SHAREENUM: WE WRAPPED SAMBA SO YOU DON'T HAVE TO

Lucas Morris @lucasjmorris
Michael McAtee @michael.mcatee

About Us

- Lucas Morris
  - Manager at Crowe Horwath LLP
  - “Manager”, Pentester, Code Monkey
- Michael McAtee
  - Senior Consultant at Crowe Horwath LLP
  - Pentester, SysAdmin, [something funny here]

About Us

- **Lucas Morris**
  -  => emperorcow@gmail.com
  -  => @lucasjmorris
  -  => github.com/emperorcow
- **Michael McAtee**
  -  => jmmcatee@gmail.com
  -  => @michaelmcatee
  -  => github.com/jmmcatee
- https://github.com/emperorcow/shareenum

Overview

- SMB / CIFS Refresher
- Windows Permissions Refresher
  - (DACLs, SDDL, ACEs, etc.)
- The Problem With Scanning Today
- What Share Scanning Is Good For
- Tools!

Windows File Sharing

- CIFS
  - Basically SMB 1.0
    - Mostly open & is the published spec that others implement to

- SMB
  - SMB 1.0: Windows XP, Server 2003 R2, & Prior
  - SMB 2.0: Windows Vista, Server 2008, & Above
  - SMB 2.1: Windows 7, Server 2008 R2, & Above
  - SMB 3.0: Windows 8, Server 2012, & Above
  - SMB 3.02: Windows 8.1, Server 2012 R2

Types of Shares

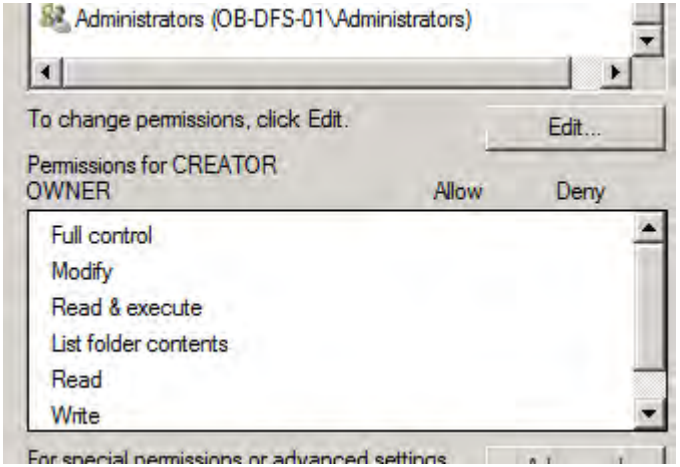
- Special Types of Shares (IPC$, ADMIN$, C$)
  - $ = Hidden… usually
  - IPC$ = **I**nter**P**rocess **C**ommunication
  - ADMIN$ = C:\Windows\System32
  - C$, D$, etc. = Drive Shares
  - These are default an rarely removed
    - Although you can disable them

      (http://support.microsoft.com/kb/954422)

Shares - Permissions

- **Discretionary Access Control List (DACL)**

```
REVISION:1,OWNER:2K8-WIN7-01\ShareEnumUser1,
GROUP:PROD\Domain Users,
ACL:2K8\shareenumdomuser1:0/16/0x001f01ff
```



- **Access Control Entry (ACE)**

```
BUILTIN\Administrators:0/0/0x001f01ff
```

Shares - Permissions

- Shares
  - Read
    - View files & folders
    - View files & folder contents
  - Change
    - Add files & folders
    - Change data in files
    - Delete folders and files
  - Full Control
    - Change NTFS permissions

Shares - Permissions

- NTFS
  - Full Control
  - Modify
  - Read & Execute
  - List Folder Contents
  - Read
  - Write
  - Special Permissions
    - …

Shares - Permissions

- Special Permissions
  - Traverse Folder/Execute File
  - List Folder/Read Data
  - Read Attributes
  - Read Extended Attributes
  - Create Files/Write Data
  - Create Folders/Append Data
  - Write Attributes
  - Write Extended Attributes
  - Delete Subfolders and Files
  - Delete
  - Read Permissions
  - Change Permissions
  - Take Ownership

