Cain BeEF Hash:
Snagging Passwords Without Popping Boxes

Ryan Linn
SecTor 2009
Overview

- Introduction
- Background
- What are we after
- How do we get it
- What are we talking about
- What makes this different
- What are the tools involved
- Show me!
- Remediation
- Questions?
Introduction

- Information Security Engineer at SAS Institute
- Columnist for EthicalHacker.net
- Founder of OpenHash project
Many organizations have the same problems
- Patch management issues
- Poor password policies
- Legacy applications
- Vulnerable to Social Engineering

Patching is easier to mitigate
- WSUS
- IPS
- HIPS
Background

• What if we could compromise one machine

  • Client side vulnerability
    - Adobe
    - Browser Plug-in
    - Specific exploit targeted at organization

  • Exploit trust relationships within domain
    - Internal websites
    - Employee only content
    - Legacy servers
What are we after

- Access
  - To data
  - To systems
  - To passwords
  - To Something

- How do we get it?
  - Depends!
    - Passwords?
    - Two Factor Authentication?
What are we after

- Hopefully passwords
- How do we get them?
  - Hashdump
  - Social Engineering
  - LM Challenge Hashes
- Wait.. we can't do that
  - Don't know what the challenge will be ahead of time
- BAH.. we know how to fix that!
  - Squirtle
  - Metasploit
How do we get it?

- Step 1: Find a leverage point
  - Some host that is inside the local intranet zone
    - May be ours
    - May be one we exploited
- Step 2: Get traffic to our web server
  - Stored or Reflective XSS by squishy internal web server
    - May be more vulnerable than external boxes
    - Not required to be internal
How do we get it?

- **Step 3: Steal the hash**
  - Static challenge
  - Quietly if possible
    - If it isn't quiet, may alert someone to look at the server

- **Step 4: Crack the hash**
  - Rainbow Tables
    - Cain & Abel
    - rcrack/rcracki
How do we get it?

- Step 4: Crack the hash (cont)
  - Hybrid Approach
    - Plain-text.info
    - John the Ripper
  - Brute force
    - Rarely needed
      - Order pizzas.. best have lots of time
    - May become faster with CUDA & ATI Stream
- Step 5: You win!
What are we talking about?

- Creating a website listener within the trusted zone
- Creating a fake web page that can be referenced via XSS
- Requiring NTLMv1 auth
- Using static challenge to facilitate cracking
  - Allows rainbow tables to be an option
  - Allows for sorted wordlists
What makes this different?

- Using http[s] instead of smb allows for cross platform and cross browser compatibility.
- In corporate environment, more likely to have integrated auth enabled in alternative browsers than UNC paths.
- Individuals without integrated auth/alternative platforms are used to typing in passwords so may catch those.
- Extended tools and techniques to speed up process.
Capturing LM/NTLM Challenge Hashes

1. Rogue attacker machine targets Internal Website, injects stored XSS

2. Domain Member requests webpage

3. Internal Website returns content with XSS pointing at rogue machine

4. Client connects to Metasploit listener on Rogue machine and requests page

5. Metasploit returns HTTP 401 with WWW-Authenticate set to NTLM

6. Domain Member connects to Metasploit with Type 1 Message including Workstation, Domain, and auth flags

7. Metasploit returns type 2 message, with static challenge

8. Domain Member response with information about domain, user, host, LM + Challenge hash and NTLM + challenge hash
Tools Involved

- Access to the local intranet zone
  - Walk in and plug-in
  - Wireless ?
    - aircrack-ng
  - Exploit
    - Metasploit
    - Milw0rm
    - Commercial tools
Tools Involved

- XSS
  - W3af
  - Paros
  - GrendelScan
  - Burp Proxy
  - Tamper Data
Tools Involved

- Hash Capture
  - Metasploit: Pen tester swiss army knife
  - Squirtle: First to present this at Defcon 16

- Password Recovery
  - Cain & Abel
  - Plain-Text.info
  - John
Show me!

- Get on the network
  - Walk In
- Find XSS
  - Find and exploit
- Hook Bots
  - BeEF Injection
- Capture Hashes
  - Metasploit
- Crack password
  - Cain & Abel
  - Plain-Text.info
- We Win
Remediation

- Make it harder
  - Strong password policy
  - Don't store LM hashes
  - Limit local zone
  - NAC NAP paddywack protect your intranet zones
  - Deep Packet Inspection

Secure internal sites like they were outside
Remediation

- Beat the tools available
  - Harder to crack NTLM, few tools support NTLMv2
  - Force NTLMv2 authentication only
  - Not many NTLM tables available
Questions?

- Ryan Linn
  - E-mail: sussurro@happypacket.net
  - Twitter: @sussurro
- EthicalHacker.net
- OpenHash.net
References

- Metasploit - http://www.metasploit.com
- BeEF - http://www.bindshell.net
- Cain & Abel - www.oxid.it
- Plain-Text.info - http://plain-text.info
- Squirtle - http://code.google.com/p/squirtle/
- Samurai WTF - http://samurai.inguardians.com/
- OpenHash Project - http://www.openhash.net
- Google - http://www.google.com
Thanks

- SecTor group for hosting this event
- Tool development teams used today
- HD Moore for code optimization suggestions
- Kurt Grutzmacher for advice with Metasploit module and some of original research
- Brian Wilson (both of them)