance Management

Attack Example

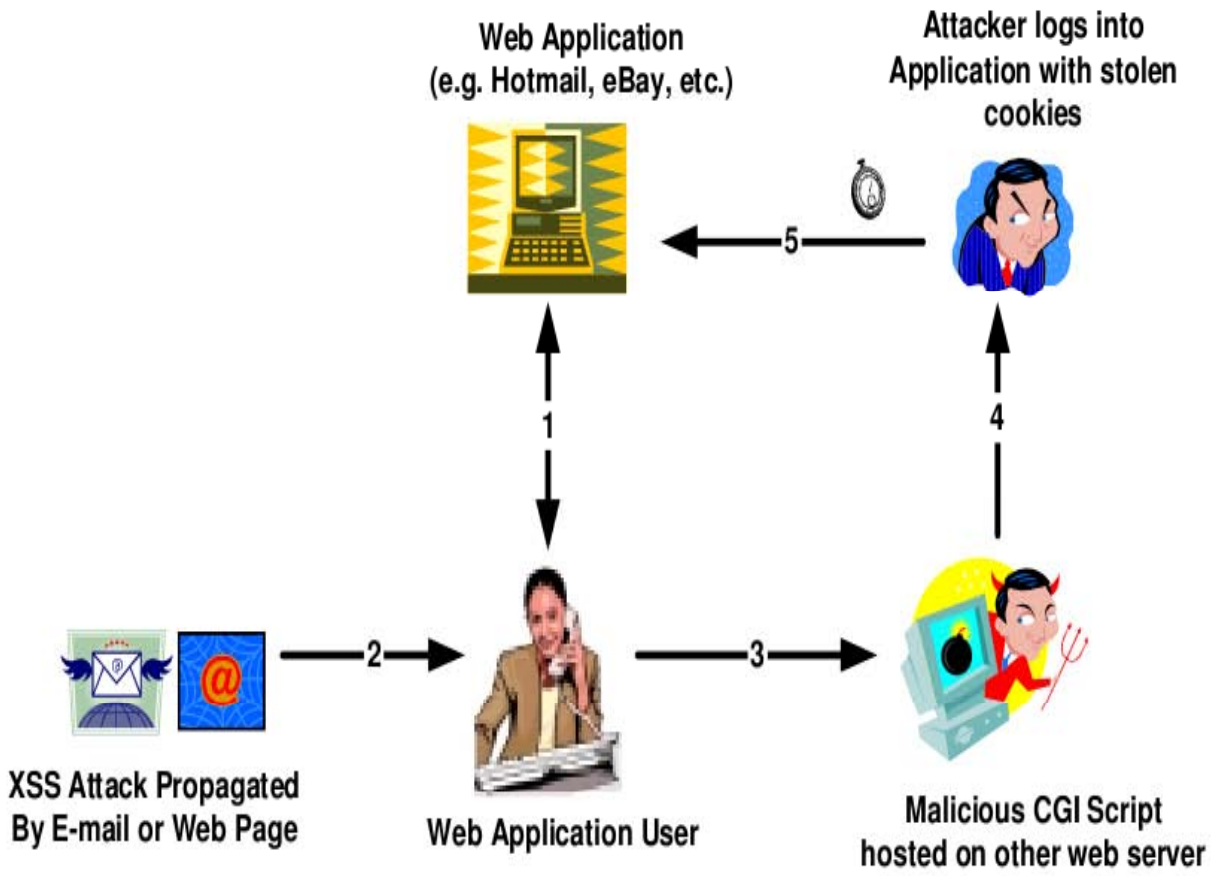
1. **Internet Searches to gather information about employees of a specific company**

   Twitter, Facebook, MySpace, LinkedIn, YouTube, classmates.com, etc

2. **Attacker sends invitations to befriend potential victims**
3. **Victims accepts invitation from Attacker**
4. **Since employees are likely to check social networking sites at work, the attacker sends a link to a malicious website, an obfuscated link using TinyURL or a email a malicious file containing malware**
5. **Employee gets message from new friend at work and clicks on the link or opens the malicious PDF from workstation on the network. Game Over**

tracesecurity
Security Compliance Management

Attack Example



tracesecurity
Security Compliance Management

Tools available for social engineering attacks

Social Engineering Toolkit (SET)

