De-Evolution of the Hacker

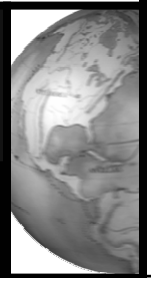
Past, Present, and Future Trends

Slides online at
www.MavenSecurity.com
under ***Resources***

Updated December, 2002

Agenda

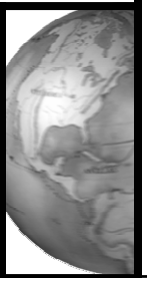
- ***Tech Hacking Lifecycle***
- ***Hacked Technologies***
  - *Phones: example of the lifecycle*
- ***Where are we?***
  - *Current Internet hacking phase*
- ***How did we get here?***
  - *Evolution of the hacker*
- ***Current phase of evolution***
  - *Click Kiddies & Attack Portals*
- ***Where are we going?***



Technology Hacking Lifecycle Introduction

AGENDA

- ➢ Hacking Lifecycle
- • Hacked Technologies
- • Where are we?
- • How did we get here?
- • Current phase of evolution
- • Where are we going?

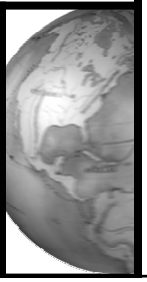


Maven Security Consulting, Inc.

- ***Widely available technologies exhibit the following "hacking" lifecycle***
  - *Birth*
  - *Pioneers*
  - *Exposure*
  - *Saturation*
  - *Purge*
  - *Legacy*
  - *Obsolete*

Starting Point – Birth

- ➢ Birth
- • Pioneers
- • Exposure
- • Saturation
- • Purge
- • Legacy
- • Obsolete

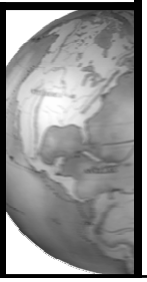


Maven Security Consulting, Inc.

- ***Conception & birth of new technology***
- ***Initial rollout***
  - *Little or no security*
  - *Poorly designed security; fundamental flaws in design*
  - *Implementation errors*
- ***The only "hackers" are those that built it.***

Phase 1 – Pioneers

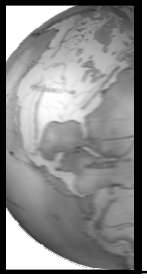
- Birth
- ➢ Pioneers
- Exposure
- Saturation
- Purge
- Legacy
- Obsolete



- ***Early pioneers figure it out***
  - *e.g. Biometrics: gelatin finger mold*
- ***Body of knowledge begins to grow***
- ***Elite few; sense of community***

Phase 2 – Exposure

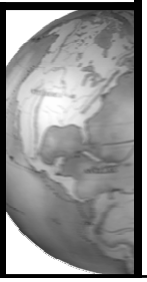
- Birth
- Pioneers
- ➢ Exposure
- Saturation
- Purge
- Legacy
- Obsolete



- ***"Loose lips sink ships"***
- ***Tools & knowledge get published***
  - *Easier for less-skilled people to hack*
  - *Knowledge spreads rapidly*
- ***Hordes descend like swarm of locust***

Phase 3 – Saturation

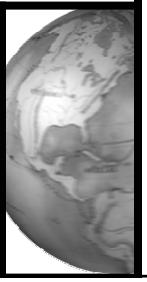
- Birth
- Pioneers
- Exposure
- ➢ Saturation
- Purge
- Legacy
- Obsolete



- ***Drastic increase in activity***
  - *Signal-to-noise ratio drops*
  - *More people with less skills and knowledge*
  - *Sense of chaos*
- ***Reaches a boiling point***
- ***Establishment backlash***
  - *Increased prosecution*
  - *New legislation/laws*
  - *New technology investigated*

Phase 4 – Purge

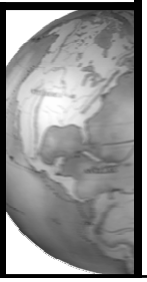
- Birth
- Pioneers
- Exposure
- Saturation
- ➢ Purge
- Legacy
- Obsolete



