Still Passing the Hash 15 Years Later…

Using the Keys to the Kingdom to Access All Your Data

Alva ‘Skip’ Duckwall
Chris Campbell

Help Us Get Better!

Please Fill Out The Speaker Surveys!

Do You Know Who I Am?

Alva 'Skip' Duckwall

- Full Scope Pen-Tester for Northrop Grumman
- GSE, OSCP, CISSP, CISA, RHCE, among others
- 19 Years Working with Linux

Chris Campbell

- Full Scope Pen-Tester for Northrop Grumman
- MSIA, OSCP, CISSP, CISA, MCSE, among others
- Former Army Signal Officer

Shameless Plug

Patches available from:

http://code.google.com/p/passing-the-hash/

Also Chris and I will be blogging about how to use the various tools in the coming weeks:

http://passing-the-hash.blogspot.com/

Twitter @passingthehash @obscuresec (chris)

A Little History

In 1997 Paul Ashton posted the theory about the first "Pass the Hash" attack to NTBugTraq against the Lan Manager protocol

The result?

A modified Samba client that accepts LM hashes instead of a password to access a remote file share.

Your Data is Your Kingdom

Business Relies on Data

- Email
- Files on a share
- Intranet applications (Sharepoint)
- Databases

What would happen if somebody else had control of your data?

Typical Day at the Microsoft Office

Regular user's day:

- Login
- Check email
- Visit the intranet

Sysad's day - all of the above plus:

- Log into a database
- Manage servers / services

All of this and the password only gets typed once

The Windows Single Sign On

Once a user logs in, their credentials are cached locally and reused by the OS on the user's behalf

- User prompted parely after initial login
- Password hashes are cached locally
- Plaintext as well (Digest Auth)

Windows Password Hashes

Passwords hashed 2 different ways:

- LM (Lan Manager) Hash
- NTLM Hash

Modern versions of Windows don't save LM hashes, however they are still calculated and stored in memory if the password is 14 characters or less, even if they aren't saved...

Logging In

When a user logs in, a security token is created containing:

- Security IDentifiers (SID) for the user
- SIDs for all groups the user is a member of
- Default ACLs (if no other ACLs apply)
- Per user audit settings
- Impersonation level

Impersonation

Tokens have 4 different security levels:

- Anonymous
- Identification
- Impersonation
- Delegation

Interactive logins (Windows Console) -> delegation tokens

Non-interactive (Network Login) -> impersonation tokens

"Incognito" tool / module allows for a lot of post exploitation fun with tokens allowing a malicious user to steal other identities of people logged into a server...

Windows Authentication Methods

Kerberos

- Uses tickets
- Tickets can be reused for lower overhead

NTLM

- Challenge-response protocol
- Every transaction authenticated, high overhead

Digest Authentication

- Hashed password (usually with MD5)
- Requires plaintext password to be stored

Windows Authentication Methods (contd)

Smart Cards

- Two-factor authentication, bolted onto kerberos
- Only for interactive (console) sessions
- Hashes still stored on the back end

Keyfobs, etc (SecurID)

- Two-factor authentication
- Only used for interactive logons
- Radius (or radius-like) used on the back end - gives thumbs up/down on 2nd factor
- Password hashes used on the back end

Kerberos vs. NTLM

Kerberos

- Default
- Both client/server must be in the domain
- Reliance on DNS

NTLM

- Used if client/server not in the domain
- Used if addressed by IP

Services that Can Use NTLM

- Web Services
  - Sharepoint
  - Custom web apps (.net based)
- Exchange
  - MAPI
  - IMAP / POP3
  - SMTP
- Things that can't join the domain
  - Appliances
  - Printers / copiers / digital senders

Difficult to Eliminate NTLM

Only recently implemented

- Requires windows 7 for all clients
- Domain must be at 2008R2 functional level

Probably will break things

- Copiers / printers / digital senders
- Web apps / appliances
- Internet / customer-facing applications
- Anything not in the domain

Passing the Hash

Windows authentication protocols operate on password hashes

- Kerberos uses the NT hash as encryption keys
- NTLM uses password hashes as part of the challenge response
  - Password hash along with nonce hashed to confirm knowledge of the password
  - Excellent detailed descriptions of the process available at the Davenport website

Knocked Over the DC, Got the Hashes, Now What?

