Telnet Brute Force Fix Manual

1) **Strong Passwords (By Manonarayanan Janardhan Bhagavathi):**
   Use secure credentials to protect yourself from attacks. The stronger the combination, the more difficult it will be for attackers to gain access.

   To reduce the risk of brute force attacks, system administrators can take several steps in backend protection for passwords:

   - Encrypt passwords with high encryption rates
   - Randomize password hashes by adding a unique salt to each password
   - Use two-factor authentication
   - Install an intrusion detection system
   - Limit login retries and throttle rate of repeated logins
   - Use Captcha to stop robots
   - Use an IP denylist to block known attackers.

2) **Remove unused accounts (By Manonarayanan Janardhan Bhagavathi):**
   Delete unmaintained accounts to avoid vulnerabilities, which will have the potential to be security risks.

3) **IPBan Tool (By Manonarayanan Janardhan Bhagavathi):**
   IPBan Tool is designed to prevent any brute-force login attempts by blocking them immediately. It also keeps a close eye on the log files to detect any suspicious activity, such as failed login attempts. Once such activity is detected, the system takes action by blocking the IP addresses associated with it. This ensures that your system remains secure and protected against any unauthorized access.

   Windows Installation:
   Requirements - OS: Windows Server 2016 and Windows 10 or the later versions

   .NET Framework: 4.7.2 or later

   Powershell: 5.1 or greater

(Note: You need administrative privileges to install to configure IPBan on the Windows Server. Additionally, enable the Firewall to use IPBan on the Windows Server)

Installation Process

- Open Remote Desktop Connection in Windows. Launch the application by entering the IP Address or hostname of your server and pressing "Connect."
- Enter your credentials to connect your remote server
- Open Powershell on your remote server
- Paste this command on your remote server and run it

#ipban command for windows
$ProgressPreference = 'SilentlyContinue';
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;
iex ((New-Object
System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/DigitalRuby/IPBan/master/IPBanCore/Windows/Scripts/install_latest.ps1'))

Linux Installation

Requirements - OS: Ubuntu x64

Debian x64

CentOS x64

RedHat x64

(Note: All the operating systems of Linux require firewalld)

Installation Process

- Open the terminal as a root user.
- Paste the command lines and run them

#single command as the root user
sudo -i

#ipban command for linux
bash <(wget -qO-
https://raw.githubusercontent.com/DigitalRuby/IPBan/master/IPBanCore/Linux/Scripts/Install.sh)

4) **DenyHost (By Tharun Emuri):**

DenyHosts is a security tool designed to prevent brute force attacks on network services, including Telnet. This manual will guide you through the installation and configuration of DenyHosts on different Operating Systems (OS) to prevent Telnet brute force attacks.

Supported OS

- Ubuntu/Debian
- CentOS/RHEL
- Fedora
- Windows (using Cygwin)

Installation and Configuration
Ubuntu/Debian

1. **Installation**: *sudo apt-get install denyhosts*
2. **Configuration**: Edit */etc/denyhosts.conf* to enable Telnet protection
    - *sudo nano /etc/denyhosts.conf*

- Uncomment *HOSTS_DENY_telnet = /etc/hosts.deny*
- Save and exit

3. **Restart**: *sudo service denyhosts restart*

CentOS/RHEL

1. **Installation**: *sudo yum install denyhosts*
2. **Configuration**: Edit /etc/denyhosts.conf to enable Telnet protection
   - *sudo nano /etc/denyhosts.conf*
   - Uncomment *HOSTS_DENY_telnet = /etc/hosts.deny*
   - Save and exit
3. **Restart**: *sudo service denyhosts restart*

Fedora

1. **Installation**: *sudo dnf install denyhosts*
2. **Configuration**: Edit */etc/denyhosts.conf* to enable Telnet protection
   - *sudo nano /etc/denyhosts.conf*
   - Uncomment *HOSTS_DENY_telnet = /etc/hosts.deny*
   - Save and exit
3. **Restart**: *sudo systemctl restart denyhosts*

Windows (using Cygwin)

1. **Installation**: Install Cygwin and then run setup.exe to install denyhosts package
2. **Configuration**: Edit *C:\cygwin\etc\denyhosts.conf* to enable Telnet protection
   - Uncomment *HOSTS_DENY_telnet = /etc/hosts.deny*
   - Save and exit
3. **Restart**: *cygrunsrv -start denyhosts*

Script

```
#!/bin/bash

# Function to check if the user is root
is_root() {
    if [ "$(id -u)" != "0" ]; then
        echo "This script must be run as root." >&2
        exit 1
    fi
}

# Function to install and configure denyhosts
install_denyhosts() {
    distro=$(awk -F= '/^NAME/{print $2}' /etc/os-release)

    if [[ "$distro" =~ ^(Ubuntu|Debian)$ ]]; then
        apt-get update
        apt-get install -y denyhosts
    elif [[ "$distro" =~ ^(CentOS|RedHat)$ ]]; then
        yum update
        yum install -y denyhosts
    elif [[ "$distro" == "Fedora" ]]; then
        dnf update
        dnf install -y denyhosts
    else
        echo "Unsupported distribution. Manual installation required."
```

```
        exit 1
    fi

# Configure denyhosts
    sed -i 's/DENY_HOSTS_ALLOW = /DENY_HOSTS_ALLOW = ALL/g' /etc/denyhosts.conf
    sed -i 's/#BLOCKINGPERIOD = 432000/BLOCKINGPERIOD = 86400/g'
/etc/denyhosts.conf
    sed -i 's/#PURGE_DENY = 5d/PURGE_DENY = 1d/g' /etc/denyhosts.conf
    sed -i 's/#PURGE_HOSTS_DENY = 5d/PURGE_HOSTS_DENY = 1d/g'
/etc/denyhosts.conf

 # Configure email notifications (optional)
    read -p "Do you want to enable email notifications? (y/n) " enable_email
    if [[ "$enable_email" =~ ^[Yy]$ ]]; then
        read -p "Enter the hostname or domain: " hostname_domain
        read -p "Enter the admin email address: " admin_email
        read -p "Enter the SMTP server hostname or IP: " smtp_host

        sed -i "s/#HOSTNAME_DOMAIN=/HOSTNAME_DOMAIN=$hostname_domain/g"
/etc/denyhosts.conf
        sed -i "s/#ADMIN_EMAIL=/ADMIN_EMAIL=$admin_email/g" /etc/denyhosts.conf
        sed -i "s/#SMTP_HOST=/SMTP_HOST=$smtp_host/g" /etc/denyhosts.conf
    fi

    systemctl restart denyhosts
}

# Main script
is_root

read -p "Do you want to install and configure denyhosts? (y/n) " confirm
if [[ "$confirm" =~ ^[Yy]$ ]]; then
    install_denyhosts
    echo "denyhosts installed and configured successfully."
else
    echo "denyhosts installation skipped."
fi
```

Additional Tips

- Make sure to regularly update your DenyHosts installation to ensure you have the latest protection rules.
- Consider combining DenyHosts with other security measures, such as firewall rules and strong passwords, to further enhance your security posture.

Troubleshooting

- Check the DenyHosts logs for errors or issues: sudo cat /var/log/denyhosts
- Verify that the hosts.deny file is being updated correctly: sudo cat /etc/hosts.deny

By following this manual, one should now have DenyHosts installed and configured to prevent Telnet brute force attacks on your system.