VeriSign

iDEFENSE
A VeriSign Company

Exploitation Frameworks: A Comparative Study

iDefense Intelligence Operations

Dec. 15, 2005

Where it all comes together.

Overview

- iDefense Overview
- Exploitation Frameworks Background
  - What is an exploitation framework?
  - Metrics for comparison
- Exploitation Frameworks Defined
  - Metasploit Framework
  - CANVAS
  - Core Impact
- Conclusions
- Q&A

About iDefense: Overview

- iDefense, a VeriSign Company, is a leader in cyber threat intelligence.
- Industry-Leading Service Offerings
  - Intelligence is all that iDefense does
- Marquee Customer and Partner Base
  - Government, financial services, retail, telecom and others
- Experienced Intelligence Teams
  - iDefense Labs
  - Vulnerability Aggregation Team (VAT)
  - Malicious Code Team (Malcode)
  - Threat Intelligence Team
  - Rapid Response Team
- In business since 1998, iDefense became a VeriSign Company in July 2005

iDefense Intelligence Services

Daily / Hourly Research Deliverables

+ Comprehensive Vulnerability Feed
  - Most comprehensive, timely, technical feed in the industry
+ iDefense Exclusive Vulnerabilities
  - More than 250 contributors around the globe
  - Released to vendor and iDefense customers only
  - More than 160 iDefense Exclusive vulnerabilities so far in 2005
+ Malicious Code Research and Reporting

iDefense Intelligence Services

Weekly / Semi-Monthly Research deliverables

+ Weekly Threat Report
  - Weekly compilation of worldwide threats
  - Critical Infrastructure, State of the Hack, Cyber Crime, Terrorism and Homeland Security, Global Threat

+ iDefense Topical Research Papers
  - Examples:
    - Security of Enterprise Web-Based E-Mail Interfaces
    - Security Comparisons: Internet Explorer vs. Firefox
    - Phishing and Pharming: A Comparison
    - Mitigating the Threat from Keyloggers

+ Focused Threat Intelligence Reporting
  - Topics specific to individual customers

Overview

- iDefense Overview
- Exploitation Frameworks Background
  - What is an exploitation framework?
  - Metrics for comparison
- Exploitation Frameworks Defined
  - Metasploit Framework
  - CANVAS
  - Core Impact
- Conclusions
- Q&A

Background

- Metasploit Framework
  - Open-source project created in mid-2003 by H.D. Moore
  - Created for pen-testing and research; a free alternative to others
  - Widely used by hacking community since it is free
- CANVAS
  - Offered by Immunity Inc., started by Dave Aitel in 2002
  - Aimed at promoting exploit development and providing a penetration testing platform
- Core Impact
  - Core Impact was developed by CORE Security Technologies in 1996
  - Dubbed as the first fully automated penetration testing product
  - Expensive product used mainly by corporations

Metrics for Comparison

- Costs
- Supported platforms and installation
- Documentation
- Number of available exploits
- Types of available exploits
- Payload options
- Method of announcing and delivering new exploit modules
- Exploit module creation response time
- Effectiveness of exploits
- Ability to make custom exploits
- Product support and maintenance
- Overall usability

Metasploit Framework – Costs, Installation and Documentation

- **Costs**
  - Free
- **Platforms and Installation**
  - Available for Unix/Linux environments
  - Can be used on win32 platforms via a provided Cygwin environment
  - Downloadable as a Tar, or as a Windows installer
- **Documentation**
  - 34-page user guide that is fairly comprehensive

Metasploit Framework – Exploits and Payloads

- **Number of Available Exploits**
  - Currently 108 exploits
  - More will be released with version 3.0, Q1 2006
- **Types of Available Exploits**
  - Operating Systems: Windows, Unix, BSD, Solaris, IRIX, Mac OS X
  - Applications: AIM, CA BrightStor, IIS, Oracle, IMAP, Samba, Novell Zenworks, AWStats, etc.
- **Payload Options**
  - Reverse shell, bind shell, execute command, inject a VNC server, etc.
  - Includes options for covering tracks