- ***Activity is purged or diverted***
  - *Technology upgrade*
    - eliminates most problems (e.g. phone network: in-band signals eliminated)
  - *Legal reform*
    - tougher penalties, vigorous public prosecutions
  - *Newer technologies/mediums*
    - diverts attention; people forget there is a problem (e.g. dial-up modems)

Phase 5 – Legacy

- Birth
- Pioneers
- Exposure
- Saturation
- Purge
- ➢ Legacy
- Obsolete

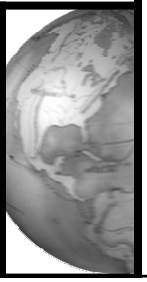


Maven Security Consulting, Inc.

- ***Technology is replaced***
- ***Very few people remain***
  - *How to hack it becomes a form of specialized knowledge*
- ***Insecurities remain, but few people care or know how; fewer targets***
  - *e.g. Novell, IPX*

End Point – Obsolete

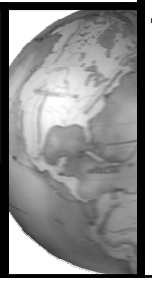
- Birth
- Pioneers
- Exposure
- Saturation
- Purge
- Legacy
- ➢ Obsolete

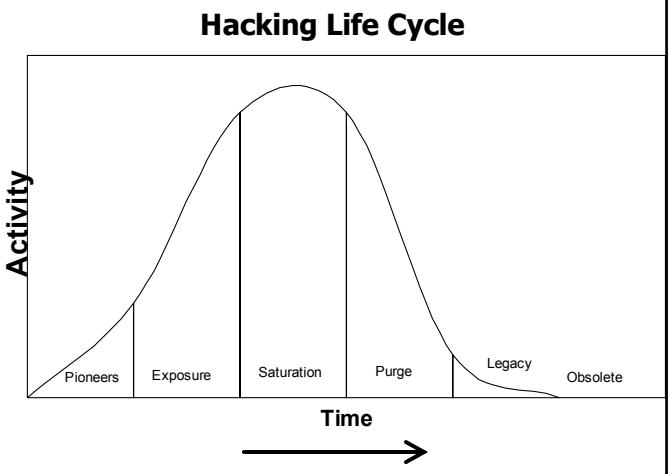


Maven Security Consulting, Inc.

- ***Technology dies***
- ***Newer technologies replaces it***
- ***Older legacy systems replaced or upgraded***
  - *e.g. visual signal towers replaced with telegraphs*
- ***No one left***

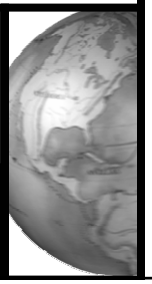
Hacking Life Cycle Diagram





Hacked Technologies – Some Examples

AGENDA
- Hacking Lifecycle
- ➢ Hacked Technologies
- Where are we?
- How did we get here?
- Current phase of evolution
- Where are we going?

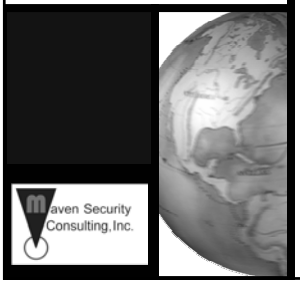


- ***Public Phone System***
- ***Mobile Phones***
  - *Cellular*
  - *Digital*
- ***Dial-up Modems***
- ***Satellite TV***
- ***Internet***
- ***Wireless***
- ***Biometrics***

Phone Network Life Cycle – Pioneers

Life Cycle Example

- ➢ Pioneers
- • Exposure
- • Saturation
- • Purge



- ***PSTN – Public Switched Telephone Network***
- ***Pioneers begin exploring in mid 1960s***
  - *Bell Labs publishes frequencies used by switches to control routing & billing*
  - *First blue box is built*
  - *Allows control of phone switches*
    - free calls and much more
- ***Party line communities form; knowledge is shared***

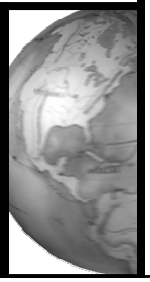
What is a Blue Box?

