

Don't Get Cracked on Hostile WiFi

Mackenzie "maco" Morgan

<http://ubuntulinuextipstricks.blogspot.com>

Ohio Linux Fest

11 Oct 2008

Scenario



- Open WiFi
- Security conference
- Hackers everywhere

Disclaimer

- You won't be low-hanging fruit
- But won't stop OSI Layer 2 attacks

Before You Go

- VPN
- Firewall & services
- Users & passwords
- DNS
- Hashes
- Disable SHMConfig in xorg.conf
- Phone a friend

VPN

- Creates encrypted tunnel
- Termination point
 - DD-WRT on your router at home
 - School network
 - Online services

Firewall Goals

- Drop all inbound on all interfaces
- Minimal outbound ports on wireless interface
 - VPN port
 - DNS
- Whitelist outbound ports on tunnel interface

Firewall & Services

- UFW alone is insufficient
 - Cannot do outbound
 - Need to edit `/etc/ufw/before.rules` and `/etc/default/ufw`
- Outbound matters
 - No phoning home
- Drop, not reject – takes longer to port scan
- No external services
 - Are you going to SSH into the laptop you're holding?
- IPv6 firewall is `ip6tables`, not `iptables`

Default drop in UFW

/etc/default/ufw

```
IPV6=no  
DEFAULT_INPUT_POLICY="DROP"  
DEFAULT_OUTPUT_POLICY="DROP"  
DEFAULT_FORWARD_POLICY="DROP"
```

But that's not enough...

/etc/ufw/before.rules has these lines by default:

```
# connection tracking for outbound  
-A ufw-before-output -p tcp -m state --state\  
NEW,ESTABLISHED,RELATED -j ACCEPT  
-A ufw-before-output -p udp -m state --state\  
NEW,ESTABLISHED,RELATED -j ACCEPT
```

Other Example Rules

```
# DNS
-A ufw-before-output -p udp --dport 53 -j ACCEPT

# Ping
-A ufw-before-output -p icmp --icmp-type echo-request -j ACCEPT

# Allow VPN running on port 4500 through wireless interface
-A ufw-before-output -p 50 -d x.x.x.x -o wlan0 -j ACCEPT
-A ufw-before-output -p udp -d x.x.x.x --sport 4500 --dport 4500\
-o wlan0 -j ACCEPT

# Allow outbound SSH, HTTP/S, Jabber, and IRC on tunnel interface
-A ufw-before-output -p tcp -m multiport\
--dports 22,80,443,5222,6667 -o tun0 -j ACCEPT
```

Port numbers for protocols can be found in
`/etc/services`

Users & Passwords

- Temporary **strong** password for you
- Disable unneeded users
 - `passwd -l`
 - Set `/bin/false` as shell in `/etc/passwd`

DNS

- Hardcode your DNS servers
- /etc/dhcp3/dhclient.conf

```
prepend domain-name-servers 208.67.222.222;  
prepend domain-name-servers 208.67.220.220;
```

- DNS Sec if you're *really* paranoid

Hashes

- Not-from-repository binaries
- Configuration files
- Will come in handy later

SHMConfig

- Used for configuring synaptics touchpads with synclient or Gsynaptics
- Creates area of 777 memory
- Turn it **OFF!**

One Last Thing...

- Test your setup
 - Netstat
 - Nmap (or Zenmap)

While There

- Bluetooth
- Wireshark
- Logs
- Physical Security

Bluetooth

- Can't really firewall it off
- Blacklist the module
- /etc/modprobe.d/blacklist
 - Add line "blacklist hci_usb"
- Don't forget your cell phone

Wireshark & Logs

- Watch `/var/log/kern.log`
- Look for connection attempts

Physical Security

- Theft of hardware isn't the only threat
- Don't leave your laptop unattended
- Don't let any untrusted person touch it
- Use the buddy system to protect the laptop
- DVDs, CDs, and flash drives: Do Not Mount

Afterward

- Verify binaries
- Check environment variables
- Check for new services
- Change password again
- Use Netstat to check for oddly-open ports

Verifying binaries

- From repositories
 - rpm -Va
 - debsums -c
- Compare hashes of non-repository binaries with ones from before

If You're Really Worried...

- Reinstall!

New Security Features

- Shadow 4.1
 - SHA-256 and SHA-512 for `/etc/shadow`
 - MD-5 and SHA-1 are no longer recommended by NIST
- Touchpad configuration can be changed without SHMConfig

Questions?

See Also

- DNS Sec:
 - <http://ubuntuforums.org/showthread.php?t=492489>
- NSA SNAC Guide:
 - <http://www.nsa.gov/snac/os/redhat/rhel5-guide-i731.pdf>
- `man iptables`
- IANA ports list:
 - <http://www.iana.org/assignments/port-numbers>