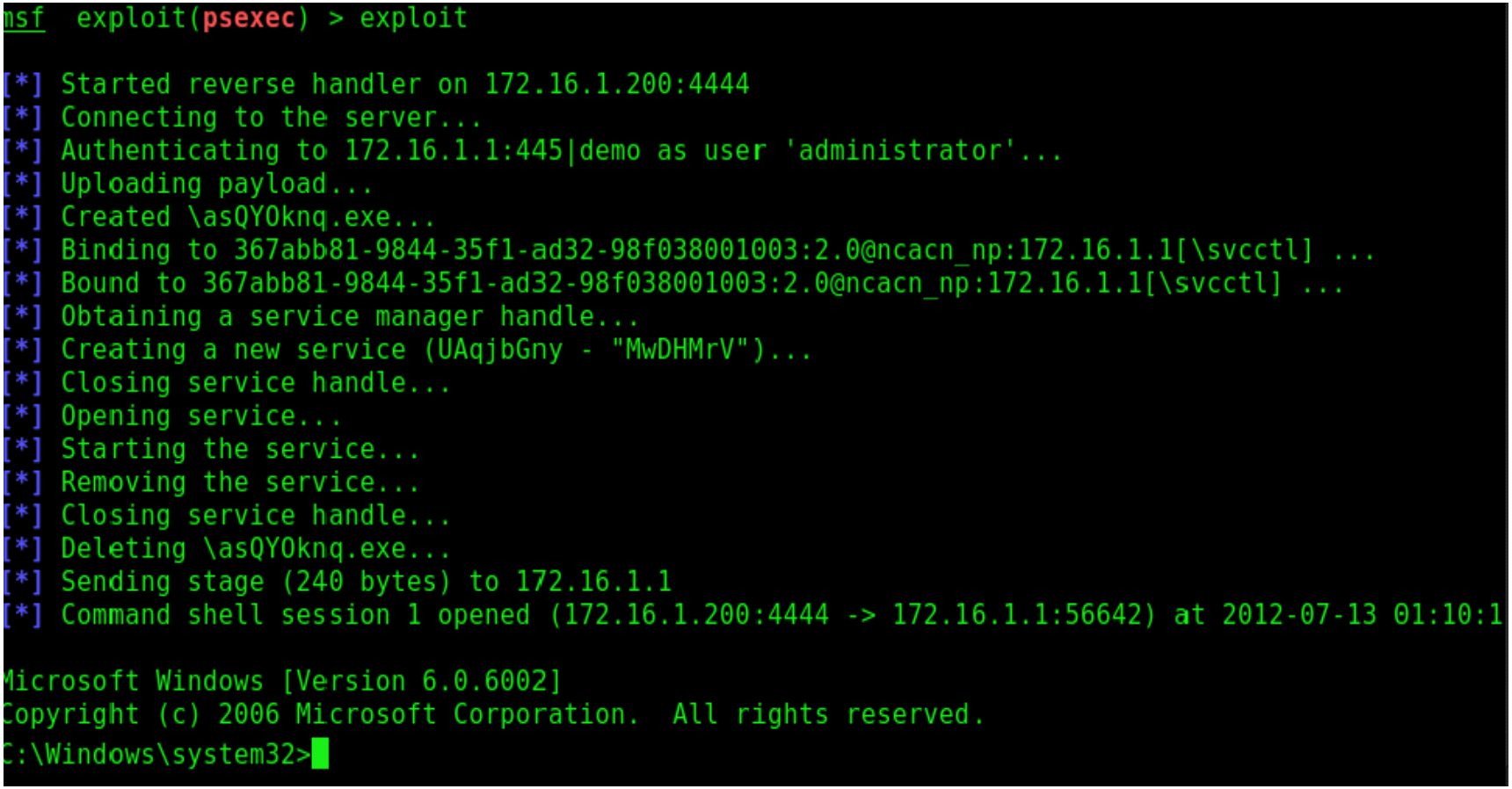
Maybe crack the passwords?

