Beyond Exploits
introduction

Hello
my name is

HD Moore

RAPID7
Chief Security Officer

metasploit
Founder & Chief Architect
survey

Favorite non-exploit attack vector?

• Sent via twitter to ~10,000 folks
• At midnight on a Saturday…
Answer: Guns
Answer: Beer
survey results

Answer: Seduction
survey results

The serious answers

• Social engineering and phishing campaigns
• Physical access, swapping disks, post-it notes
• Guessing default and common passwords
• Dumping password hashes from services
• Attacking insecure web applications
• Exposed SMB and NFS shares
• ARP spoofing and sniffing
• Attacking link-local IPv6
Exploits are not that important

• The same methods worked 10 years ago too
• The media still focuses on the latest bug
• We are still finding more bugs than ever
• Exploits are always going to part of security
• The standby techniques continue to work
survey results

“I haven’t used an actual exploit during a penetration test since I started this job”
The case for Metasploit

- 500k line code base, highly active dev team
- 120k users update from SVN each month
- Large, highly-motivated community
- Huge library of reusable code
- Standardized
  - Module formats
  - Module options
  - User interfaces
  - User automation
  - Post-exploitation
The meatware is vulnerable

- Proper social engineering is manual work
- Email, IM, Facebook, USB keys, netbooks

- Metasploit can generate the payloads
  - Generate exe, dll, doc, etc with ./msfpayload
  - Create PDFs with embedded EXEs
  - Build signed java applets

- Metasploit can automate data collection
  
  ```
  msf > set AutoRunScript winenum
  ```
Excellent password testing tools

• Include common and default wordlists
• Support for multiple concurrent targets
• Automatic database storage of results
• Support for databases
  • MS-SQL, Oracle, MySQL, PostgreSQL, DB2
• Support for admin interfaces
  • SMB, SSH, Telnet, FTP, VNC
• Support for web frameworks
  • Tomcat, JBoss, Axis2, HTTP
password hashes

Working with NTLM hashes

• The hash is the secret used for authentication
• The clear-text password is not needed at all
• Compromise any system and dump hashes
• SMB modules can authenticate with a hash
• Remote code execution via psexec + hash
• Capture challenges with capture/smb
• Relay authentication with smb_relay
• Convert LANMAN to NTLM with lm2ntlm.rb
• Replay hashes across the entire network [1]

1. The commercial Metasploit products automate this completely
Capturing and cracking hashes

- Launch auxiliary/server/capture/smb
- Embed a UNC image link into .DOC
- Email this *safe* document to targets
- Wait for the authentication attempt
- Crack with rainbow tables
- Login to Outlook Web Access
- Login to the corporate VPN
- Single-sign on is great 😊
Relaying NTLM authentication

• Launch exploit/windows/smb/smb_relay
• Specify a SMBHOST target (DC)
• Set AutoRunScript to add a backdoor
• Wait for an automated task...[1]
• Relay SMB authentication, get a session
• Use a script to install a backdoor
• Pass go, collect $200

1. Hijack a Windows server name to speed this process up
Finding and exploiting web apps

- Web application audits are mostly manual
- Metasploit WMAP modules are helpful
- Import web scan results (NetSparker, Nikto)
- Use generic exploits for custom apps (RFI)
- Platform-agnostic PHP and Java payloads
- Encode normal payloads as .ASP or .DLL
- Leverage session automation scripts
- Exploit XSS using BEEF integration
- Exploit SQL with payload staging
network shares

Quickly find open network shares

• Use smb_enumshares to find SMB shares
• SMB module can use NTLM hashes
• Use nfsmount to identify NFS exports
• Both can work on entire ranges
• Both store results in the database
• View the results with db_notes
ARP, WPAD, and WiFi

- The idea is to “become the network”
- Simple ARP spoofing is still effective
- Become the proxy by becoming WPAD
- Hijack the WiFi using Karmetasploit
- Leverage Metasploit modules
  - Steal stored cookies for any web site
  - Force the target to auto-fill login forms
  - Send back exploits for all web sites
  - Take over network shares & printers
  - Sniff passwords with pSnuffle
Attacking link-local IPv6 hosts

- All modern OSs ship with IPv6 enabled
- Addresses are automatic “link-local” (FE80)
- Reachable by anyone on the same link
- Often bypass non-IPv6 firewalls
- Metasploit is IPv6 ready
  - The Rex Socket library supports IPv6
  - Almost all exploits and auxiliary modules
  - IPv6 specific payloads (reverse/bind)
  - Bind now works through Toredo!
Importing and exporting data

- NeXpose, Qualys, Retina, Nessus (NBE,v1,v2)
- Nmap XML, NetSparker XML, AMap, IP lists
- Metasploit Pro, Metasploit Express
- Consolidate your data in one place
- Work with it through DB* commands
- All-in-one Win32 installation (3.5.0)
- Export back out with db_export
Metasploit today

- Expanding to cover general purpose tasks
- Still useful in a 100% patched environment
- Techniques and tools beat vulnerabilities
- Version 3.5.0 just released!
Questions?