Module - 5
System Hacking

1. **Gaining Access :**
    1. **Password Attacks :**
        1. Cracking :
            - Revealing a password from locally stored data or via :.
            - Purpose of cracking a password
            - Automated and/or manual Method

        2. Complexity :
            - Upper Case
            - Lower Case
            - Numbers
            - Special Characters :
                using @,$,3,0,! Also known as Fab-Five !!

        3. Architecture :
            - Windows :
              Local Machine : SAM Database
              C:\windows\system32\config\sam
              Mounted as HKLM/SAM
              C:\windows\repair : this contain a copy SAM file
               - Active Directory : ntds.dit
                 C:\windows\NTDS\ntds.dit
                 new-technology directory system

            - Linux :
              Local Machine :
                  /etc/shadow

            - Apple :
              /var/db/dslocal/nods/default/users
              <user>.plist => ShadowHashData Property

        4. Techiniques Used :
            1. Dictionary Attacks
            2. Brute-Force Attacks
            3. Syllable Attacks - we take a password and combine it with Dictionary and Brute Force attacks
            4. Hybrid Attacks
                - Batman
                - Batman1
                - Batman2
                - Batman3
            5. Rule Based Attacks - Combination of Brute-Force, Dictionary and Syllable Attacks
            6. Guessing

        5. Types of Attacks :
            1. Passive Attacks :
                - Sniffing
                - Man in the middle
                - Side jacking : It allow an attacker to go to any WiFi access point , so attacker be able to steal the cookie of other user on the same wifi when an victime makes any transaction.
            2. Active Online :
                - **Hash Injection** (Pass the Hash)
                - **Trojan / Keylogger**
                - **LLMNR / NBT-NS** : They are used in order to perform name resolution
                When DNS fails to resolve the name through a query the host machine then perform an Un-Authenticated UDP broadcast asking if anyone name is equal to given. Name
                LLMNR uses port **UDP 5355**
                NBT-NS **port 137**

            3. Offline Attacks :
                - Rainbow
                - Distributed Network

- Pre-Computed Hash

4. **Non - Electronic Attacks :**
    1. **Dumpster Diving** : we look through trash
    2. **Shoulder Surfing** : Watching over shoulder
    3. **Social Engineering** : Manipulating user

6. **The Hash** :

    1. LM Hash / NTLM Stores password up to 14 Characters
    2. NTLM Hash

Add NTLM and Stored As:

- Bwayne:1005:86D8D0AEB8D112F8F9954FC9DF57E012:ED7B273FDE21FFE559AC8D1B9D3729BC:::
- Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E17D93985BF:::
- Guest:501:NOPASSWORD**********:NOPASSWORD**********:::

NOTE:

- Any hash that ends with: AAD3B435B51404EE means something to you:

5D567324BA3CCEF8**AAD3B435B51404EE** = The last seven characters are blank

- Any password over 14 characters: the LM Hash value is "dummied" with **AAD3B435B51404EE AAD3B435B51404EE**

 # NTLM Authentication :

NTLM is used when :

There is no kerberos trust between two different forest
Authentication is attempted by IP. Kerberos requires DNS
if one or both system not in the same domain.
if your firewall is blocking ports

How it is used ?

Challenged Response algorithm
password are not transmitted
V1 came with NT
V2 came with NT SP4

 # Kerberos Authentication :

Better, Stronger, faster
Ticket Based
Fast
Avoids the Transmission of Password
Time Based (PDC)

 # Salting :

Append or Prepending random strings
Done Before Hasing
Prevent duplicate Hashes
Unique to each password

 # Rainbow Tables :

Precomputed Hash table
Huge Files
SSD & Cloud Computing

2. Gaining Access - Privilege Escalation :

DLL Hijacking :

Winndows have DLL

Apple : have DYLIB

 # Methods of Escalation :

1. Pwn the admin / root account
2. Take advantage of Vulnerability
3. Fire up tools

 # Countermeasures

1.Encryption
2. Least Privilege
3. Updates
4. Limit Interactive Logins
5. Service Account don't need all rights
6. Limit the extent of code that runs "high"
7. Privilege separation approach
8. Test OS and app meticulously
9. Multi Factor
10. Stress Test

 # Types of Escalation :

1. Vertical Escalation :

- user get admin level access
- Create Users
- Configure System Settings
- Extract Data

2. Horizontal Escalation :

- Same Excess, but with different user account

 # Using you CPU to escalate :

Spectre and Meltdown :

This is the CPU Vulnerability

Spectre :

- Spectre Affects the cpu from Intel, ARM, AMD, Samsung, Qualcomm, Apple
- This Vulnerability tricks the processor into exploiting a speculative execultion to read restricted data
- It is basically used to increase the speed by jumping some conditions
- It allows the attacker to force the processors to accomplish a speculative execution of a read before bounds checking is performed.

Meltdown :

- It affect the Apple, ARM, Intel
- This vulnerability actually tricks the process to access out-of-bounds memory by exploiting CPU optimization mechanisms through again. Speculative execution.

 # Other Types of escalation Technique :

1. **Access Tokens** : token is used to determine the owner of the process
2. **Application Shimming** : window operating system uses WACF (Windows Application Compatibility Framework) : It allows windows 10 to run older programs like program of XP. This Shims provide a buffer between the application and Operating System.