- Works for weak or easily guessed passwords
- Can look impressive if wildly successful (>50%)
- Might not be allowed by the rules of engagement
- Lacks C-level “wow“-factor

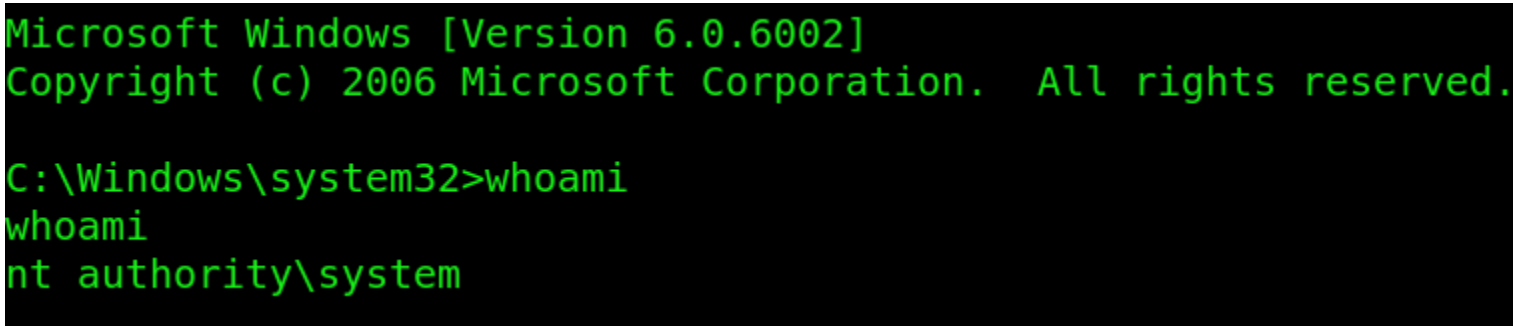
Perhaps a Traditional Pass The Hash Attack?

```
msf > search smb hash

Matching Modules
================

   Name                                  Disclosure Date          Rank    Description
   ----                                  ---------------          ----    -----------
   auxiliary/admin/oracle/ora_ntlm_stealer  2009-04-07 00:00:00 UTC  normal  Oracle SMB Relay Code Execution
   auxiliary/admin/smb/upload_file                                  normal  SMB File Upload Utility
   auxiliary/server/capture/smb                                     normal  Authentication Capture: SMB
   auxiliary/spoof/nbns/nbns_response                               normal  NetBIOS Name Service Spoofer
   exploit/windows/smb/psexec            1999-01-01 00:00:00 UTC  manual  Microsoft Windows Authenticated User Code Execution
```

Super Sexy for Pentesters...



For C-Level Folks... Not so Much



“I don’t know anybody named NT System in my company…”

Boring!

"You logged into the Domain Controller, but you can't read my email. We're secure, right?"

Remember, the crown jewels of the network is the **data**. Nobody gets excited unless that's put at risk.

Slightly More Interesting PTH

Access File Shares

- Find all sorts of interesting things
  - Personally Identifiable Information (PII)
  - Database backups
  - Saved email
  - Inventory information
  - Design specs
- Accessing proprietary information starts getting some attention
- We can use a modified samba client (more later)

Accessing Data

Many Windows applications “Pass The Hash” to access data.

Why can't we?

Demo Domain Assumptions

- Sitting inside the domain
- Already dumped the hashes (post exploitation)
- We care about 3 people
  - Alice
  - Bob
  - CEO

Our Windows Attack Platform

- Windows 7 – fully-patched
- Not in the domain
- No AV
- No Host-Based Intrusion Detection System
- Latest version of the Windows Credential Editor (WCE) by Hernan Ochoa
- Client software we want to use

WCE Overview

Written by Hernan Ochoa of Amplia Security

- Successor to the “Pass The Hash Toolkit”
- Capable of examining memory to list hashes for all logged in users (-l)
- Can be used to inject or dump Kerberos tickets (-k / -K)
- Can be used to change the credentials of the currently logged in session (-s)
- Can be used to launch a program with different credentials in a new session (-c)

Why Not CMD.EXE?

Running WCE with both '-s' and '-c' allows us to create a new process running as an arbitrary domain user with their hash.

Using cmd.exe as the process, any command executed from this DOS box will be running as that user, ***even if the local computer isn't on the domain***!

Or explorer.exe

Using task manager, We kill explorer.exe and restart it using WCE.

This allows us to browse file shares using explorer.exe as the user. Also, any programs started with the "Start Menu" automatically get launched as that user as well...

Now What?

Launch IE at the local Sharepoint site.

Internet Explorer might need to be configured to automatically pass credentials:

1. IE config: security -> custom level for the zone -> automatic logon only in intranet zone
2. Add Sharepoint to the “Local Intranets Group”

How About Outlook?

Use Outlook to access email/calendar for our impersonated user.

1. Enable profiles in the mail control panel: control panel -> mail -> always prompt for profiles
2. Create a profile for each user

Access File Shares

We can either use the explorer.exe trick or use net commands to mount / browse file shares.