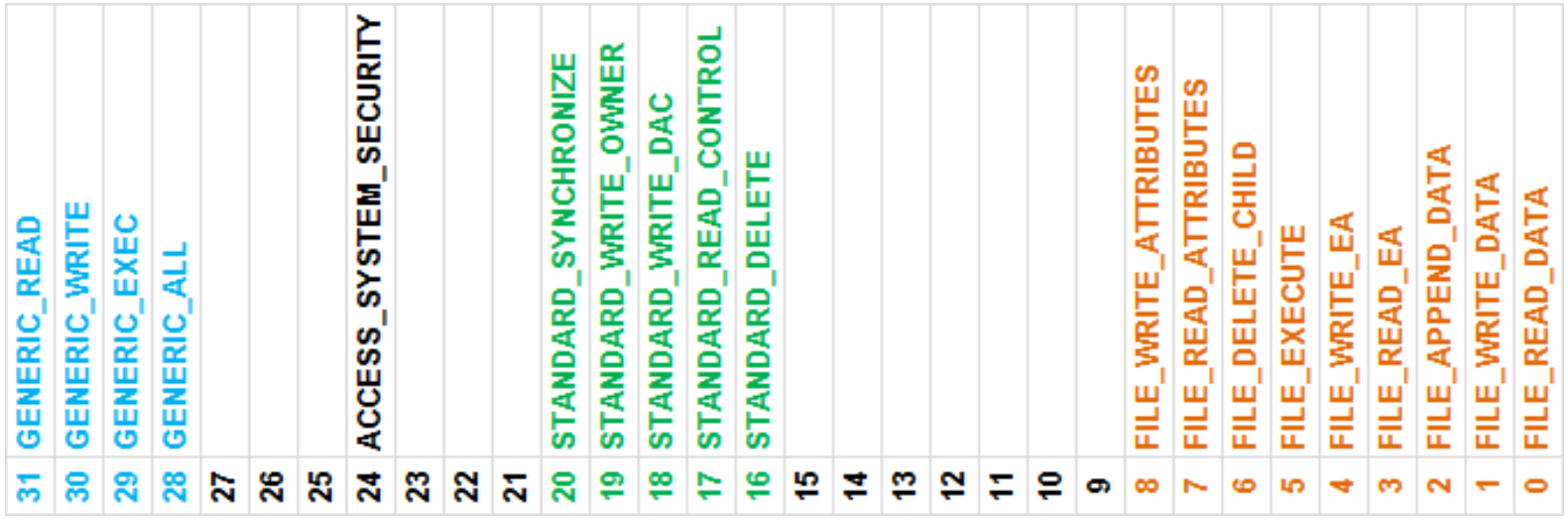
Shares - Permissions

- Attributes
  - READONLY
  - HIDDEN
  - SYSTEM
  - ARCHIVE
  - TEMPORARY
  - COMPRESSED (Directory Only)
  - OFFLINE
  - NOT_CONTENT_INDEXED

- Extended Attributes
  - Custom and starting to be used in Windows 8

Shares - Permissions

- **Access Masks**
  - Generic Access Rights
  - Standard Access Rights
  - File and Directory Access Rights



- **DOS Mode Flags:** Read Only, Hidden

The Problem

- Share scanning can be a pentester's best friend

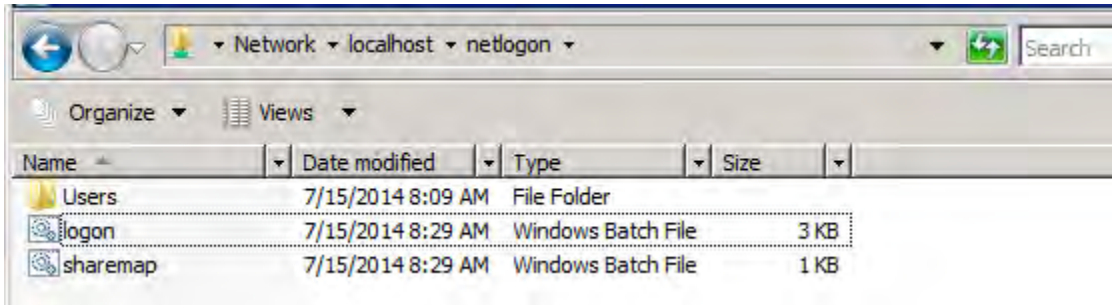
- But…
  - Current tools have a variety of issues
    - Does not support all authentication mechanisms (NTLMv2 & NTLMSSP)
    - Can be very noisy, get us caught
    - S…L…O……W
    - Only pulls information at the top level of the share

Why We Scan Shares

- Sensitive Data (Obviously!)
  - \HR
  - \IT
  - \Backups
  - \Source
- System Fingerprinting
  - What kind of shares does this system have?
  - What does that tell me about the system?

Why We Scan Shares

- Recon
  - NETLOGON & SYSVOL



  - Windows Deployment Services
    - Images and Credentials

Why We Scan Shares

- Credential Reuse
  - Is the local administrator password reused?
  - Do all systems have their local administrator renamed to “AdminWhatAdmin” and have the same password?
  - Does the local “ITHelpDesk” account exist everywhere with a password we’ve found?

Why We Scan Shares

- Local Administrator Access
  - Where Do I Have Admin on a box?
  - Does “Domain Users” have Admin somewhere?
  - What about a single user?

Share Scanning Tools

- **Nmap NSE (smb-enum-shares)**
- **SysInternal's ShareEnum**
- **Nessus**
- **Metasploit**
- **SMBClient**
- **WinShareEnum** (github.com/nccgroup/WinShareEnum)
- Manually though ***explorer*** or ***net use***

Our Tool

- Why implement our own protocols, someone else already has… Samba.
- We're using the same libraries as smbclient, but its much faster to go native than parse command line output.
- Supports the same authentication methods that Samba does (NTLMv2 & NTLMSSP!)

Our Tool

- Gathers DACLs and parses ACEs for each object
- Able to recursively load subdirectories and files
- CSV output so you can filter easily
- Supports Anonymous, Regular Creds, and Pass the Hash

Demo

- Or a video of a demo…

- Demo 1: Local Administrator Password Reuse
- Demo 2: Sensitive Shares
- Demo 3: Recursively enumerating a share

https://www.github.com/emperorcow/shareenum

Questions?

Also, if you know about the Samba RPC and IDL code, we'd love to buy you a beer.

The End

- **Lucas Morris**
  -  => emperorcow@gmail.com
  -  => @lucasjmorris
  -  => github.com/emperorcow
- **Michael McAtee**
  -  => jmmcatee@gmail.com
  -  => @michaelmcatee
  -  => github.com/jmmcatee
- https://github.com/emperorcow/shareenum