Inject Malicios DLL, bypass uac, capture memory address, backdoors

3. **File System Permissions weakness**
4. **Path Interception**
5. **Scheduled Task**
6. **Launch Daemons**
7. **Plist Modification** : These files exists actually for application or service, it includes the necessary information that is needed to configure them
8. **Setuid and Setgid** : some can set the sid and gid
9. **Web Shell** : Attackers can inject malicious scripts to web server

3. Maintaining access (Phase - 3) - Executing Application :

Goals :

1. Make sure we can get back in
2. See what's going on
3. Detect More Information

Spyware and Backdoors :

1. **Spyware** :
   - Capture keystrokes
   - Capture Screenshots
   - Capture authentication credentials
   - Capture Emails
   - Capture Web Forms
   - Capture habits

   Types of Spyware :
   1. Desktop
   2. Video
   3. Printings
   4. USB
   5. Audio
   6. Email/Internet
   7. Screen Capture
   8. GPS
   9. Monitoring
   10. IoT

2. Backdoors :

1. Remote Admin utility
2. Total Control of Target
3. Use exploits
4. Backdoor consist of two elements : 1. Client , 2. Server
5. Automation Buit-in

Type of Backdoors :

1. Back Orifice
2. Sercom
3. RemoteExec

3. Keylogger :

1. Software Keylogger
   Records Keystrokes, Mouse strokes, screen shots , login activity
2. Hardware Keylogger
   small software is installed on adapters, keyboards, mouse

- Wi-Fi loggers
- Bluetooth loggers
- Acoustic Logger
- Rootkit loggers
- Driver Keylogger
- Hypervisor logger

4. Maintaining Access (Phase-3) - Hiding your tools :

1. Rootkits :

This allows attacker to gain administrative control over a computer
These are extremely hard to remove

Why are Rootkits Used :

1. Remote Control
2. Eavesdropping
3. Polymorphism : it allow rootkit to rewrite the core assembly code so signature based antivirus is useless here.

The only way to find rootkits that use polymorphism would be to use a technology that looks deep insisde the operating system and compare it against a base line.

TYPES OF ROOTKITS :

1. **User-Mode Rookits** : the rootkit runs on the computer with administrative rights or privileges
   It can be easily detected by antivirus or anti spyware
2. **Kernel Mode** : load the rootkits at the same level as the operating system

3. **Hybrid** : Rootkits with some of the characteristics from user-mode and some from kernel mode
4. **Firmware** : This rootkits hides in the firmware when the computer shut downs
5. **Vitual Rookits**

2. Alternate Data Streams

Macintosh file system actually store its data into two part
1. Data Fork : it it where the we store the data itself about the file
2. Resource Fork : It gives us some additional information about a file
creating :

c:\>notepad superdale.txt:hidingfromyou.txt
c:\>dir
superdale.txt and this will show a size of 0
to get the data of the hidden file
c:\>notepad superdale.txt:hidingfromyou.txt
c:\> dir /r : This will display the al the Alternate data stream

Creating with a File :

c:\> notepad batman.txt
c:\> type evilfile.exe > batman.txt:evil2.exe
c:\> start batman.txt:evil2.exe
creating a symbolic link : it is basically a type of shortcut
c:\> mklink joker.exe batman.txt:evil2.exe
to hide this file run
c:\> attrib +h joker.exe
c:\> joker
size of file is not increase

 # Detecting Rootkits :

1. **Integrity-Based** : Subsitute to both huiristic and signature based detection
this capture the snapshot of clean machine in database and compare the workstation with that snapshot
2. **Signature Base** : Compare the files and executables with its database that has been created of known rootkits.
3. **Run Time Execution path profiling** : This compare the run time execution path of all the process and the executables files
4. **Heuristic / Behaviour Based Detection** : This works by identifying the deviation of the normal operating system behaviour and its pattern.
5. **Detecting via File Systems** : C:\> dir /s /b /ah
/s : sub directories
/b : bare format : no need to give any header information
/ah : /a for add the following attributes and /h for hidden files
/a-h : don't give the hidden attributes
c:\> dir /s /b /a-h

3. Steganography

- Hiding data inside or behind other data
- unlike alternate data stream, the size of the image file will increase in size
- Replace unused data bits with the hidden file bits
- Extremely hard to detect

 # Steganography is divide into two parts :

1. **Technical** : Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size reduction methods.
2. **Linguistic** : hides the message in carrier or some type of media that used to transfer files back and forth or communicate

 # Steganography Types :

1. Image Based
2. Document Based
3. Folder Based
4. Audio based
5. Video based
6. Web Based : Hidden URLs, Hidden Image, Hidden Location
7. White Space based
8. Email Based
9. DVD Rom
10. Natural Text based : convert information into a flow of text like a play
11. OS based

 # Covering Tracks (Phase - 5) : Clearing Logs and Evidences :

What is the need to cover the tracks ??

1. Remain Obscure
2. Avoid trace backs
3. Convince “victims”

Basics Methods :

1. Clear Browser History
2. Delete Cookies
3. Clear password manager
4. Delete any private data
5. Clear logs

Advanced Methods :

1. Disable Auditing
2. Do Damage
3. Enable Auditing on again

tools :

1. Auditpol : auditpol /set /category:”logon/logoff” /success:disable /failure:disable

windows logs files path : windows/System32/winevt/Logs

Bash History :

```
export HISTSIZE=0
history -c
history -w
cat /dev/null > ~.bash_history && history -c && exit
        Deletes the complete command history of the current user
shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit
```