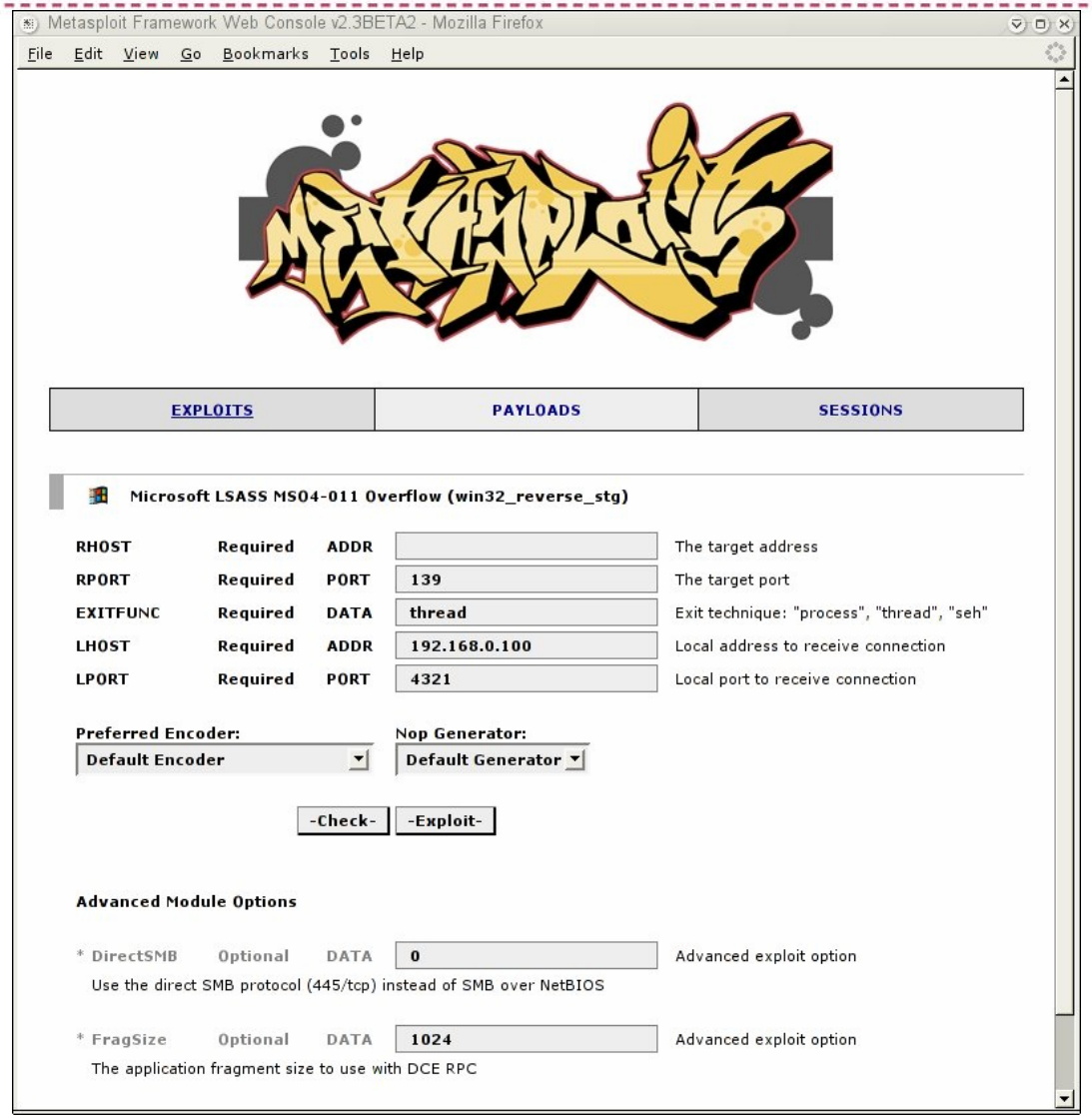
Metasploit Framework – Announcing, Creation and Effectiveness

- **Delivery of New Exploit Modules**
  - Announced on public website
  - New exploit modules can be downloaded via simple command
- **Exploit Module Creation Response Time**
  - Depends on intricacy of issue
  - Between four days and one year
- **Effectiveness of Exploits**
  - When tested against vulnerable systems, the vulnerability was always exploited
  - LSASS exploitation verified

Metasploit Framework – Custom Exploits, Support and Usability

- **Custom Exploits**
  - Well-documented, open scripting language
- **Product Support and Maintenance**
  - Release new versions and updates every three to four months
  - No publicized support channels
- **Overall Usability**
  - Very strong command-line interface (CLI)
  - Fairly simple Web-based graphical user interface (GUI)
  - More advanced GUI expected with version 3.0

