Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

System Hacking

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Password Cracking

- Start of the “breaking in” process
- Passwords are usually stored as hashes
- Passwords that are longer are more difficult to crack
- Dictionary Attacks- uses a word list to test against the hash
- Brute Force – every possible combination of character used
- Hybrid, Syllable, Rule-based are other types
- Hashcat is a good tool for cracking passwords

Packet Sniffing

- The process of capturing network traffic in the form of packets with a program like Wireshark and then analyzed later to find sensitive information
- Anything using clear-text is vulnerable
  - Telnet, FTP, SMTP, rlogin

Man-in-the-Middle

- A third party comes in the middle of two parties that are trying to communicate with each other
- Telnet and FTP are vulnerable
- SSL Strip
- Burp Suite
- Browser Exploitation Framework

Replay Attack

- Packets are captured using a packet sniffer
- Packets can be placed back on the network
- Usually in the form of a password
- Valid credentials are replayed

Active Online Attacks

- Password Guessing
  - People often do not change default creds
  - Birthday, dog's name, spouse's name, common words
- Trojans, Spyware, and Keyloggers
- Hash Injection

Offline Attacks

- Precomputed Hashes or Rainbow Tables
- Generating Rainbow Tables
- Creating Rainbow Tables
- Working with RainbowCrack

Distributed Network Attacks

- Using multiple computers to do something such as cracking a password.
- Drops form larger pools
- Millions of computers could be used

Obtaining Passwords

- **Default Passwords**
  - http://cirt.net
  - http://default-passwords.info
  - http://www.passwordsdatabase.com
  - https://w3dt.net
  - http://open-sez.me
  - http://securityoverride.org
  - http://www.routerpasswords.com
  - http://www.fortypoundhead.com
- **Guessing**
- **USB Password Theft**
  - PSPV
  - USB rubber ducky from Hak 5

Microsoft Security Accounts Manager

- Database the stores security principals
- Credentials
- Passwords
- Only works when system is powered off

Windows Passwords stored in SAM

- Stored in hash format
- LM/NTLM hashing mechanism
- C:\windows\system32\config\SAM
- Only works on systems older than Windows XP
- Tools to crack SAM password
  - Ophcrack
  - L0phtCrack

NTLM Authentication

- **NT LAN Manager**
  - **Protocol exclusive to Microsoft**
  - **Should be phased out**
  - **Security Support Provider**

Kerberos

- **Protocol consists of the following:**
  - **Key distribution center**
  - **Authentication Server (AS)**
  - **Ticket granting Server (TGS)**
  - **A ticket is required to use a system with Kerebos**
  - **First authenticate with the AS, creating a session key based on your password together with a value representing the service you're connecting to.**
  - **This request serves as the TGT (ticket granting ticket)**
  - **Access the server with the TGT through the TGS**

Privilege Escalation

- **Horizontal Escalation**
  - **Hack a user with the same privileges**
- **Vertical Escalation**
  - **Hack a user with higher privileges such as admin**
- **Tools**
  - **Active Password Changer**
  - **Trinity Rescue Kit**
  - **ERD Commander**
  - **Windows Recovery Environment**
  - **Password Resetter**

Executing Applications

- **Backdoors**
  - **Rootkits, trojans, remote access tools**
- **Crackers**
  - **Cracking code or obtaining passwords**
- **Keyloggers**
  - **Sniffs keyboard data to obtain all text typed on a keyboard**
- **Malware**
  - **Software to capture info, alter or compromise a system**

Planting a Backdoor

- Can run commands remotely
- PsTools Suite
  - PsExec
- PsExec
- PDQ Deploy
- RemoteExec
- DameWare
- Netcat

Using Netcat

- **Nc –l –p 1313**
  - **Tells netcat to listen on a specific port**
- **Nc <target ip address> 1313**
  - **Initiate connection with the target**
- **A console window will appear**

Covering Your Tracks

- Disabling Auditing
  - Auditpol
  - Auditpol \\<ip target address> /clear
  - Tools
    - Dump Event Log, ELSave, WinZapper, Ccleaner, Wipe, MRU-Blaster, Tracks Eraser Pro
- Data Hiding
- Alternate Data Streams
  - Part of NTFS
  - Hide the file: type file.exe > hideinhere.doc:file.exe
  - Get the file: start hideinhere.doc:file.exe
  - Hard to detect

Summary

- Understand the process of gaining access to a system
- Know the different types of password cracking
- Understand the difference between horizontal and vertical privilege escalation
  - Horizontal – hacker has same level as another regular user
  - Vertical – hacker gains administration rights
- Know the methods for covering your tracks
  - Data hiding
  - Destroying logs