- Allows to launch a phishing attack against large groups
- Clone Websites such as FaceBook, Online Banking, etc
- Creates a website for you (no experience needed)
- Create malicious payloads such as infected PDFs, pictures, etc

Metasploit Framework

- Free for everyone
- Web-Based frontend
- Hundreds of exploits available for use

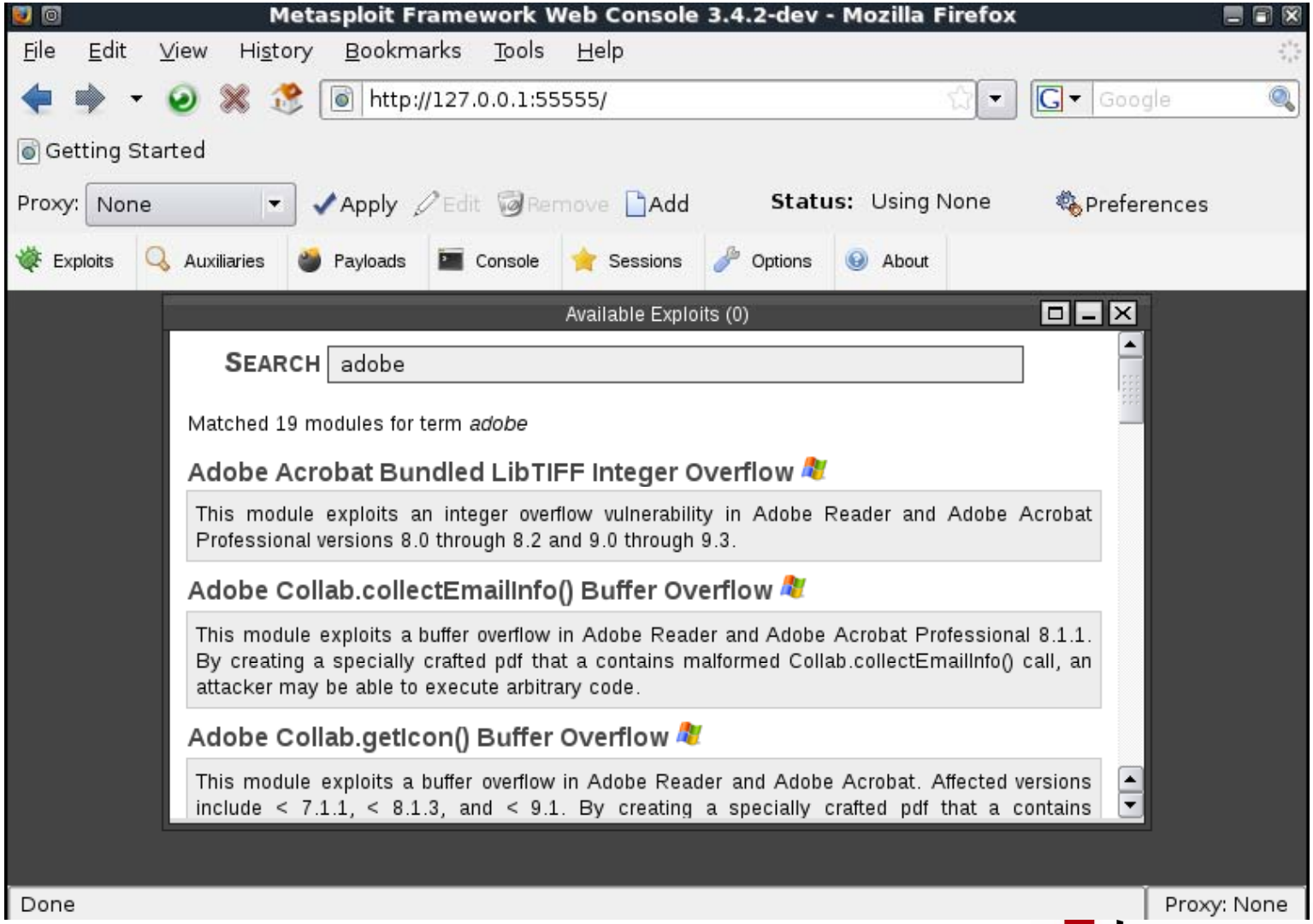
BeEF –Browser Exploitation Framework

tracesecurity
Security Compliance Management

Social Engineering Toolkit

```
  [---]        The Social-Engineer Toolkit (SET)          [---]
  [---]         Written by David Kennedy (ReL1K)          [---]
  [---]                  Version: 0.5                     [---]
  [---]          Codename: 'Return of the Lemon'          [---]
  [---]      Report bugs to: davek@social-engineer.org    [---]
  [---]        Homepage: http://www.secmaniac.com         [---]
  [---]      Framework: http://www.social-engineer.org    [---]
  [---]       Unpublished Java Applet by: Thomas Werth    [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Select from the menu on what you would like to do:

1. Spear-Phishing Attack Vectors
2. Website Attack Vectors
3. Infectious USB/CD/DVD Generator
4. Update the Metasploit Framework
5. Update the Social-Engineer Toolkit
6. Create a Payload and Listener
7. Mass Mailer Attack
8. Help, Credits, and About
9. Exit the Social-Engineer Toolkit

Enter your choice:
```

Metasploit Framework



tracesecurity
Security Compliance Management

Beef Exploitation Framework

View Zombies Standa

Browser Exploitation Framework

BeEF