Screenshots – Metasploit



CANVAS – Costs, Installation and Documentation

- **Costs**
  - Initial purchase fee of $1,244 for three months (10-seat package)
  - Each additional quarter of support and updates is $619 (10-seat package)
  - $3,101 for a 10-seat license for the year
- **Platforms and Installation**
  - Officially runs on Linux and Windows Environments
  - Easy to install on Linux
  - Install can be complex on Windows systems, which requires third-party components such as Python (fussy about versions of components)
- **Documentation**
  - Offers basic user documentation
  - Documentation offered is not the most intuitive

CANVAS – Exploits and Payloads

- **Number of Available Exploits**
  - Roughly 90 to 100 exploits
- **Types of Available Exploits**
  - Operating Systems: Windows, Unix, Solaris, BSD
  - Applications: Oracle, Snort, CA Unicenter, NAI ePolicy Orchestrator, Compaq Web Management, etc.
  - Hardware: Linksys
- **Payload Options**
  - Each exploit provides a specific payload (e.g., connect-back payload or a connection-recycling payload)
  - Does not provide specific payload options
  - Upon successful exploitation, a command window (Listener Shell) is presented, allowing for uploading and downloading files, executing commands and taking screenshots

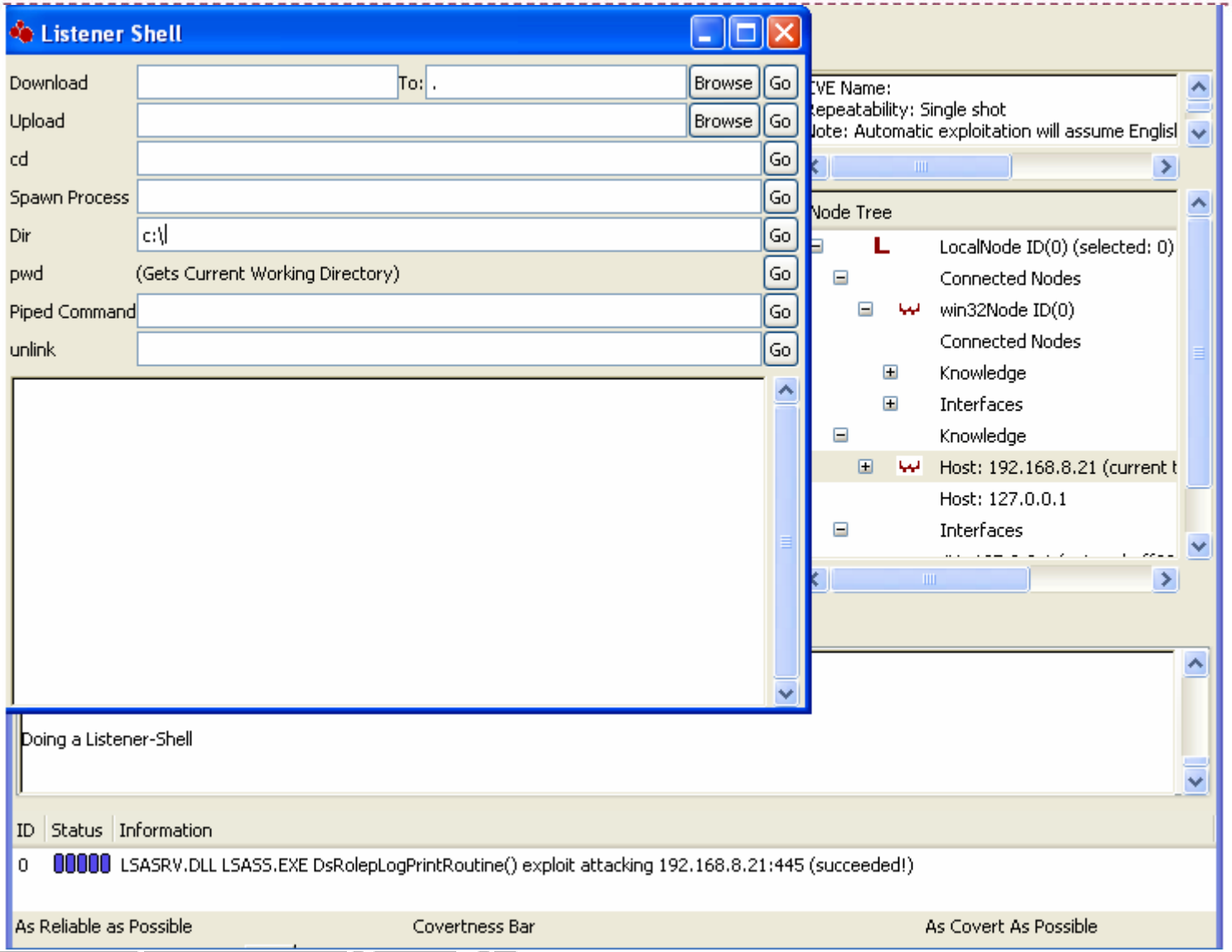
CANVAS – Announcing, Creation and Effectiveness

