Security Principles

- **CIA**
- **C**onfidentiality
- **I**ntegrity
- **A**vailability

- **AAA**
- **A**uthentication
- **A**uthorization
- **A**ccounting

THREATS

- System Crash/Hardware failures
- Admin access control weakness
- Malware
- Social Engineering
- Man in the Middle Attacks
- Denial of Service Attacks
- Physical Intrusion
- Wireless Attacks

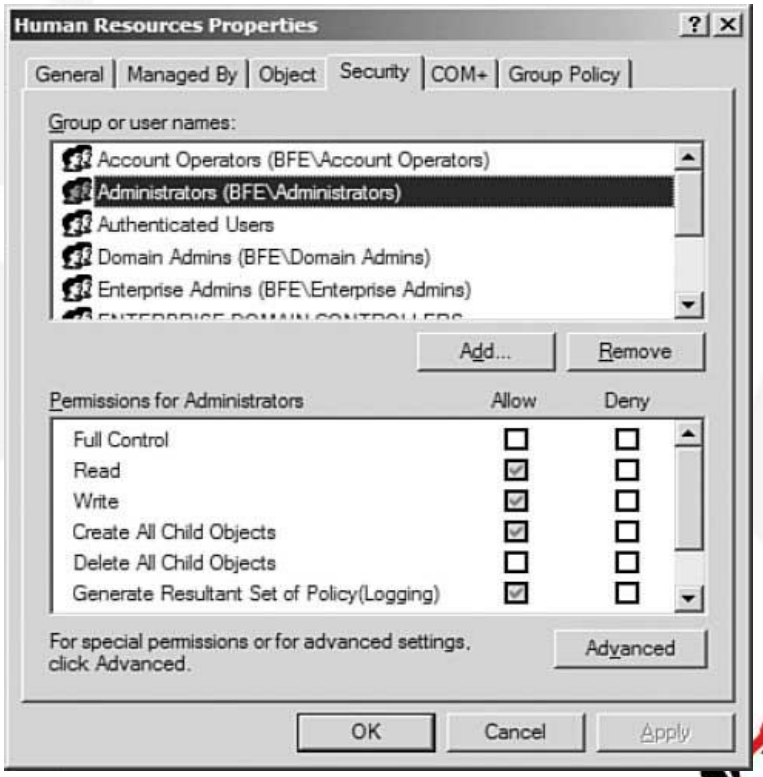
System Failures

- Hard Drives
- Power Failures
- Network Devices
- Servers

- Redundant Systems
- RAID
- UPS
- Clusters (High Availability)
- Redundant NIC / Switches

Admin Access Control

- Access Control Lists (ACL)
- Least amount of privilege
- Need to Know principle
- Accounts security



Malicious Software (Malware)

- Virus
- Worm
- Trojan Horse
- Rootkit
- Adware/Spyware

Prevention:

- Antimalware / Antivirus
- System well patched and maintained

Social Engineering

- Using or manipulating users for nefarious gain.
- Phishing.
- Vishing.
- Hoax.

<u>Prevention</u>

- User training and awareness.

Man in the Middle Attack (MITM)

Interception

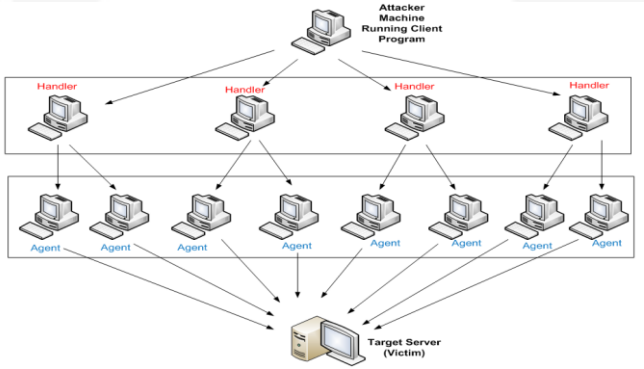
- Gain access to sensitive data
- Manipulate data

Prevention

- Encryption
- Data Integrity

Denial of Service (DOS)

Flooding techniques



- Smurf Attack (ICMP)
- Fraggle Attack
- TCP/SYN Flood
- DDoS – Distributed Denial of service (many computers attempting to access a web service, in order to break it.)
- Zombies / Botnets – A group of computers controlled to perform malicious attacks.

