NETWORK SECURITY:
PROTECTING SOHO NETWORKS

JIM GILSINN
WHO AM I?

- Electrical engineer
  - 25 years engineering
  - 15 years ICS/SCADA networking & security

- ICS/SCADA networking & security
  - Policies & procedures
  - Designs
  - Assessments
  - Standards
WHERE DO I WORK?
WHERE DO I REALLY WORK?
ENOUGH ABOUT ME… WHAT AM I HEAR TO TALK ABOUT?

• Most Consumer-Grade Routers Are Vulnerable
• Small Office/Home Office (SOHO) Networks Are Especially Vulnerable
• Millions of Computers in Botnets
• Rise of Ransomware
• What can you do to protect yourself?
THERE IS A BETTER WAY

• You Can Build A Secure SOHO Network
• And...It Won’t Cost $6M
SMALL OFFICE/HOME OFFICE (SOHO) NETWORKS

- Small Office
  - 1-10 employees
  - Single main site
  - 1-2 main servers

- Home Office
  - Telework
  - Remote/virtual office
  - VPN to main office
4 MAIN AREAS OF FOCUS

• Firewall & Primary Network Connections
• Wireless Networking
• Remote Access
• Network Monitoring
FIREWALL & PRIMARY NETWORK CONNECTIONS
FIRST: DITCH THE STANDARD CONSUMER-GRADE ROUTER
FIRST: DITCH THE STANDARD CONSUMER-GRADE ROUTER

- They may look cool
- They may say they have tons of features, usually not security related
- They rarely get updated
- They often aren’t securely designed/built
DITCH THE ISP ROUTER TOO

• If you have admin privileges on your ISP router,
  • Turn off WiFi
  • Turn off routing

• Only use it as a MODEM only

• Get a public IP address
USE A TRUE FIREWALL/UTM

- OPNsense
  - Your next open source firewall
- Untangle
- pfSense
PFSENSE IS MY CHOICE

- Commercial Company
  - Sell hardware-based firewalls & service
  - Software is same for open-source & commercial hardware

- FreeBSD-Based
  - Command-line option available to install additional tools

- Large Number of Add-Ons
PFSENSE HARDWARE EASY TO FIND

• Hardware requirements for pfSense are pretty minimal
• Really depends on
  • Network throughput
  • Number of add-ons
• An old computer with 2 decent gigabit network cards should work
• I run a fanless computer
USE A SMART NETWORK SWITCH

- Have a Layer 2+ or 3 switch right behind your firewall
- My recommendation for most people is Netgear GS-108E
  - Inexpensive ($60)
  - Mirror port (Very Important)
  - Web configurable
YOU CAN ALWAYS GO BIGGER

- Larger network switches
- Servers
- Rack Equipment
CONSIDER REMOTE PARTS OF YOUR NETWORK

• Home Power Networking
  • Be careful in locations that share electrical wiring (like apartments/condominiums)

• Wireless Repeater
  • Latency can be an issue
WIRELESS NETWORKING
REPLACE YOUR WIFI SYSTEM: 2 CHOICES

• Replace Firmware
  • DD-WRT
  • OpenWrt

• Pros
  • Uses existing hardware
  • Cheap

• Cons
  • Limited by existing hardware

• Install Commercial-Grade Access Points
  • Ubiquiti
  • Cisco

• Pros
  • Designed for SOHO
  • Multiple SSIDs

• Cons
  • Low cost, but not free
I run 2 Ubiquiti UniFi APs
- Coverage area in 3-story townhouse
- Large number of competing networks

Controller
- Java-based software
- Available for Windows/Mac/Linux
- Many people run on Raspberry Pi
REMOTE ACCESS
VIRTUAL PRIVATE NETWORKS (VPNS)

• Employees Need Access While Working Remotely
  • Small office employees often work remotely
  • Virtual employees always need company services

• Types of Services
  • Email or Inter-Office Messaging
  • Servers
  • Phone
MULTIPLE VPN CONNECTIONS

• I Have 2 VPN Settings Currently
  • Outgoing – VoIP connection for my work phone
  • Incoming – Access my home network remotely

• I Use Incoming While on Travel
  • Secure, encrypted access from any hotel/coffee-shop
NETWORK MONITORING
MONITORING CONSISTS OF MULTIPLE PARTS

• Scanning

• Intrusion Detection

• Monitoring
SCANNING

- Passive Scanning
  - This is where that mirror port comes in handy

- Active Scanning
  - Looking for Vulnerabilities
  - WARNING: Only scan your network or networks you have permission to scan.
WIRESHARK

• Network Scanner & Packet Decoder
  • 2200+ Protocols, 150k+ fields
  • Extensible
  • Also has non-Ethernet-based protocols

• GNU GPL Open-Source
  • Very strict about licensing

• De Facto Standard

• Download From Wireshark.org
  • Apt & Yum repositories well out of date

• Extremely Powerful!!
OTHER PACKET CAPTURE & ANALYSIS TOOLS

• Other Packet Sniffers Exist
  • TCPdump
  • NetworkMiner

• All of the Packet Sniffers Require Administrator Access
  • Promiscuous mode

• Wireless Packet Capture
  • Aircrack
  • Kismet
  • Netstumbler

• Wireless Usually Requires Different Wireless Adapter
  • Internal cards don’t usually allow promiscuous mode
ACTIVE SCANNING & BEYOND

- Device Vulnerabilities
  - Nmap
  - Nessus/OpenVAS

- Web Site Vulnerabilities
  - Burp Suite
  - Browser Exploitation Framework (BeEF)

- Exploitation
  - Metasploit

- Linux Distros (Red Team)
  - Kali
  - Pentoo
**INTRUSION DETECTION**

- Network-Based Intrusion Detection System (NIDS)
  - Snort
  - Bro
  - Suricata
- Host-Based Intrusion Detection System (HIDS)
  - OSSEC

- NIDS Should Be Installed As Close to Firewall As Possible
  - Inside the firewall
  - At primary network switch via mirror port

- Linux Distros (Blue Team)
  - Security Onion
  - REMnux
MONITORING

- Network Security Monitoring (NSM) and Security Incident & Event Management (SIEM)
  - OSSIM
  - Splunk
  - Snorby
  - SGUIL
  - Squert
- ELSA
- SiLK & flowBAT
- Aggregate & Alert
- Dashboards
TO WRAP IT ALL UP...
SUMMARY

• There are a ton of free and open-source tools out there

• Start simple and build

• Know your network first in order to defend it
QUESTIONS

• Jim Gilsinn
• jimgilsinn@gmail.com
• @JimGilsinn