Company
User Name
Password
LOGIN
Remember me on this computer
Copyright © 2009 activision Inc. All rights reserved.

Browser Exploitation Framew

File Edit View History Bookmarks Tools Help

http://beef/ui/#

View Zombies Standard Modules Browser Modules Network Modules Options Help

Browser Exploitation Framework

BeEF

Autorun
Disabled

Zombies

Details [Hide]

Browser
Internet Explorer 8.0
Operating System
Windows NT 5.1
Screen
1024x768 with 32-bit colour
Cookie
BeEFSession=b47ae01c566729223e20efd41f8f6625

Page Content [Show] [UNSAFE View Content Popup]

Key Logger [Hide]

Keys
anftrdjnpubalpassword

Module Results [Hide] [Clear]

Data not available

tracesecurity
Security Compliance Management

Example Attack

Shell - Social Engineering Toolkit

Session Edit View Bookmarks Settings Help

```
Enter what type of attack you would like to utilize.

The Java Applet attack will spoof a Java Certificate and
delivery a metasploit based payload.

The Metasploit browser exploit method will utilize select
Metasploit browser exploits through an iframe and deliver
a Metasploit payload.

1. The Java Applet Attack Method
2. The Metasploit Browser Exploit Method
3. Return to the previous menu.

Enter your choice (press enter for default): 2
SET supports both HTTP and HTTPS
Example: http://www.thisisafakesite.com
Enter the url to clone: http://www.tracesecurity.com

[*] Cloning the website: http://www.tracesecurity.com
[*] This could take a little bit...
[*] Injecting iframes into cloned website....
[*] Malicious iframe injection successful...crafting payload.
```