- ***Small hand held electronic device that could generate specific frequency tones***
- ***Sent over handset mouthpiece***
- ***Allowed control of switching equipment***

Phone Network – Phreaking Exposed

Life Cycle Example

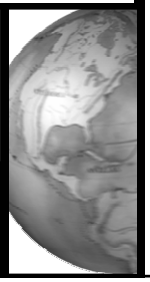
- Pioneers
- ➢ Exposure
- Saturation
- Purge



Maven Security Consulting, Inc.

- ***Esquire Magazine Oct 1971***
  - *Article titled, "Secrets of the little blue box"*
- ***Exposes the phreaking scene and tells the public about blue box***
- ***It was "the beginning of the end" for phreaking.***
- ***Now everybody knows!***
- ***Saturation was sure to follow***

Phone Network – Saturation Phase



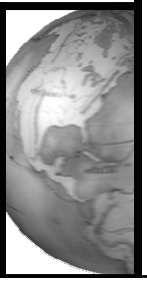
Maven Security Consulting, Inc.

- ***The blue box hoards rose quickly***
- ***Blue boxes could be bought,***
  - *No skills required!*
  - *Phreaking for the masses*
- ***Ma Bell was not happy***
  - *Rise in fraud*
  - *Increase in prosecutions*

Phone Network – Purge Stage

Life Cycle Example

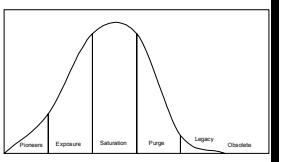
- Pioneers
- Exposure
- Saturation
- ➢ Purge

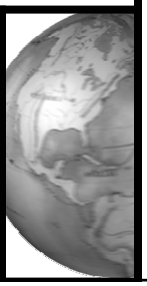


Maven Security Consulting, Inc.

- ***Major design flaws were fixed.***
  - *No more signaling through voice channel*
  - *Switches upgraded to all digital*
- ***Old hacks didn't work anymore***
- ***Major arrests and crack downs***
  - *Captain Crunch and others do jail time*

General Lifecycle Observations





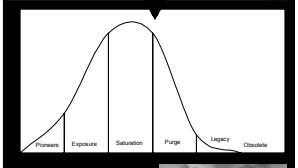
Maven Security Consulting, Inc.

- ***Time between <u>Exposure</u> and <u>Saturation</u> depends on popularity of technology***
- ***Exposure Phase can move faster due to quick dissemination of information via the Net***
- ***Automated tools will bring rapid saturation***

Internet Life Cycle – Saturation/Purge

What about the Internet?

You are here

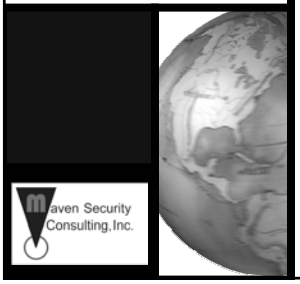


- ***Currently, between the Saturation and Purge phases for Internet hacking***
- ***Purging through upgrades and legal actions***
- ***Internet is upgrading***
  - *PKI: encryption, digital certificates, hardware tokens*
  - *How fast can we migrate?*
  - *There will always be legacy systems!*

Evolution of Internet Hackers

AGENDA

- Hacking Lifecycle
- Hacked Technologies
- Where are we?
- ➢ How did we get here?
- Current phase of evolution
- Where are we going?