Prevention

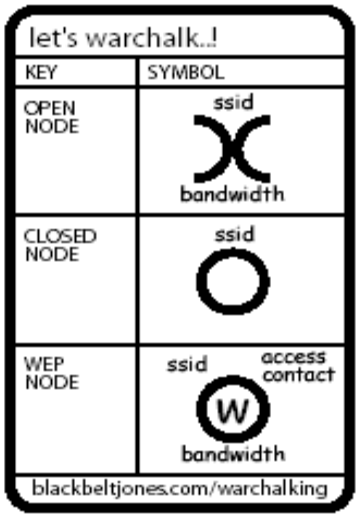
- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems

Physical Intrusion

- Server Room Security
- Building Security
- Disposal Policy
- Dumpster Diving
- Piggy Backing
- Shoulder Surfing – Ensure passwords are not easily visible by oth
- Tailgating – Following an employee past security
- Physical Security barriers
- CCTV
- Mantrap - Turnstile
- Partitions

Wireless Security

- Wardriving - Looking for unsecured wireless networks
- Warchalking - Marking on the street unsecured wirelesss netv
- Rogue Access Point - Malicious Access Point on your network.
- Evil Twin - Clone Server or equipment added to a network.
- Encryption Cracking - When your encryption method is broke
- Tips to prevent attack:
- Shielding - Using shielded cables that are not easily accessible.
- Disable SSID - Not allowing WiFi name being broadcast.
- WPA2 (rather than WEP) - More secure WiFi Password encrytion
- MAC Filters- Only allowing certain devices with a u
  access your network.



Securing User Accounts

- Authentication
- **Something that you know** – Username, Password, Pin
- **Something that you have** – Token, Smartcard, Common Access Card
- **Something that you are** – Retinal scan, fingerprint (Biometric)
- *Multi-factoring – 2 or more authentication methods*

Authentication Protocols

- Password Authentication Protocol **PAP**
- Challenge Handshake Protocol **CHAP**
- Microsoft CHAP **MS-CHAP (MS-CHAPv2)**
- Extensible Authentication Protocol **EAP**
- **802.1x** - Network Access Control

A A A

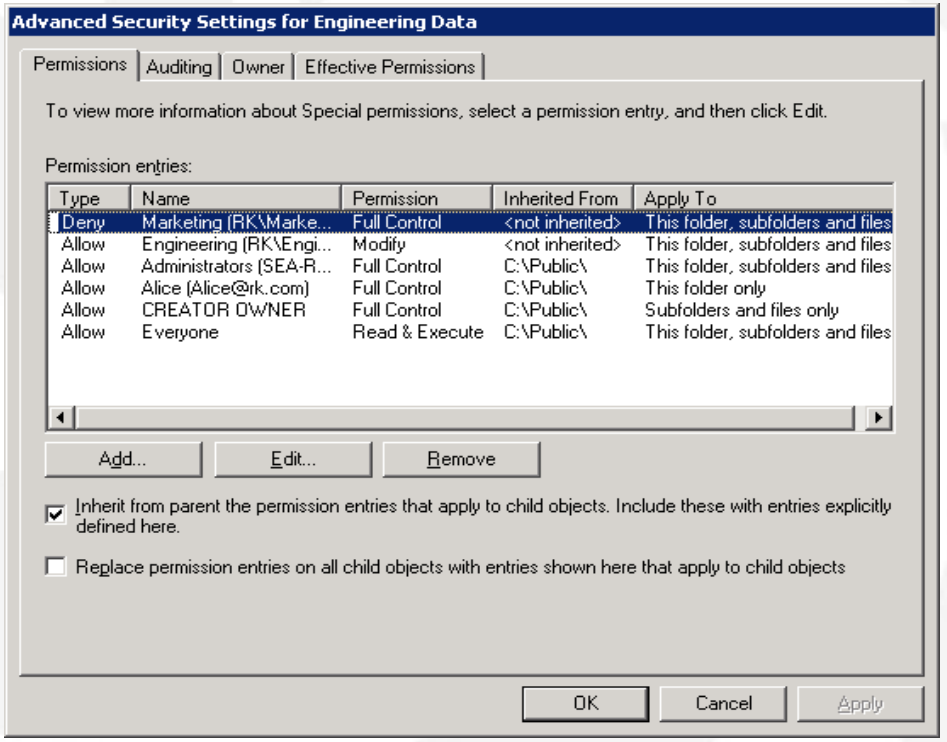
- Centralized Authentication, Authorization and Accounting:
- Remote Authentication Dial-in User Service **RADIUS**
- Terminal Access Controller Access-Controller System **TACACS+** (Cisco)