Shell

tracesecurity
Security Compliance Management

Attacker's IP address

Shell - Social Engineering Toolkit

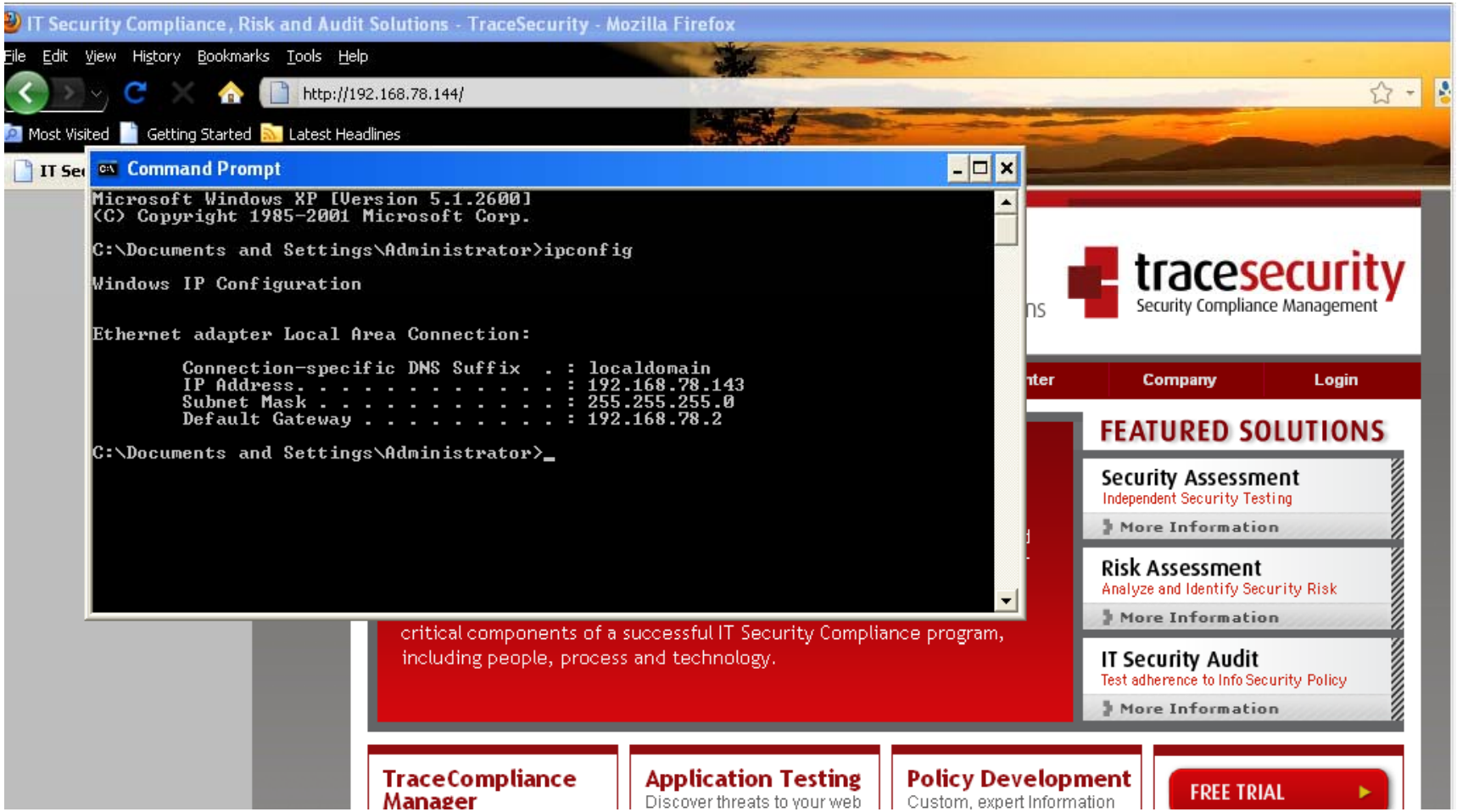
Session Edit View Bookmarks Settings Help

```
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[-] Unknown command: exploit.
msf > ifconfig
[*] exec: ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0c:29:d8:ea:b6
          inet addr:192.168.78.144  Bcast:192.168.78.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed8:eab6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:435 errors:0 dropped:0 overruns:0 frame:0
          TX packets:319 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:350483 (350.4 KB)  TX bytes:29756 (29.7 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1023 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1023 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3059730 (3.0 MB)  TX bytes:3059730 (3.0 MB)
```

Shell

tracesecurity
Security Compliance Management

Victim's IP address



tracesecurity
Security Compliance Management

Cloned Website

IT Security Compliance, Risk and Audit Solutions - TraceSecurity - Windows Internet Explorer

Back to Google (Alt+Left) 192.168.78.144/

File Edit View Favorites Tools Help

Favorites Suggested Sites Free Hotmail Web Slice Gallery

IT Security Compliance, Risk and Audit Solutions - Tra...

