The preparation for a Cyber-Attack
The Cyber World

• Areas of concern
  – Cyber Espionage
  – Cyber Warfare
  – Cyber Crime
  – Cyber Terrorism
TARGETS AND MOTIVES

• Corporate
  – Types - DOS – SYN – ICMP – Port – DNS –
    • Trojans #1 attack and access method – over 79%
  – Thief –
    • Personnel info
    • Corporate info
  – Defacement
  – Takeover/control
  – Financial (directly)
  – Extortion
  – Revenge
  – Corporate or personnel image and reputation
• Individual/Personal – Yours and Family - entire Life
  – .............
• Governmental/Military
  – Secrets
  – Weapon Control
• Political, Religious......
Goals of Cyber-attacks

• Money
• Power
• Control
• Publicity
• Revenge
• Crackers
• Learning
• Future protection/Penetration testing
• Or Just to do it!
Data and data sources

» Intelligence

» Intelligence is lots of data – small pieces add up
  > Male/female
  > Initials to real name
  > Address
  > Residence
  > Work history
  > Type of system used
  > Weaknesses

» Where do you get data
  > Social networks
  > Stolen items – RFID’s, laptops, wallets, papers (trash)
  > Shoulder surfing – looking over someone's back
  > Phishing
  > Personally from employee or target person, internal mole
What is needed for a cyber attack

» Goal – Reason for attack – end desire

» Intelligence
  > Lots of data
  > Information

» Five steps in an attack
  > Reconnaissance
  > Probing
  > Actual attack
  > Maintaining presence
    + To continue original attack desired effect
    + To allow for future attacks
      – continued surveillance
      – Light footing
  > Covering attack track
    + How it was done
    + Access point
    + Residual for future or continued access
Information – many sources
Hooking the bones together!
Small easily found data!

- Small things hook big part together
  - Ligaments for human bones
  - Data for the cyber anatomy of the target

- Little items lead to big information
  - A family member
  - A phone number
  - A license plate
  - House street, number
  - Travel info
  - Pet info, friends info....etc
  - More small pieces of info – best place to
Data for Personal attack

The Eight piece puzzle for personal ID thief (Impersonation)

- Full Name
  - Including Spouse full info
- Address
  - Current
  - Last known
- Dependents and ages
  - Birth dates
- Phone Numbers
- Education
  - High School
  - College
  - Trade
- E-mail – already hacked
- Current employee

Any of theses –

- Social security – Drivers license – DOB and place – Hobbies – Family info

- the average CV/resume contains all of these
- Note: CVs can be easily obtained through fake recruitments
Data and info source tools

• Why not attack the server and clients
• Tools for Inside and outside exploits/data
  – Nmap – Top line scanner and exploit viewer
  – Nessus – Access Scanner
  – Nikto 2 – Web Scanner
    • Scripts as well as most applications
  – Armitage – Metasploit tool – good and bad
  – Hashcat – Password digger
  – WiFite – Wireless configuration tester
  – Wireshark – packet capture and analyzer
    • T-Shark – automated
      – With SNORT
  – SET – Social Engineering Toolset
    • Easy to use Human attack tool kit
  – MANY MORE – focused to general
    • OWASP, pMap, WIFI password dump, iSafe Keylogger, AFF...etc
    • Estimate over 1000 different tools for any OS
    • More to exploit Internet places – Facebook, Linkedin.....etc
Attack data and access sources

» Old Media attacks
  > Café wifi
  > School networks
  > Guest networks at corporations
  > Airplane and airport wifi

» New targets
  > 3 and 4 G networks
  > Public WLANs
  > Corporate tunnels
  > The cloud
  > WiFi everywhere
  > Cell phone and tablet platforms
  > WLAN’s
  > Physical attacks - Botting – Keyloggers (very common among financial institutions) - BIOS - Firmware

» DO NOT RULE OUT – PHYSICAL ACCESS
Problems—the why

Four Top Trends in cyber world

- Increase in Business Networks complexity
  - Bigger networks
  - Lack of visualization to recognize attacks and ploys
  - Less trained network employees

- Increasing criminal Motivation
  - More money on the net

- Increasing commoditization of weapon focused software
  - Hack for pay
  - Tools to hack for pay
  - Including specialized attack methods and support

- Lack of user knowledge
  - More users
  - More access methods
  - No training

- IPv6 or more accurately the push to transition from IP Before
Cyber Warfare – Enemies and Targets

» Top enemies – Espionage – Attacks - Communications
  > China, Iran, North Korea
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorists and others
  > Islamic terrorist...
Types of Cyber-attacks

- Types of Warfare attacks
  - Combination of any and all
    - Cyber and Physical
  - Nuclear
  - Military Command and control
    - Turn our weapons on us
  - Confusion
  - Social attacks
  - Monetary
    - Stock markets
    - Brokers
    - Federal Reserve
    - Banks
  - Probe attacks for potential all out warfare
    - One day they shut down everything
    - No money, no food production, no oil, no natural gas, no power
    - NO COMMUNICATIONS – TV, Radio, phones, cell, satellite
      - We have no back up communications
      - No POTS – Ham radio MAY be the only long range communications platform
The Anatomy of an attack

- Rational and reason for an attack
  - Just $
  - Revenge...etc
- Lots of data gathering leads to information leads to Intelligence about target or targets
  - To gain focus
- Small probing attacks
  - Vulnerability check
    - Network, Servers, Applications, Users
- Final Plan
  - Target
  - Method
  - Outside influences
- The Attack
  - Small nibble
  - Persistent threat
  - All out Cyber Attack
  - Cyber and Physical
- The retreat plan
  - All out with no trail or diversion trail
  - Back door or other malware let behind
  - Knowledge of weaknesses
- The future attack plan or drain of information, money or access to a deeper attack
End

The reality is that we will be attacked — Not IF but When!

There is no real end in sight, as long as there are cyber criminals, warriors and attacks! The future will be 100% CYBER WARFARE in all of its forms!