Experiment No:13

**Aim:** To demonstrate OS Backdoor and Its prevention methods

**Theory:**

A backdoor is a malicious computer program that is used to provide the attacker with unauthorized remote access to a compromised PC system by exploiting security vulnerabilities. A Backdoor works in the background and hides from the user. It is very similar to other malware viruses and, therefore, is quite difficult to detect. A backdoor is one of the most dangerous parasite types, as it gives a malicious person ability to perform any possible actions on a compromised computer. The attacker can use a backdoor to spy on a user, manage his/hers files, install additional software or dangerous threats, control the entire PC system and attack other hosts. Often a backdoor has additional destructive capabilities, such as keystroke logging, screenshot capture, file infection and encryption. Such parasite is a combination of different privacy and security threats, which works on its own and doesn’t require to be controlled at all.

Most backdoors are malicious programs that must be somehow installed to a computer. Nevertheless, some parasites do not require the installation, as their parts are already integrated into software that is running on a remote host. Programmers sometimes leave such backdoors in their software for diagnostics and troubleshooting purposes. However, hackers use them only to break into the system.

Backdoors are specific trojans, viruses, keyloggers, spyware and remote administration tools. They work in the same manner as mentioned viral applications do. However, their functions and payload are much more complex and dangerous, so they are grouped into one special category.

**How do backdoors spread themselves?**

Backdoors are not capable of propagating themselves and infecting systems without user’s knowledge. The most of such parasites must be manually installed in a bundle with other software. There are four major ways how these threats get into the system.

Unaware PC users can accidentally install typical backdoors on their computers. They can come attached to the e-mail messages or file-sharing programs. Their authors give them unsuspicious names and trick users into opening or executing such files.

Backdoors are often installed by other parasites like viruses, trojans or even spyware. They get into the system without user’s knowledge and consent, and affect each of users who uses a compromised computer. Some threats can be manually installed by malicious users who have sufficient privileges for the software installation. The small part of backdoors can spread by exploiting remote systems with certain security vulnerabilities.

Several backdoors are already integrated into particular applications. Even legitimate programs may have undocumented remote access features. The attacker needs to contact a computer with such software installed to instantly get full unauthorized access to the system or take over control over the certain software.

Some backdoors infect a computer by exploiting certain software vulnerabilities. They work similarly to worms and automatically spread without user knowledge. The user cannot notice anything suspicious, as such threats do not display any setup wizards, dialogs or warnings.

Widely spread backdoors affect mostly computers running Microsoft Windows operating system. However, lots of less prevalent parasites are designed to work under different environments, like Mac OS X and others

**What risks can be initiated by this computer infection?**

A backdoor allows the attacker to work with an infected computer as with its own PC and use it for various malicious purposes or even criminal activities. In most of the cases, it is really hard to find out who is controlling the parasite. In fact, all backdoors are very difficult to detect. They can violate user privacy for months and even years until the user will notice them. The malicious person can use a backdoor to find out everything about the user, obtain and disclose priceless information like user’s passwords, login names, credit card numbers, exact bank account details, valuable personal documents, contacts, interests, web browsing habits and much more. Backdoors can be used for destructive purposes. If the hacker was unable to obtain any valuable and useful information from an infected computer or have already stole it, he eventually may destroy the entire system in order to wipe out his tracks. This means that all hard disks would be formatted and all the files on them would be unrecoverably erased.

When backdoor finds its way to the system, it causes these activities:

* Allows the intruder to create, delete, rename, copy or edit any file, execute various commands, change any system settings, alter the Windows registry, run, control and terminate applications, install other software and parasites.
* Allows the attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for permission.
* Steals sensitive personal information, valuable documents, passwords, login names, identity details, logs user activity and tracks web browsing habits.
* Records keystrokes and captures screenshots. In addition, sends all gathered data to a predefined e-mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
* Infects files, corrupts installed applications and damages the entire system.
* Distributes infected files to remote computers with certain security vulnerabilities, performs attacks against hacker defined remote hosts.
* Installs hidden FTP server that can be used by malicious persons for various illegal purposes.
* Degrades Internet connection speed and overall system performance.
* Prevents its removal by hiding its files and providing no uninstall feature.