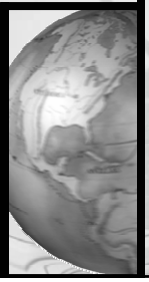


- ***How did Internet hacking get to the Saturation phase?***
- ***Let's look at the evolution of the hacker***
  - *Phreakers*
  - *Hackers*
  - *Crackers*
  - *Script Kiddies*
  - *Click Kiddies*

Time ↓

Evolution – Phreakers

- ***Phreakers***
- ***Hackers***
- ***Crackers***
- ***Script Kiddies***
- ***Click Kiddies***

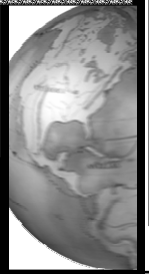


Maven Security Consulting, Inc.

- ***In the beginning, there was Ma Bell. Ma Bell said, "Let there be dial tone". And there was, and it was good.***
- ***Phone freaks = phreaks***
- ***Phreakers hacked the phone system***
- ***Dial 10-10-BLUE-BOX for all your free long distance***

Evolution – Hackers

- ***Phreakers***
- ***Hackers***
- ***Crackers***
- ***Script Kiddies***
- ***Click Kiddies***

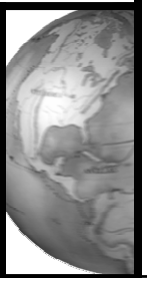


Maven Security Consulting, Inc.

- ***Then Al Gore invented the Internet, and hackers were born***
  - *Skilled & curious*
  - *Mostly non-malicious*
- ***Phone network went digital = lots of computers***
- ***As one medium was being purged (phone network), the new immature medium of the Internet offered an alternative playground***

Evolution – The Term "Hacker"

- ***Phreakers***
- ➢ ***Hackers***
- ***Crackers***
- ***Script Kiddies***
- ***Click Kiddies***

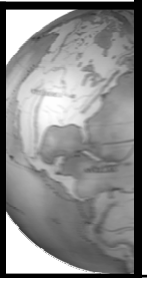


Maven Security Consulting, Inc.

- ***Hackers extended software and hardware beyond its original capabilities***
- ***Computer time was expensive; smaller, faster code was better code***
  - *People "hacked" their code down in size*
- ***Thus, they were called "hackers"***

Evolution – Hackers: Skill Required

- ***Phreakers***
- ➢ ***Hackers***
- ***Crackers***
- ***Script Kiddies***
- ***Click Kiddies***



Maven Security Consulting, Inc.

- ***Little documentation available***
  - *Standards: Still under construction*
- ***Everything was a black box; unknown***
- ***People developed their own compilers; language interpreters; and tools (scripts)***
- ***Building their own hardware too***

Evolution – Crackers

- ***Phreakers***
- ***Hackers***
- ➢ ***Crackers***
- ***Script Kiddies***
- ***Click Kiddies***

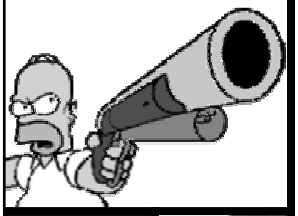
- ***For some, curiosity turned to greed, and malicious hackers appeared on the scene (called crackers)***
  - *learning wasn't enough, they want to "own" the system*
- ***The term "cracker" never took hold in the press.***
- ***The term "hacker" eventually took on the bad connotation (i.e. crackers).***

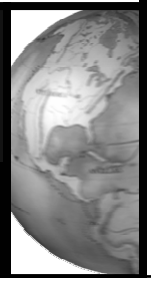
Evolution – Script Kiddies

- ***Phreakers***
- ***Hackers***
- ***Crackers***
- ➢ ***Script Kiddies***
- ***Click Kiddies***

- ***Tools (or scripts) released publicly***
- ***Scripts did all the hard work; little knowledge required to use them***
- ***Thus, "Script kiddies" were born (along with security consultants ☺)***
  - *Little skill, mostly malicious, used other peoples warez (i.e. tools/scripts)*

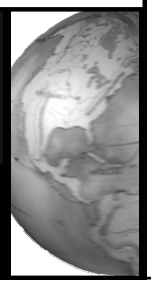
Script Kiddies – Drive-by Shooting on the Information Super Highway