CLOUD BASED COMPLIANCE

IT Security Compliance, Risk & Audit Solutions

tracesecurity
Security Compliance Management

Solutions | Products | Industries | Resource / Media Center | Company | Login

A leading provider of IT Security Compliance and Risk Management Solutions

TraceSecurity helps organizations of all sizes to achieve, maintain and demonstrate IT security compliance while significantly improving their security posture. Through a combination of its software and professional services solutions, TraceSecurity helps clients address all critical components of a successful IT Security Compliance program, including people, process and technology.

FEATURED SOLUTIONS

Security Assessment
Independent Security Testing
More Information

Risk Assessment
Analyze and Identify Security Risk
More Information

IT Security Audit
Test adherence to Info Security Policy
More Information

Risk Assessment
To secure a network, first

IT Security Audit
Validate the Information

Security Assessment
Independent testing of Info

FREE TRIAL

tracesecurity
Security Compliance Management

Game Over

Shell - Social Engineering Toolkit

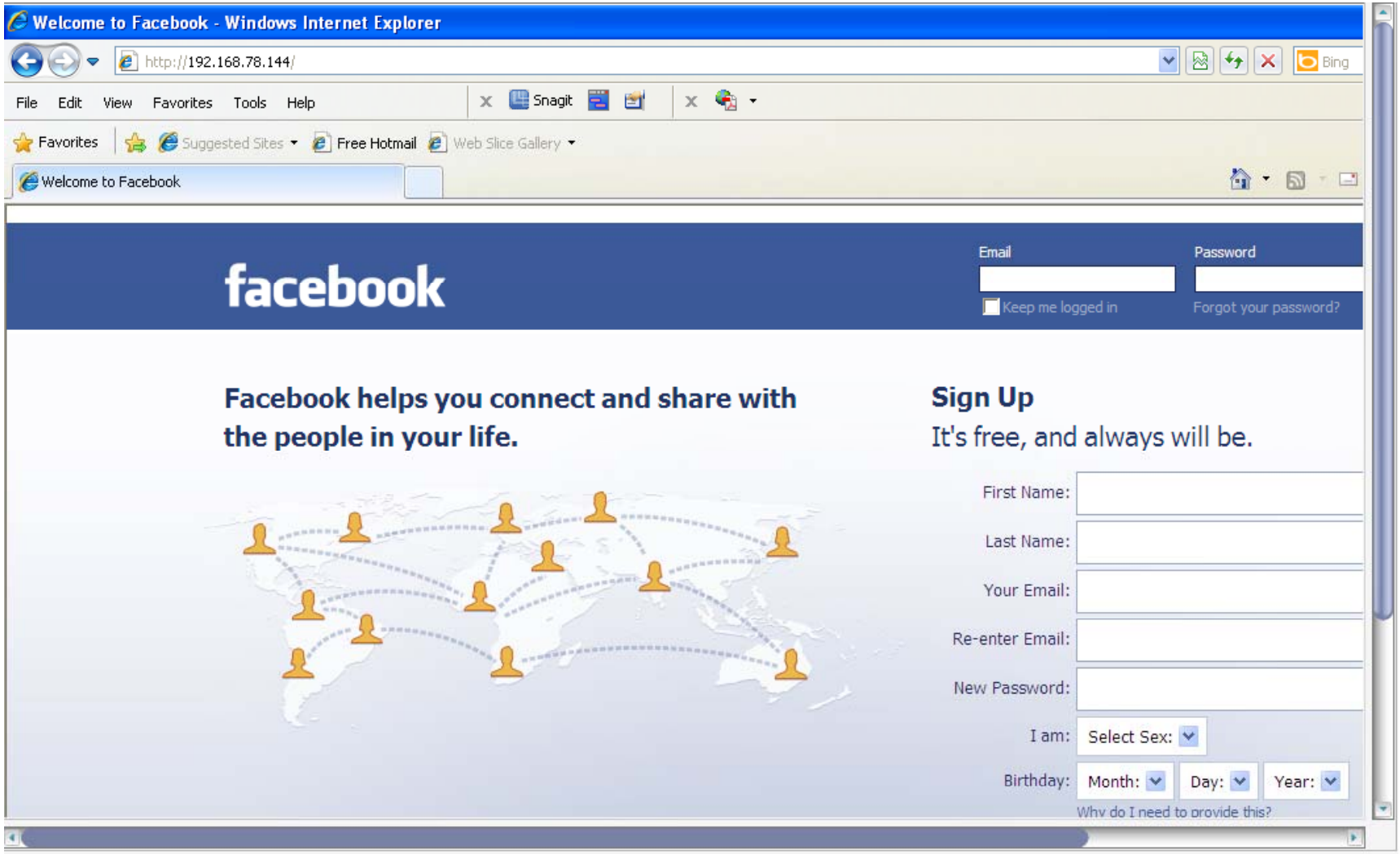
Session Edit View Bookmarks Settings Help

```
  Id  Type   Information  Connection
  --  ----   -----------  ----------
  1   shell               192.168.78.144:2525 -> 192.168.78.143:1499

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.78.143
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.78.2

C:\Documents and Settings\Administrator\Desktop>
```

