* In case of any word-based-filter,
  + try different combinations of that word by mixing their case.
  + if valid, give input after a new line OR repeat ‘filtered word’. Due to incorrect regex, these scenarios may give desired o/p.
* 127.0.0.0/8 -> these are ip address are reserved for loop-back.
* <https://www.aychedee.com/2012/03/14/etc_shadow-password-hash-formats/> to understand about /etc/shadow file

# ShellShock Exploit

* Bash till 4.3 is vulnerable
* Use [this script](https://github.com/cheetz/icmpshock) to scan for CGI-BIN based shell shock vulnerability.
* Such exploits will work only when bash file is inside cgi-bin folder. ShellShock is vulnerability in bash.
* <https://resources.infosecinstitute.com/practical-shellshock-exploitation-part-1/>
* <https://resources.infosecinstitute.com/practical-shellshock-exploitation-part-2/>
* <https://github.com/mubix/shellshocker-pocs>

# HeartBleed Vulnerability

* affected versions of OpenSSL are versions 1.0.1 through 1.0.1f, 1.0.0, 0.9.8 and 1.0.1g are not affected

For hex-editing, Notepad++ does not have any decent option. So use HxD editor.

# SMB and NetBIOS

SMB is application layer protocol. It can run directly over TCP, port 445. Alternatively, it can run over NetBIOS API. NetBIOS in-turn runs on UDP port 137,138 OR TCP ports 137 & 139.

NetBIOS is an API that runs on session-layer (of OSI model). It is not a protocol. It specifies functions like connect to a computer, send data to a computer, etc. It does not specify how this is actually done.

SMB on the other hand is a protocol. It specifies the specific format of the data that computers will send to each other the network.

For further details refer to [Quora answer](https://www.quora.com/What-is-the-difference-between-NetBIOS-and-SMB) & [stackoverflow answer](https://superuser.com/questions/694469/difference-between-netbios-and-smb)

# Active Directory Enumeration & Exploitation

Once you have login information for any AD-server, try enumerating all user of that server. For this, use [ADDirectory.py](https://github.com/SecureAuthCorp/impacket/tree/master/examples) . Similarly, you can use PSexec.py to login using AD creds. To get a better picture of various machines connected to a given AD, you can use [BloudHound](https://github.com/BloodHoundAD/BloodHound). This will aid you in enumerating machines in AD and fetching hashed password. For more details on this step refer [to](https://www.youtube.com/watch?v=jUc1J31DNdw).

# Enumerate Drupal.

* Tools like [droopescan](https://github.com/droope/droopescan) are useful