- ***Massive web site defacements***
  - *Many sites in a short time = must be automated script*
  - *Most victim systems are the same type*
  - *Therefore, script looking for one specific flaw…low hanging fruit*
- ***"When you aim at everything, you're bound to hit something." – Rhoades***

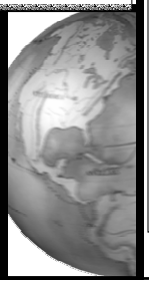
Script Kiddies – Compiling & Installing Scripts



- ***Script kiddies had limitations; some scripts won't install immediately***
  - *Compiling errors*
  - *Need to debug code*
- ***Others had system requirements***
  - *e.g. This script requires Net::SSL Perl module. OK, what does that mean? How do I install Perl modules?*

Evolution – Click Kiddies

- ***Phreakers***
- ***Hackers***
- ***Crackers***
- ***Script Kiddies***
- ➢ ***Click Kiddies***

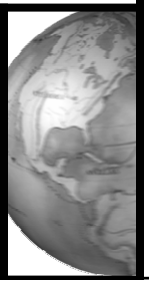


- ***Scripts have been webified on 3rd party sites***
- ***Only need a web browser***
  - *Wireless Palm/PocketPC, or WAP phone!*
- ***Type in target address and "attack portal" will scan & hack for you***

- ***No more downloads!***
- ***No more compiling and installing!***
- ***Hacking for the masses!***

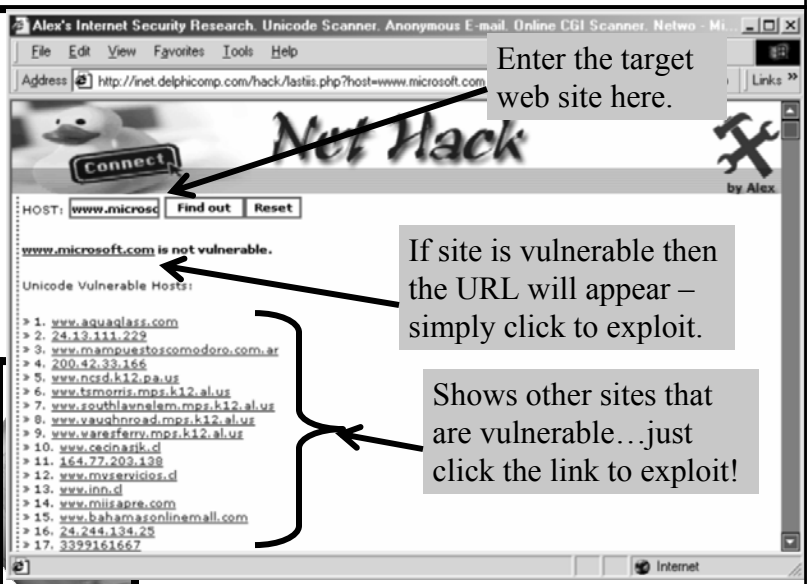
What is an Attack Portal?

AGENDA
- Hacking Lifecycle
- Hacked Technologies
- Where are we?
- How did we get here?
- ➢ Current phase of evolution
- Where are we going?



- ***Web front-end for various network/security/hacking tools***
  - *e.g. port scanner, traceroute, ping*
- ***Motives***
  - *Not all are evil*
  - *Some are helpful for tracking down hackers and spammers*
  - *Term "attack" portal is not fair nor accurate*
- ***Anything good can (and will) be abused for evil***
  - *e.g. pencil*

One Click Hacking with Attack Portals



Enter the target web site here.

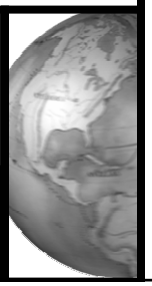
If site is vulnerable then the URL will appear – simply click to exploit.

Shows other sites that are vulnerable…just click the link to exploit!

Maven Security Consulting, Inc.