KERBEROS

- Authentication protocol for TCP/IP networks allowing centralization of authentication on a single server (Domain Controller)
- Uses UDP / TCP port 88
- Key Distribution Center
- TGT
- TGS

Authorization

- Permissions
- Rights
- Access Controls
- Share / Security Permissions
- Security Groups

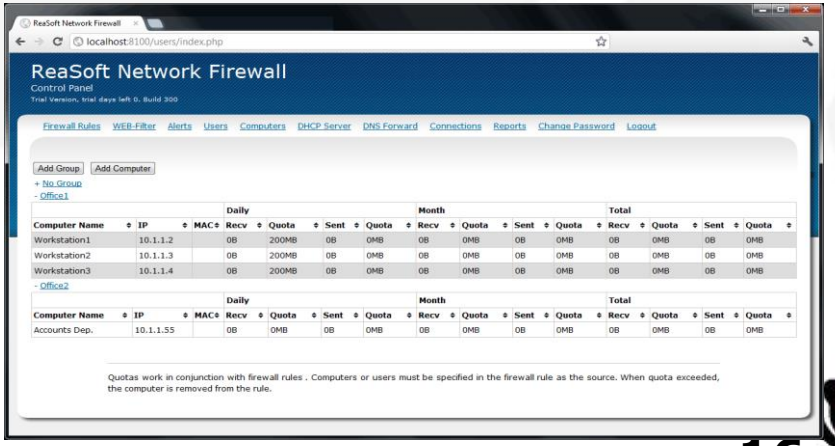


FIREWALLS

- NAT
- Port Filtering
- Packet Filtering
- MAC Filtering (*Wireless Networks*)
- Personal Firewall (*Windows*)