Shell

tracesecurity
Security Compliance Management

Facebook clone



tracesecurity
Security Compliance Management

Malicious Payload Generation

Fast-Track Web Interface - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:44444/payloadgen

Getting Started

Proxy: None Apply Edit Remove Add Status: Using None Preferences

Page Load Error | Fast-Track Web Interface

- Fast-Track Main
- Fast-Track Updates
- Autopwn Automation
- Microsoft SQL Tools
- Mass Client-Side Attack
- Exploits
- Binary to Hex Payload Converter
- Payload Generator
- Fast-Track Tutorials
- Fast-Track Changelog
- Fast-Track Credits

Fast-Track Payload Generator

The Metasploit Payload Generator is a simple tool to make it extremely easy to generate a payload and listener on the Metasploit framework. This does not actually exploit any systems, it will generate a metasploit payload for you and save it to an executable. You then need to someone get it on the remote server by yourself and get it to execute correctly.

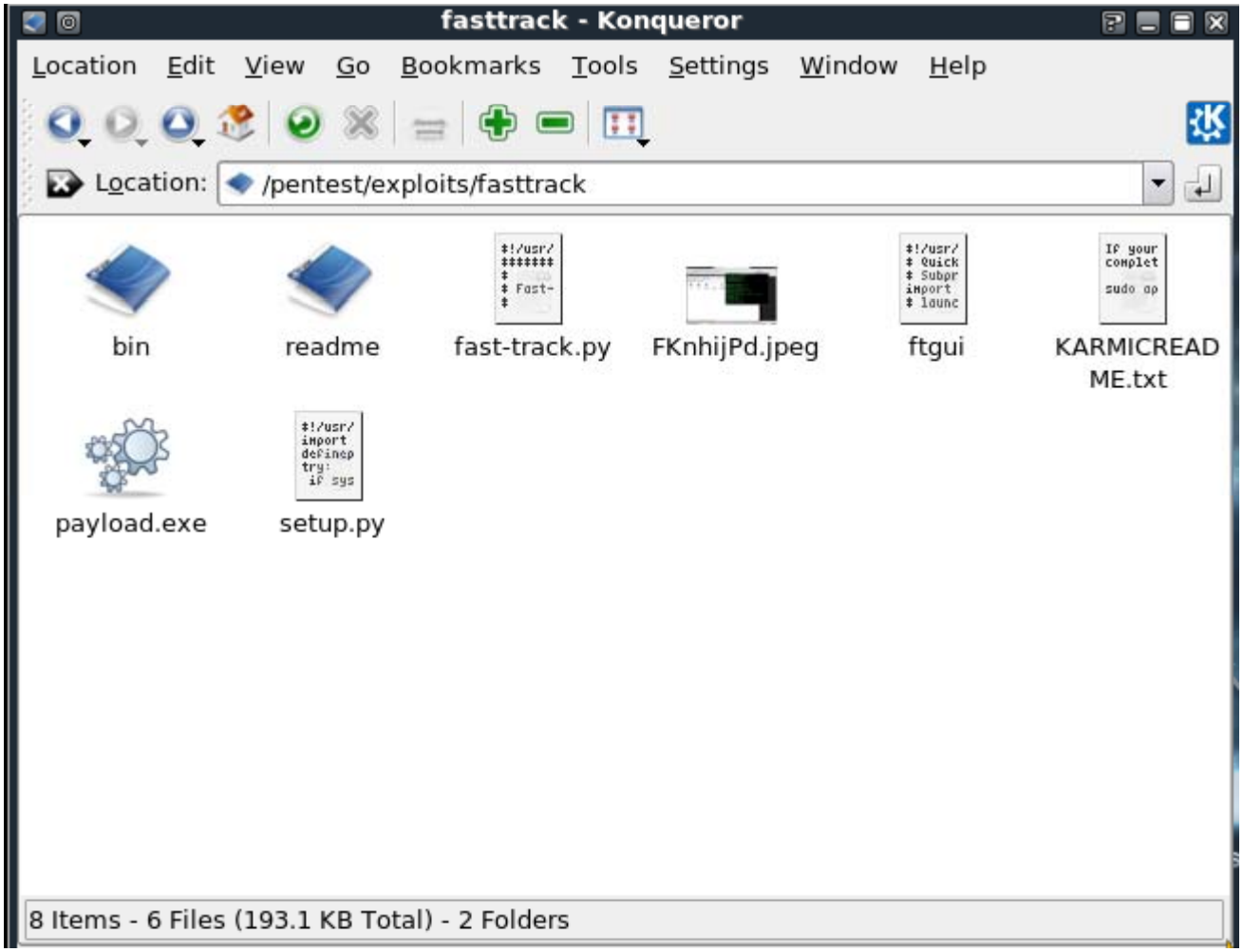
This will also encode your payload to get past most AV and IDS/IPS.

Payload Generator Options

Simply hit launch in order to start the payload generator

tracesecurity
Security Compliance Management

Malicious Payload



tracesecurity
Security Compliance Management

Virus Detection/Analysis website

VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.virustotal.com/file-scan/report.html?id=

Getting Started

Proxy: None Apply Edit Remove Add Status: Using None Preferences

VT Community Sign in ▼ Languages ▼

VIRUS TOTAL

Virustotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name:	**payload.exe**
Submission date:	**2010-08-12 16:20:41 (UTC)**
Current status:	**finished**
Result:	**13/ 42 (31.0%)**

VT Community

not reviewed

Safety score: -

Compact Print results

tracesecurity
Security Compliance Management

Risk Mitigation

- **Employee Awareness Training**
  - **Most effective against social engineering attacks**
- **Take a proactive approach to managing security and risk**
- **Perform a Risk Assessment**
  - **Identify all risks associated with use of social networks**
- **Ensure strong network security controls are in place**
- **Establish Policies and Guidelines addressing social network usage and maintenance**
  - **Password changes**
  - **Change Management**
- **Periodically test for compliance using a variety of techniques**

tracesecurity
Security Compliance Management

Questions ????????

Questions ????????

Questions ????????

Questions ????????

tracesecurity
Security Compliance Management

Questions ????????

- http://www.social-engineer.org
- http://metasploit.com
- http://www.us-cert.gov/reading_room/
- http://www.onguardonline.gov

tracesecurity
Security Compliance Management