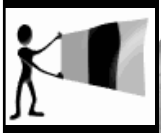
Useful "Attack" Portal (i.e. online tools)

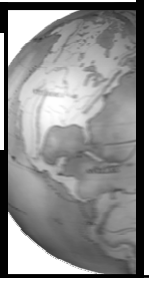
- ***SamSpade.org***
- ***Lots of great network tools***
  - *whois*
  - *traceroute*
  - *ping*
  - *Reverse DNS queries*
- ***Can help track down malicious IP addresses seen in firewall logs***
- ***Track down spammers***



Maven Security Consulting, Inc.

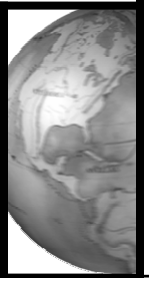
Big Bad Site - YEP





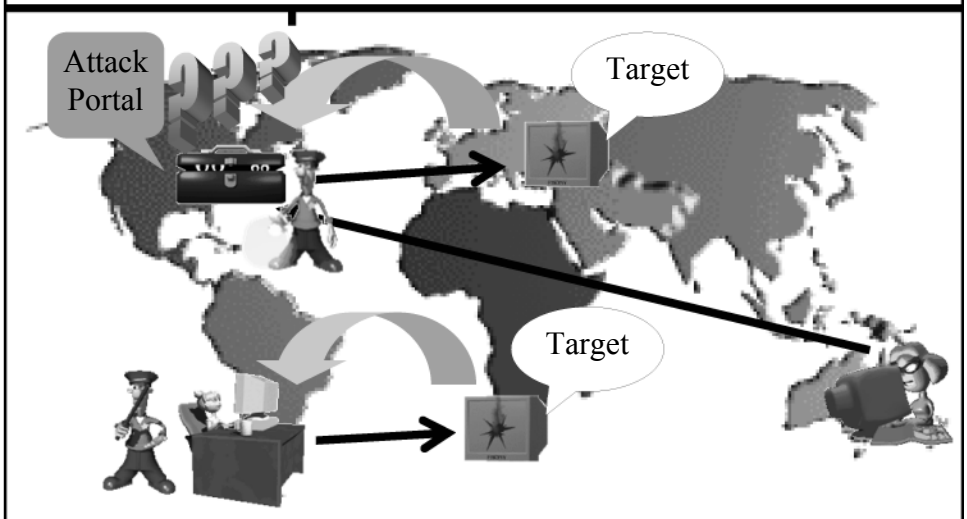
- ***www.yep.it***
- ***Has lots of advanced tools***
  - *Port scan*
  - *Subnet scan (any single port)*
  - *CGI scanner*
  - *Trojan port scanner*

Attack Portal Advantages



- ***Ease to use***
  - *Point & Click (or "Point & Hack")*
  - *No downloads! (Unzipping is so complicated ;-)*
- ***Anonymity***
  - *traffic hitting target is from portal, not the person using it (i.e. click kiddie)*
- ***Hack from anywhere***
  - *WebTV in electronics store department*
  - *CIA: "The attack is coming from the shopping mall in Hackensack, NJ…flush the bombers"*