Note: The '/savecred' doesn't work with hashes. Apparently it only saves a plaintext password... who knew?

MS SQL

Simply launch the MSSQL client and point it at a database to log in, assuming it uses Windows Authentication...

Access or monkey with the data, depending on the ROE of course...

Sysadmin Tasks

Simply run from the command line:

- PSExec (Sysinternals)
- WMI
- PowerShell
  - new feature in Win8, Web PowerShell
- WinRM (if enabled)
- Active Directory Users and Computers
- Computer Management

Windows Demo

Pictures worth a thousand words...

Demo Gotcha's

Outlook 2007 inconsistent

- One demo environment worked fine, another didn't
- Outlook 2003 worked perfectly ;-)

ADUC couldn't assign passwords, but could change group membership, create computer accounts

Demo Gotcha's (contd)

Can't open Multiple GUI apps as multiple users at the same time (IE/Outlook)

Probably just spawns another thread rather than another process

It Works, But...

Obviously Windows behaves strangely if you do this... expect other magical failures or side effects!

What About Linux?

Meh, I'm a Linux guy...

How about we do all of that with Linux instead?

The Foofus Patch

The previously mentioned modified version of Samba was patched by JMK of Foofus.net.

- Allows us to set an env. variable with the password hash we want to substitute
- Substitutes the hash in all the appropriate places for NTLM authentication

An Additional Technique We Added

Instead of the env. variable, the hash can be specified as the password as long as it's in one of 2 forms:

- LM:NT (65 chars)
- LM:NT::: (68 chars, thanks JMK for the suggestion)
- If the password is 65 or 68 characters long, substitute the hash

Benefits of the New Technique

- Easier to use in scripts - just change the password

- Allows us to pass hashes in GUI programs without the need to kill and reset environmental variables

Anatomy of a Patch

- Find where the application hashes the password in the source code (grep –i md4)
- Check to see if the password is 65 or 68 characters
- If so, convert the 32-byte NT Hash into a 16-byte array by converting 2 hex nibbles into a byte, then substitute

Samba - Just for Shares, Right?

- Libraries for Interfacing with MS DCE/RPC
- Utilities for managing Windows domains / users

Multiple 3rd party programs link in with Samba for access to MS DCE/RPC. Patching Samba will patch downstream programs...

We are releasing "The Pass the Hash Rosetta Stone". It's a list of Samba commands and their corresponding Windows net commands for common tasks.

Utilities That Link with Samba

Winexe

- PSExec Clone (32/64 bit)

WMI

- Run basic WMI queries from Linux
- Includes blind command execution via WMI

Openchange

- Open-source framework to interface with Exchange from Linux

What About Firefox?

By default Firefox tries to query the local OS for NTLM creds if enabled using Samba

Or

Use Firefox's built-in implementation based on Davenport

- Patched Firefox's NTLM implementation with the 65/68 character Hash Patch
- Enabled in "about:config"
- network.auth.force-generic-ntlm -> true

What About MSSQL?

FreeTDS

- Provides libraries to interface with Sybase / MSSQL
- NTLM authentication code based on Davenport (Guess what we already have code for?)
- Combine with SQSH (SQL Shell) to gain interactive access to MSSQL for Linux

Linux Demo

Defenses

Try to Eliminate the Use of NTLM

- Difficult to do
- Requires 2008R2 domain functional level
- All clients need to be Windows 7
- Will break things that can't do Kerberos
  - Printers / copiers / digital senders
  - Appliances / NAS devices
  - Can’t join new computers to the domain

Of course, a “Defense-in-Depth” approach to prevent compromise of the DC works too!

Kerberos Is Safe, Right?

Kerberos uses NT hashes for encrypting tickets to principals

- Discussed in more detail in the whitepaper
- Short version: Compromising the encryption keys is still **very bad**(tm)!

Quick Recap

Windows + WCE + Hashes = Access To Data

- Native Windows tools work albeit oddly at times
- Definitely not exactly how Windows wants to work

Linux + PTH Tools + Hashes = Access To Data

- Open-source tools FTW!
- Exchange, MS SQL, Sharepoint, File shares and WMI

Shouts!

Aaron, Pete, Mike, Jeff, Brian, Don, Devin, Sean, jcran, Will, Damien, Mubix

JMK at foofus for the 68 character suggestion

Questions?

Help Us Get Better!

Please Fill Out The Speaker Surveys!