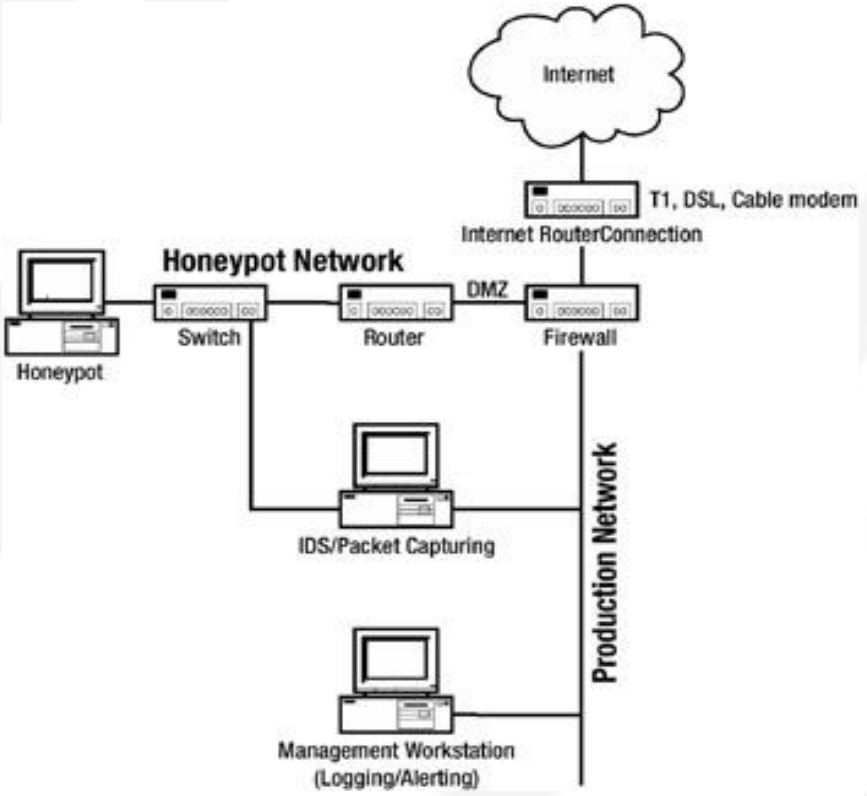
Host Based

- Network Firewall



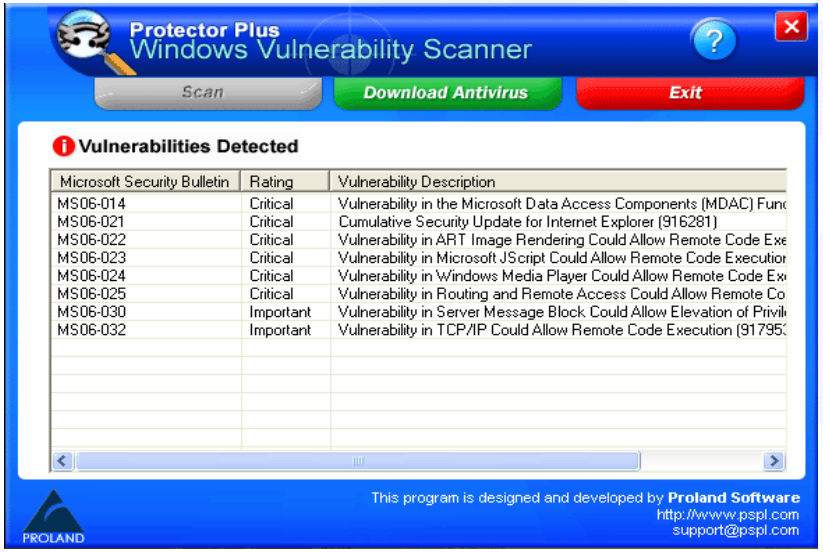
Network Zones

- Demilitarized Zone (DMZ) – network between 2 firewalls
- Transitional Network
- Honey Pot / Honey Nets
- IDS / IPS