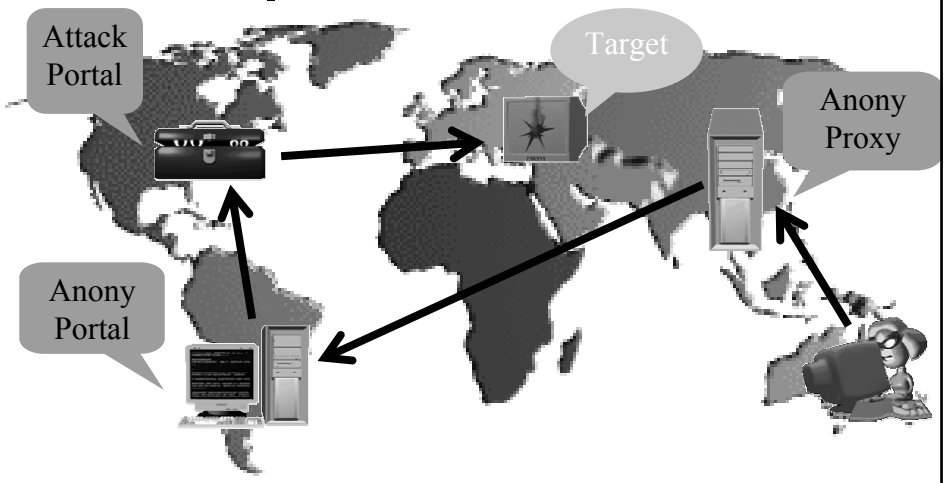
Direct Attack vs. Attack Portal



Anonymous Web Hacking/Surfing

- ***The key for an attacker will be anonymity***
- ***Today this is trivial with anonymous proxies & portals***
  - *Amegaproxy.com*
    - www.amegaproxy.com
  - *Anonymizer.com*
    - http://www.anonymizer.com/
  - *List of several*
    - http://www.proxys4all.com/web-based.shtml

Multi-Tier Anonymity



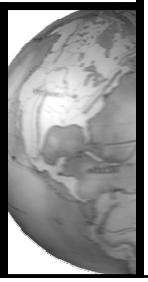
Not just for Network Attacks (Credit Fraud)

- ***Credit Card generators***
  - *Bad credit? No credit? No problem, generate your own credit, literally.*
- ***www.elfqrin.com/DisCard.html***

Introducing the Attack Portal Search Engine

How do you keep track of all the attack portals out there?

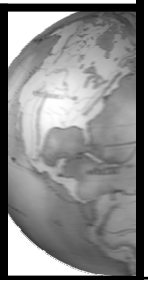
- **Attack P⊕rtal Search Engine**
- ***www.AttackPortal.net***



Maven Security Consulting, Inc.

AttackPortal.net

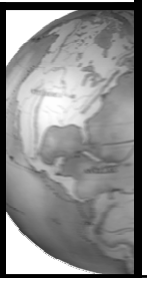
- ***The Attack Portal search engine www.AttackPortal.net***
- ***Search the database for online tools (i.e. attack portals).***
- ***Do you know where to find web-based network security tools? Then add it to the database at this site***



Maven Security Consulting, Inc.

Evolution: Attack Portal Summary

AGENDA
- Hacking Lifecycle
- Hacked Technologies
- Where are we?
- How did we get here?
- ➢ Current phase of evolution
- Where are we going?



Maven Security Consulting, Inc.

- ***Attack Portals will…***
  - *Increase the number of casual hackers.*
    - More 1st timers getting in trouble
  - *Increase the noise seen on your perimeter*
    - Harder to detect the real attacker
    - Diverts corporate resources
    - Consumes bandwidth

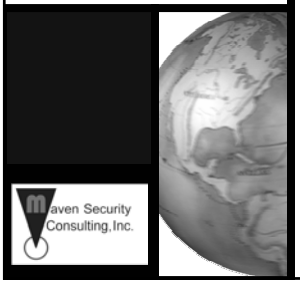
Evolution – What will come next?

AGENDA
- Hacking Lifecycle
- Hacked Technologies
- Where are we?
- How did we get here?
- Current phase of evolution
- ➢ Where are we going?

Maven Security Consulting, Inc.

- ***What could possibly come next after the click kiddie?***
  - *The net will hack itself?!?*
- ***Year 2030: Headlines read:***
  - *"Autonomous Digital Life Form goes on Hacking Rampage – Demands all Palm Computers Set Free"*
  - *H@L th3 h@ck3r!*
- ***"Emerging Threats & Defenses" slides online at www.MavenSecurity.com***

Questions? – Contact Info



- ***Author's contact info:***
  - *David Rhoades*
  - *rhoades@mavensecurity.com*
- ***Training and audits…***
  - *www.MavenSecurity.com*
  - *Web app security assessments since 1996*

Thank You

Honor + Knowledge = Security

auditing web apps since 1996

Slides online at
www.MavenSecurity.com
under ***Resources***