



Tactical Exploitation

“the other way to pen-test “

hdm / valsmith

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
- New tools, fun techniques
- 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 dont 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
 - www.Paterva.com

personnel discovery

- These tools give us
 - Full names, usernames, email
 - Employment history
 - Phone numbers
 - Personal sites

personnel discovery

CASE STUDY

personnel discovery

- Started with just a name and title
- Found online personnel directory
- Found people / email addresses
- Email name = username = target

personnel discovery

DEMO

network discovery

- Identify your target assets
 - Find unknown networks
 - Find third-party hosts
- Dozens of great tools...
 - Lets 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
 - RevHosts PIG/VHH modules:
 - <http://revhosts.net/>

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

CASE STUDY

network discovery

DEMO

firewalls and ips

- Firewalls have gotten **snobby**
 - Content filtering is now common
 - Intrusion prevention is annoying
- Identify and fingerprint
 - Increase your stealthiness
 - Customize your exploits

firewalls and ips

- Firewall identification
 - NAT device source port ranges
 - Handling of interesting TCP
- IPS identification
 - Use “drop with no alert” sigs
 - Traverse sig tree to find vendor

firewall and ips

CASE STUDY

firewall and ips

DEMO

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

- Some new tools
 - W3AF for locating web apps
 - Metasploit 3 includes scanners

application discovery

CASE STUDY

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

client app discovery

- Existing tools
 - BEEF for browser fun
 - Not much else...

client app discovery

- Shiny new tools
 - Metasploit 3 SMTP / HTTP
 - Metasploit 3 SMB services

client app discovery

CASE STUDY

client app discovery

DEMO

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
 - Web pages being uploaded

process discovery

- Existing tools?
 - None :-)
- New tools
 - Metasploit 3 profiling modules
 - More on exploiting this later...

process discovery

CASE STUDY

process discovery

DEMO

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 file transfers

- FTP transfers
 - Active FTP source ports
 - Passive FTP servers
- NFS transfers
- TFTP transfers

attacking mail services

- Four different attack points
 - The mail relay servers
 - The antivirus gateways
 - The real mail server
 - The users mail client
 - File name clobbering...

attacking web servers

- Brute force files and directories
- Brute force virtual hosts
- Standard application flaws
- Load balancer fun...
- Clueless users cgi-bin's are often the Achilles heel

attacking dns servers

- Brute force host name entries
- Brute force internal hosts
- XID sequence analysis
- Return extra answers...

attacking db servers

- Well-known user/pass combos
 - Business apps hardcode auth
- Features available to anonymous
- No-patch bugs (DB2, Ingres, etc)

authentication relays

- SMB/CIFS clients are fun!
 - Steal hashes, redirect, MITM
 - Remote shell, no vuln needed
- NTLM relay between protocols
 - SMB/HTTP/SMTP/POP3/IMAP

social engineering

- Give away free toys
 - CDRROMs, 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

file services

- SMB is awesome
 - Look for AFP exports of SMB data
- NAS storage devices
 - Rarely, if ever, patch Samba :-)

file services

- NFS is your friend
 - Dont forget its easy cousin NIS
- Scan for port 111 / 2049
 - *showmount -e / showmount -a*
 - Whats exported, whose mounting?

file services

- Exported NFS home directories
 - Important target!
- If you get control
 - Own **every node** that mounts it

file services

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

file 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

CASE STUDY

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`

wins services

- Advertise your WINS service
 - Control name lookups
 - Attack other client apps

license servers

- A soft spot in desktop apps
- Computer Associates
 - Bugs and simple to spoof
- FlexLM network services

remote desktops

- RDP
 - Great for gathering other targets
 - Domain lists available pre-auth
 - If not available, start your own:
 - *net start "terminal services"*

remote desktops

- VNC
 - The authentication bug is great :)
 - MITM attacks are still viable
 - Install your own with Metasploit 3
 - *vncinject payloads*

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 :)

trust relationships

CASE STUDY

Hijacking SSH

CASE STUDY

Hijacking Kerberos

CASE STUDY

Hijacking NTLM

CASE STUDY

Conclusion

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