Click to edit Master subtitle style

Stamp Out Hash Corruption, Crack All the Things!





Ryan Reynolds

- Manager, Crowe Horwath
- Pentester

Twitter: @reynoldsrb





Jonathan Claudius

- SpiderLabs Security Researcher, Trustwave
- Vulnerability Research
- Twitter: @claudijd





What's inside?

- Windows Hash Extraction
- Story of What We Found
- Windows Hash Extraction Mechanics
- A Different Approach
- Why Are All the Tools Broken?
- Demo
- Patches





licket sertial k about hashes!!!





Goals of Getting Hashes

- Privilege Escalation
- Password Analysis
- Forensics Investigations





Windows Password Hashes

- Two Types of Hashes:
 - LM (Lan Manager)
 - Old Hashing Algorithm w/ Security Flaws
 - Case insensitivity, Broken into 2 Components
 - NTLM (NT Lan Manager)
 - Newer Hashing Algorithm w/ Security Flaws
 - Not salted, but is case sensitive





Windows Password Hashes

- Two Methods to Get Hashes:
 - Injection via LSASS
 - Reads hashes from memory
 - Registry Reading via SAM/SYSTEM
 - Reads hashes from local registry hives





Click to edit Master subtitle style

Story Time...





Failed Attempt 1

- Social Engineering Engagement
 - Gained Physical Access
 - Dumped Hashes on a Bank Workstation

- Failed to Crack
 - John the Ripper
 - Rainbow Tables





Failed Attempt 2

- Internal Penetration Assessment
 - Popped a Shell via Missing Patch
 - Dumped Hashes on System

- Fail to Crack
 - Rainbow Tables (via all LM Space & French)
 - Pass the Hash (PTH)





Example Hashes

- Via Registry (Metasploit)
 - LM: 4500a2115ce8e23a993o3f76oba6cc96
 - NTLM: 5cobd165cea577e98fa923o8f996cf45
- Via Injection (PwDump6)
 - LM: aad3b435b51404eeaad3b435b51404ee
 - NTLM: 5f1bec25dd42d41183dof45obf9b1d6b





Metasploit Framework

Overview Activity Roadmap Issues Wiki Repository

Bug #4402

Hashdump script/post module breaks with passwords greater than 14 When using "run hashdump" or the post/windows/gather/hashdump module on a Windows 2008 server with a password of larger than 14 characters, the hash that is returned is incorrect.





"Our Powers Combined..."

- Beers
- Hacking
- More Beers







Whereite to Hashes Live?





Where Do Hashes Live?

- HKLM\SAM
 - Store security information for each user (including hash data)

- HKLM\SYSTEM
 - Stores the SYSKEY ("salts" the SAM information for security purposes)





What The Registry Looks Like

- HKLM\SAM\SAM\domains\account\users\
 - Users: 000001F4, ..1F5, etc.

Name	Type	Data
(Default)	REG_SZ	(value not set)
F	REG_BINARY	02 00 01 00 00 00 00 00 8d
V V	REG_BINARY	00 00 00 00 bc 00 00 00 02





What's Inside These Values?

- For each user, we have two values...
 - "F" Binary Data
 - Last Logon, Account Expires, Password Expiry, etc.
 - "V"- Binary Data
 - Username, LM Hash Data, NT Hash Data, etc.





A Closer Look At Raw Data

Raw Data w/ LM & NTLM Data

```
...0000AAAAAAAA0000BBBBBBBB00000...
```

Raw Data w/ just NTLM Hash Data

```
...00000000BBBBBBBBB000000000000...
```





Registry Extraction Tools

- Metasploit Hashdump Script
- Creddump
- Samdump2
- Cain and Able
- Pwdump7
- FGDump 3.0
- Others





Current Parsing Logic

OFFSET

HASH DATA

LM & NTLM

If size > 40 bytes?

NTLM

Else If size > 20 bytes?

None

Else





Click to edit Master subtitle style

The "Flaw"





Remember these?