**How to Reset Windows Password through a Backdoor**

We can Reset Windows Password through a Backdoor. Resetting Windows Password is not a tough task, Some Techies can easily reset windows password without a reset disk. Use of Backdoor to Reset windows password is quit popular now a days. To Recover Windows Password through CMD We need to Create A Backdoor.We will use a windows feature easy of access icon which is located at bottom right corner in windows login screen. Microsoft bought this feature in Windows for Physically disabled persons.The easy of access icon is wired to Utilman.exe file which is available in C:/Windows/System32.

We will replace that file with the Command Prompt and when Someone will click on easy of access icon on a locked screen then a CMD window will open and there We can easily login into locked Computer by resetting windows passwords or creating a new user from CMD.

**To Replace Utilman from CMD , we need to open a command window**

* If your machine is not locked and you have passwords to enter in system then open CMD as Administrator and skip below step and move to command section
* If your computer is locked then to Reset Forgotten Windows Passwords you need to follow below step to open CMD.

**How to Open CMD in a Locked Computer to Recover Windows Password**

* Remove the operating system hard drive from the target system and slave it into another system with a working operating system. From there you can swap out the files on the slave drive
* Use the Windows Vista, 7,8 or 10 DVD
  + Look for link Repair Your Computer and click on that
  + Then select option “Use recovery tools that can help fix problems starting Windows.
  + Select an operating system to repair”
  + Now You Will be asked to “Choose a Recovery tool” select Command Prompt

**How to Create Backdoor to Reset Windows Password**

So now we all are in Administrator Command Prompt. Type these Commands and press enter.

* REN "C:\Windows\System32\Utilman.exe" "Utilman\_org.exe"

//Rename Utilman to Utilma\_org

* copy "C:\Windows\System32\cmd.exe" “cmd\_copy.exe"

//copy cmd as cmd\_copy

* REN "C:\Windows\System32\cmd\_copy.exe" "Utilman.exe"

//Rename cmd\_copy to Utilman

**Reset Forgotten Windows Password or Create a New User with cmd**

Go to Logon Windows Screen. Click on easy of access icon. a CMD window will open type these commands to crack windows passwords.

* To Create a New user type these Commands

net user username password /add

* To Change the Password of existing User type these commands .type net user to know the username and don’t forget the star

net user username

**Revert All Changes as it was**

type these commands and press enter

del "C:\Windows\System32\Utilman.exe"

REN "C:\Windows\System32\Utilman\_org.exe" "Utilman.exe"

**Removing a backdoor from the system**

Backdoors are extremely dangerous parasites that must be removed from the system. You can hardly find or remove a backdoor manually. That’s why we highly recommend using automatic removal option. There are lots of programs that are offered for the removal of backdoor viruses. However, the most reliable one is considered Reimage. You can also try Plumbytes Anti-Malware as an alternative security tool. However, make sure that you update this and other programs before launching them. This will help you to prevent failures and other issues that can appear when trying to get rid of a particular backdoor.

**Best practices to protect against back doors include:**

* Require all admin or root access to be done via a jumpserver or “jump box”. A jumpserver is a specially secured box that all administrators are required to log into to gain access to devices on the network.
* Multi-factor authentication to all devices especially for root or admin access including via the jumpserver.
* Implement network segmentation – allow access to device administration only from specific subnets and specific boxes i.e jumpserver.
* Require vendors/business partners and their suppliers to provide proof they are providing adequate security for their products.

**Conclusion:**

Thus OS Backdoor very hard to detect. In our system we have to be sure that each service running in system is from trusted application provider.