- **Delivery of New Exploit Modules**
  - Delivery of CANVAS is performed strictly via the Internet
  - E-mail notifications are sent to CANVAS customers for new exploit modules
  - Exploit modules can be found in the main functionality tree
- **Exploit Module Creation Response Time**
  - Usually within a week for high-profile issues
  - Immunity resells a package called VulnDisco, which contains original vulnerabilities and exploits designed to be used with CANVAS
- **Effectiveness of Exploits**
  - Very effective against vulnerable systems
  - Allows user to launch further attacks after using a different exploit on a specified host
  - LSASS exploitation verified

CANVAS – Custom Exploits, Support and Usability

- **Custom Exploits**
  - Users may code their own exploits
  - Exploit modules need to be written in Python
- **Product Support and Maintenance**
  - Maintained on a monthly basis
  - E-mail support is offered
- **Overall Usability**
  - Command-line interface (CLI)
  - Graphical user interface (GUI)
  - Immunity expects users to have considerable knowledge of penetration testing and exploits

Screenshots – CANVAS



CORE IMPACT – Costs, Installation and Documentation

- **Costs**
  - $25,000 per year for an unrestricted license with no IP restrictions
  - $15,000 per year for no IP restriction, but only eight targets may be discovered or attacked at a time
  - “Pay as you go” approach
- **Platforms and Installation**
  - Available only for Windows operating systems
  - Installed through a Windows installation wizard
- **Documentation**
  - Extensive user guide detailing features and use
  - Modules reference that explains each exploit
  - Developers guide that explains how to write exploits

CORE IMPACT – Exploits and Payloads

- **Number of Available Exploits**
  - Currently 155 available exploits
  - Three to four exploits released per month
- **Types of Available Exploits**
  - Exploits span multiple vendors and products
  - Typically high-profile exploits for highly distributed software are chosen for inclusion
  - Remote, local and client-side exploits are available
- **Payload Options**
  - Employs the use of “agents” instead of shells
  - Agents allow for any type of code execution and a shell-like interface
  - After installation, agents may also scan and attack the network of the compromised host

CORE IMPACT – Announcing, Creation and Effectiveness

+ **Delivery of New Exploit Modules**
  - Exploits announced publicly
  - Only delivered to customers
  - Exploit modules delivered by running the module update function on the client