- Via Registry (Metasploit)
 - LM: 4500a2115ce8e23a993o3f76oba6cc96
 - NTLM: 5cobd165cea577e98fa923o8f996cf45
- Via Injection (PwDump6)
 - LM: aad3b435b51404eeaad3b435b51404ee
 - NTLM: 5f1bec25dd42d41183dof45obf9b1d6b





The "Flaw"

HASH DATA **OFFSET** DATA++ If size > 40 bytes? LM & NTLM Mana





The "Flaw"

BAD

- ...0000AAAAAAAA0000BBBBBBBB00000...







Root Cause?

How do we get "DATA++"?

OFFSET

HASH DATA

DATA++

- By following Microsoft best practices
 - Set Password History
 - No LM Hashes





Raw Look at "V" Data Structure

HKEY LOCAL MACHINE\sam\sam\domains\account\users\00003ed REG BINARY 000000000000000000844400 0000000D40000002000100D4000000A00000000000000E0000000 REG BINARY 00000000C8010000840000000000000001001480B400000C40000014000000440000002003000 020000002C014004400050101010000000000100000002C01400FFF1F000101000000000050700000020070000400000 .010000000000010000 0102000000000052000000 F070F00010200000000 0000240044000200010500000000000500000003FAD1462235F636B07E53B2BED0300001020000 0700000010001009AC412C7DA10C788963DF9DF7E6B5EF401000100B0FD8B04845B3E6836EC62ED D3EC84CA0100010015F478C0D71D99AB56AB61F0921DE0EF9C21D096BE07202EDF579D32EF31DF17 8E47CFC180A85D50451DBBCD73DB89F3E81DC94989A51D23610F8669762EBFD5DF73B40F40B95683 5E95719E0C18D4B27CAC2754CA807AD818CB4C27677A52621BA0A5AFB8CAA34AC3DFCDA8054B9395 14CD7E8A51840220C7E1AF65C0865C01 0181584F4E2D0652C0100010030077263 DATA++ 8DEB345851FF5B0CCA0123BB9B5C279A 3843488CD968264658858D5560A2047DB 06FC11269C826D74B1EA6C1F2B6293F952 71C091EDDC0C054E6A47881065C4F38C5C F888781246B88769BCE6E08E3ADBC06193EF250EC43775C8A5AE558A44F87484AED9BE0B73464DCD



A257CC67



How often does this occur?

- Newer OS's do not store LM
 - Windows Vista and newer
 - LM can be disabled by a proactive Sysadmin
- Password histories set through GPO





In an ideal world...

- We would want...
 - LM Exists?
 - NTLM Exists?
 - Parse correct hash data 100% of the time





Raw Look at "V" Data Structure

HKEY LOCAL MACHINE\sam\sam\domains\account\users\000003ed REG BINARY 000000000000000000844400 REG BINARY 000000 .00D400000 00E0000000 0A0000000000000EC000000000000000HEADER00000000000000HEADER00000000 00000000C8010000840000000000000001001480B400000C40000014000000440000002003000 0200000002C014004400050 0100000000002C01400FFFF1E 07000000020070000400000 0100000000000100000 0102000000000052000000 070F0001020000000000 0000240044000200010500000000002 50000003 FAD1462235 F636B07E53B2BED0300001020000 00000005200000002002000001020000000000520000000200200074006500730074003200000 0700000010001009AC412C7DA10C788963DF9DF7E6B5EF401000100B0FD8B04845B3E6836EC62ED D3EC84CA0100010015F478C0D71D99AB56AB61F0921DE0EF9C21D096BE07202EDF579D32EF31DF17 8E47CFC180A85D50451DBBCD73DB89F3E81DC94989A51D23610F8669762EBFD5DF73B40F40B95683 5E95719E0C18D4B27CAC2754CA807AD818CB4C27677A52621BA0A5AFB8CAA34AC3DFCDA8054B9395 14CD7E8A51840220C7E1AF65C0865C015 181584F4E2D0652C0100010030077263 843488CD968264658858D5560A2047DB 8DEB345851FF5B0CCA0123BB9B5C279A4 06FC11269C826D74B1EA6C1F2B6293F992E0J00D C091EDDC0C054E6A47881065C4F38C5C F888781246B88769BCE6E08E3ADBC06193EF250EC43775C8A5AE558A44F87484AED9BE0B73464DCD A257CC67





A Different Approach

- "V" hash 4 byte headers for LM & NTLN
 - ox4 (4 bytes) = Hash Not Present (false)
 - ox14 (20 bytes) = Hash Present (true)

No more guessing!