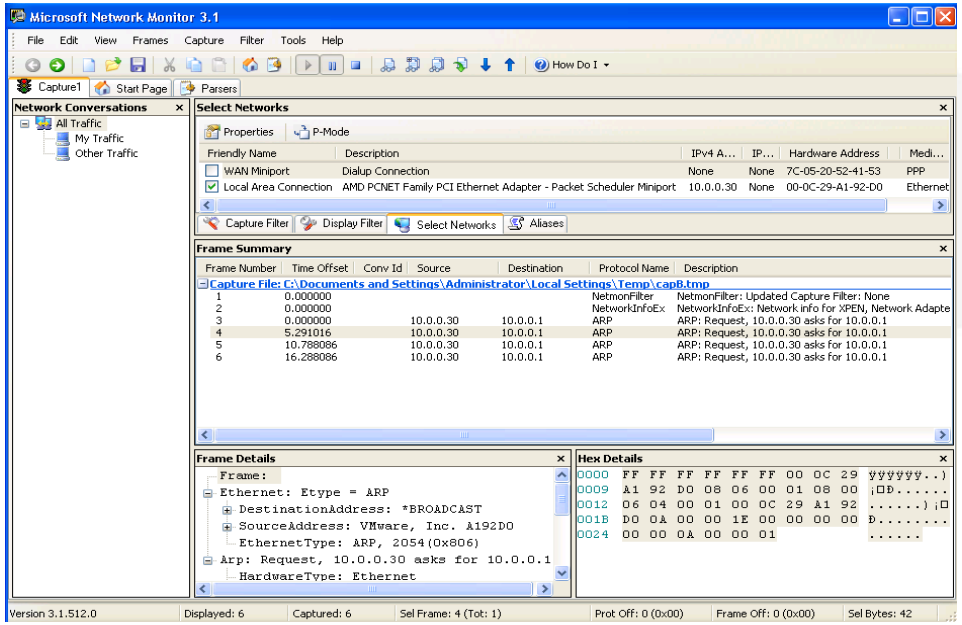
Vulnerability Scanner

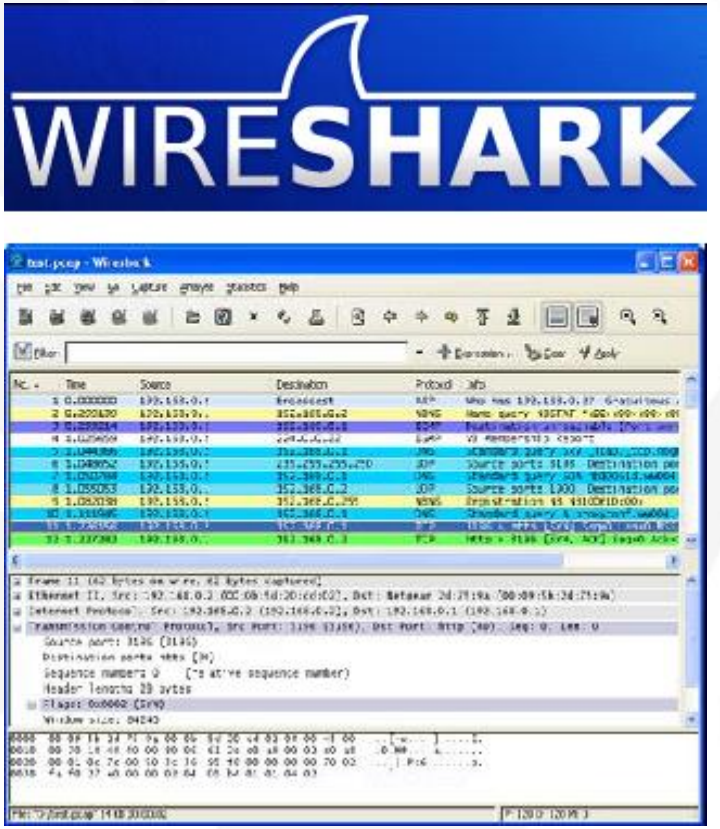
- Detects network vulnerabilities
- Open Ports
- Unnecessary Services / Applications
- Operating System vulnerabilities



PROTOCOL ANALYZERS

- Network ‘Sniffers’
- Wireshark
- Microsoft Network Monitor (Nmcap)





Controlling Data Throughput

- QoS (Quality of Service)
- Traffic Shaping (Bandwidth Shaping)
- Load Balancing
- High Availability – Clusters (Failover, NLB)
- Fault Tolerance – Redundant devices

Network Monitoring

- Baselines
- Performance Monitor
- System Logs (syslog)
- Traffic Analyser (Wireshark)
- SNMP – Simple Network Management Protocol

Windows Performance Monitoring