Module 35  
(Exploiting Windows Systems II)

- In this Module, you'll find out a little more about exploiting Windows systems. You'll know about the most common method of guessing passwords using smb. You'll become familiar with the primary countermeasures to password guessing. You'll find out about LanMan passwords and see how Rainbow tables work. You'll also find out about a few tools that can be used to crack LanMan passwords.
Remote Password Guessing

• Usually done through SMB (TCP ports 139 and 445). Often blocked by firewall.

• Done via password guessing on remote share mounts.

```bash
C:\> net use \192.168.202.44\IPC$ * /u:Administrator
Type the password for \192.168.202.44\IPC$:
The command completed successfully.
```

• Automate on Windows

```bash
FOR /F "tokens=1, 2*" %i in (credentials.txt) do net use \target\IPC$ %i /u:%j
```

• To find out how FOR works:

```bash
FOR /? 
```
Password Guessing Countermeasures

- Restrict tcp ports 135 (MSRPC), 139 and 445 (SMB), and 3389 (TS) at the firewall.
- Use host-resident Firewall to restrict access.
- Disable unnecessary services
- Enforce the use of strong (long) passwords
- Set an account lockout threshold and apply it to the administrator account.
- Log account logon failures.
Network Password Exchange Eavesdropping

- Guessing is hard work! Why not sniff.
- Requires access to network packets. (Wireless can provide this. Switches and routers can be hacked. Physical access can provide a connection.)
- Many networks still support LM (LanMan) and NTLM password encryption.
LanMan Passwords

- Character limit: 14
- Password converted to uppercase.
- Password is null-padded to 14 bytes and cut into two seven byte halves.
- Only 69 characters available for the password, so only have $69^7$ unique passwords.
- No salt is used, so this is subject to pre-computed dictionary attack.
- Rainbow Tables are a creative way to represent this kind of information.
Rainbow Tables

- The problem with computing and storing hashes is that it takes a lot of space \(2^{43}\) possible LM passwords.
- The Rainbow Table Plan is based on a trick attribute originally to Martin Hellman.
- It uses two functions \(H\), the hash function, and \(R\), the reduction function.
- The reduction function translates a hash into a possible key to be hashed.
Rainbow Tables Plan

- Starting with a hash, apply R followed by H some fixed number of times, and finally R. This yields a hash chain.
- Store the ends and the beginnings of every hash chain.
- Upon encountering a new hash, apply R (possibly followed by H and R repeatedly) until you find an word at the end of a chain.
- Then start at the beginning of that chain until you encounter the hash you presented initially.
- Failure modes exist (colliding chains, for example)
Tools for password cracking

- John the Ripper Jumbo (enhanced version of John)
- L0phtcrack, Cain (Massimiliano Montoro – www.oxid.it)

If you see this icon on your Windows box, be very suspicious!
If you can take only one tool: Cain

- WEP Cracking
- VOIP Decoding
- ARP Spoofing
- Hash calculation
- Traceroute
- Password Decryption
- Password Sniffer
- etc., etc.