A Different Approach

OFFSET

HASH DATA

DATA++

LM & NTLM

If LM.exists? && NTLM.exists?

NTLM

Else If NTLM.exists?

None

Else





A Different Approach

GOOD LOGIC

- ...0000AAAAAAAA0000BBBBBBBBB00000...
- ...00000000BBBBBBBBB000000000000...



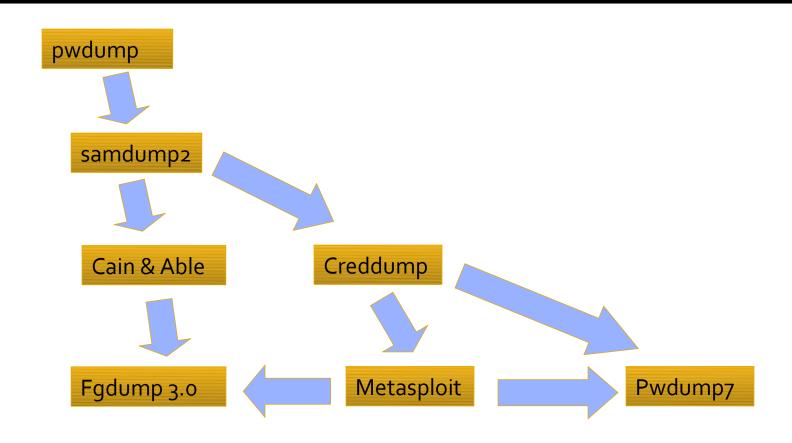


tools broken?





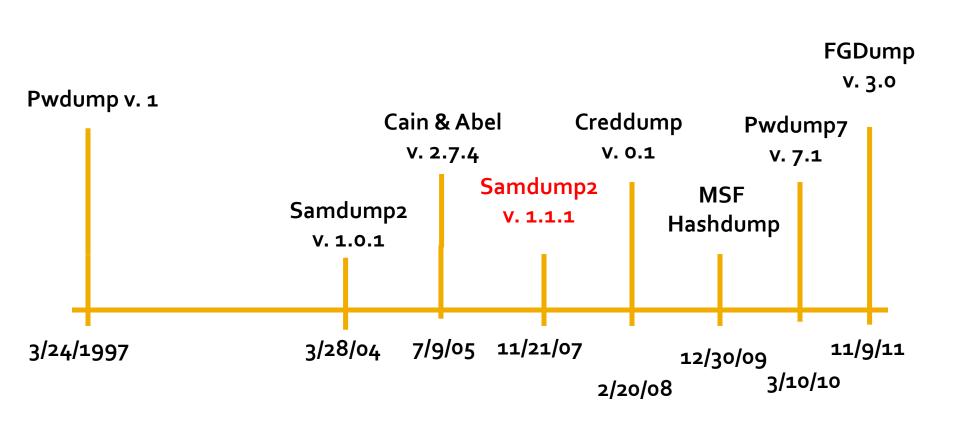
Who's Patient Zero?







Tool Timeline







Take Away

- Reverse engineering is hard
 - Exhaustive testing is time consuming

- Leveraging code is helpful
 - Fully reusing code is not always good

Open source let's others learn and help fix!





Click to edit Master subtitle style

Demonstration





Click to edit Master subtitle style

Patches!!!!





Patches

Affected Tools	Patched?
Creddump	Yes
Metasploit's Hashdump Script	Yes
L0phtcrack	Working with Author(s)
Pwdump7	Working with Author(s)
FGDump 3.0	Working with Author(s)
Samdump2	Fixed in v 1.1.1
Cain & Abel	Working with Author(s)





Click to edit Master subtitle style

Questions?