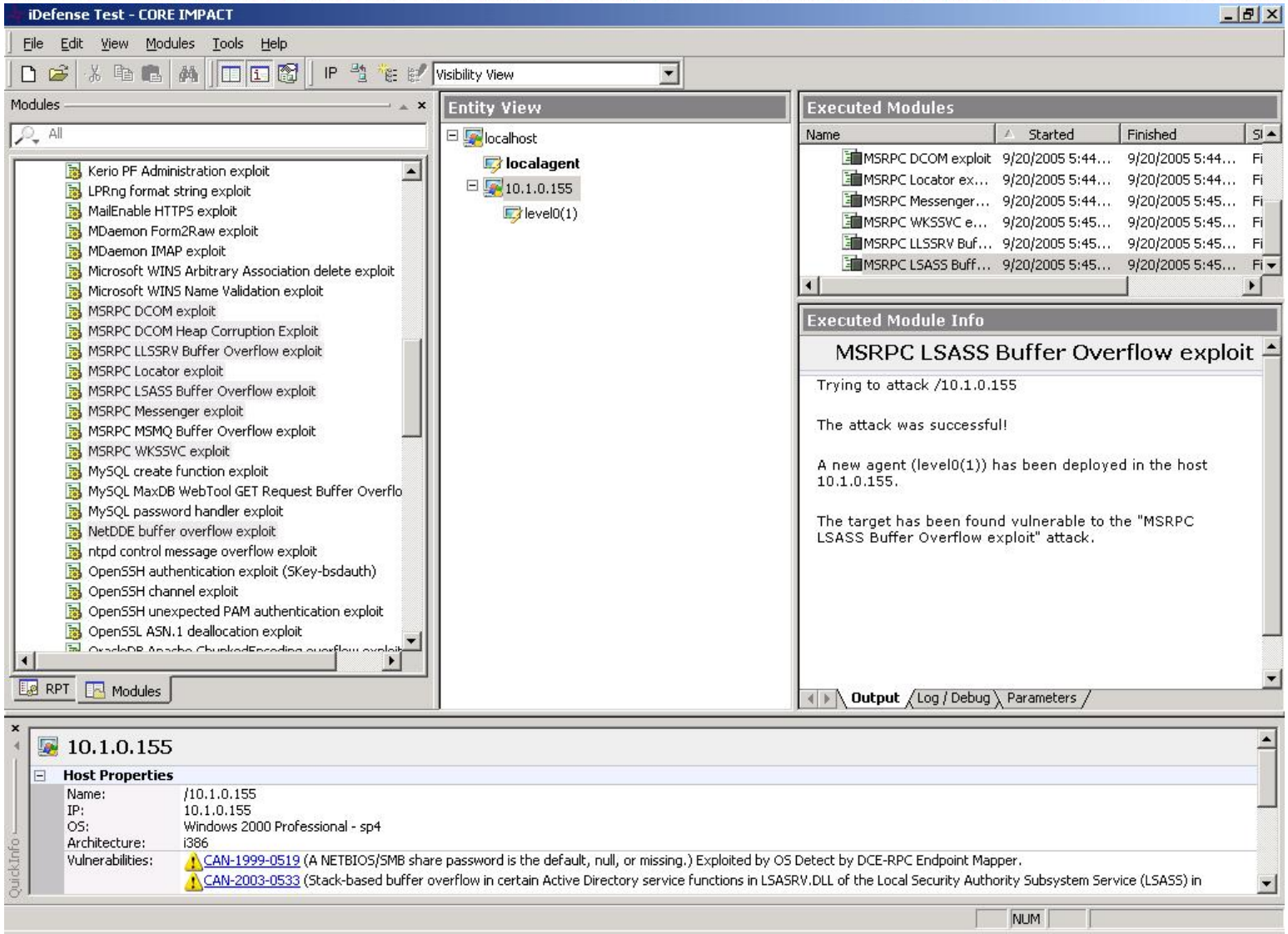
+ **Exploit Module Creation Response Time**
  - Typically published two weeks after substantial details regarding the issue are public
  - Exploits are sometimes added before public exploit code has been released

+ **Effectiveness of Exploits**
  - When tested against vulnerable systems, the vulnerability was always exploited
  - Agents are installed automatically upon exploitation
  - LSASS scan and exploitation verified

CORE IMPACT – Custom Exploits, Support and Usability

- **Custom Exploits**
  - Users may write their own exploits
  - All exploits are written in Python scripts
  - Coding is simplified – single function calls to install agents
- **Product Support and Maintenance**
  - Updated frequently – twice within four months
  - Updates are delivered through the client
  - Technical support via phone is offered to users
- **Overall Usability**
  - Completely GUI based
  - Scanning and exploitation can all be performed through wizards
  - Easy to use – few technical skills are required

Screenshots – Core Impact



Customer Concerns

- CORE IMPACT poses the lowest risk to corporate networks due to the price and lack of funds available to hackers. However, this does not take into account the software ending up in malicious hands or the ability of heavily funded hacking groups.
- CANVAS may pose a moderate risk to corporate networks. The threat is also mitigated by the price of the framework.
- Metasploit has and will continue to pose a significant threat to corporate networks. This framework has always been the “hacker’s framework,” since it may be obtained for free. Hackers looking to penetrate a large number of systems may employ the use of Metasploit in conjunction with a simple vulnerability scanner.
- No framework can replace the will and ability of a determined and skilled hacker

Conclusions

- Metasploit poses the greatest risk to vulnerable networks
  - Price
  - Availability
  - Customizable
- CORE IMPACT is the best corporate penetration testing solution
  - Fully automatic
  - Most exploits available, most maintained
  - Most professional, but also most expensive
- CANVAS is the middle-of-the-road solution for corporate penetration testing
  - More intuitive than Metasploit, not the most user friendly
  - More timely delivery of high profile exploits than Metasploit
  - Fewer total number of exploits than CORE IMPACT
  - Costs less than CORE IMPACT

Questions?