Footprinting, Recon & Scanning

Ronald Osure

KENET Cyber Security Training
October 26th - 30th 2015

Agenda

- Footprinting and Reconnaissance
- Network Scanning

Footprinting

Module Flow

Footprinting is the first step in ethical hacking, w here an attacker tries to gather information about a target

Footprinting Terminology

- Open Source or Passive information gathering
- Anonymous footprinting
- Organizational or private footprinting
- Active Information Gathering
- Pseudonymous footprinting
- Internet Footprinting

Footprinting Process

Why Footprinting

- Know Security Posture
- Reduce Attack Area
- Build Information Database
- Draw Network Map

Footprinting Threats

- Social Engineering
- System and Network Attacks
- Information Leakage
- Privacy Loss
- Corporate Espionage
- Business Loss

Footprinting Methodology

- Search Engines
- Websites
- Email
- Competitive Intelligence
- Google (Google Hacking)
- Whois
- DNS
- Network
- Social Engineering
- Social Networking Sites

Network Scanning

The process of gathering additional details about the target using highly complex and aggressive reconnaissance techniques is called scanning

Do Not Scan These IP Addresses

(Unless you want to get into trouble)

Hack the Universe

RANGE 128
128.37.0.0 Army Yuma Proving Ground
128.38.0.0 Naval Surface Warfare Center
128.43.0.0 Defence Research Establishment-Ottawa
128.47.0.0 Army Communications Electronics Command
128.49.0.0 Naval Ocean Systems Center
128.50.0.0 Department of Defense
128.51.0.0 Department of Defense
128.56.0.0 U.S. Naval Academy
128.60.0.0 Naval Research Laboratory
128.63.0.0 Army Ballistics Research Laboratory
128.80.0.0 Army Communications Electronics Command
128.102.0.0 NASA Ames Research Center
128.149.0.0 NASA Headquarters
128.154.0.0 NASA Wallops Flight Facility
128.155.0.0 NASA Langley Research Center
128.156.0.0 NASA Lewis Network Control Center
128.157.0.0 NASA Johnson Space Center
128.158.0.0 NASA Ames Research Center
128.159.0.0 NASA Ames Research Center
128.160.0.0 Naval Research Laboratory
128.161.0.0 NASA Ames Research Center
128.183.0.0 NASA Goddard Space Flight Center
128.202.0.0 50th Space Wing
128.216.0.0 MacDill Air Force Base
128.217.0.0 NASA Kennedy Space Center
128.236.0.0 U.S. Air Force Academy

RANGE 129
129.23.0.0 Strategic Defense Initiative Organization
129.29.0.0 United States Military Academy
129.50.0.0 NASA Marshall Space Flight Center
129.51.0.0 Patrick Air Force Base
129.52.0.0 Wright-Patterson Air Force Base
129.53.0.0 - 129.53.255.255 66SPTG-SCB
129.54.0.0 Vandenberg Air Force Base, CA
129.92.0.0 Air Force Institute of Technology
129.99.0.0 NASA Ames Research Center
129.131.0.0 Naval Weapons Center
129.163.0.0 NASA/Johnson Space Center
129.164.0.0 NASA IVV
129.165.0.0 NASA Goddard Space Flight Center
129.167.0.0 NASA Marshall Space Flight Center
129.168.0.0 NASA Lewis Research Center
129.190.0.0 Naval Underwater Systems Center
129.198.0.0 Air Force Flight Test Center
129.209.0.0 Army Ballistics Research Laboratory
129.229.0.0 U.S. Army Corps of Engineers
129.251.0.0 United States Air Force Academy

RANGE 130
130.40.0.0 NASA Johnson Space Center
130.90.0.0 Mather Air Force Base
130.109.0.0 Naval Coastal Systems Center
130.124.0.0 Honeywell Defense Systems Group
130.165.0.0 U.S.Army Corps of Engineers
130.167.0.0 NASA Headquarters

RANGE 131
131.6.0.0 Langley Air Force Base
131.10.0.0 Barksdale Air Force Base
131.17.0.0 Sheppard Air Force Base
131.21.0.0 Hahn Air Base
31.32.0.0 37 Communications Squadron
131.35.0.0 Fairchild Air Force Base
131.36.0.0 Yokota Air Base
131.37.0.0 Elmendorf Air Force Base
131.38.0.0 Hickam Air Force Base
131.39.0.0 354CS/SCSN

RANGE 132
132.3.0.0 Williams Air Force Base
132.5.0.0 - 132.5.255.255 49th Fighter Wing
132.6.0.0 Ankara Air Station
132.7.0.0 - 132.7.255.255 SSG/SINO
132.9.0.0 28th Bomb Wing
132.10.0.0 319 Comm Sq
132.11.0.0 Hellenikon Air Base
132.12.0.0 Myrtle Beach Air Force Base
132.13.0.0 Bentwaters Royal Air Force Base
132.14.0.0 Air Force Concentrator Network
132.15.0.0 Kadena Air Base
132.16.0.0 Kunsan Air Base
132.17.0.0 Lindsey Air Station
132.18.0.0 McGuire Air Force Base
132.19.0.0 100CS (NET-MILDENHALL)
132.20.0.0 35th Communications Squadron
132.21.0.0 Plattsburgh Air Force Base
132.22.0.0 23Communications Sq
132.24.0.0 Dover Air Force Base
132.25.0.0 786 CS/SCBM
132.27.0.0 - 132.27.255.255 39CS/SCBBN
132.28.0.0 14TH COMMUNICATION SQUADRON
132.30.0.0 Lajes Air Force Base
132.31.0.0 Loring Air Force Base
132.33.0.0 60CS/SCSNM
132.34.0.0 Cannon Air Force Base
132.35.0.0 Altus Air Force Base
132.37.0.0 75 ABW
132.38.0.0 Goodfellow AFB
132.39.0.0 K.I. Sawyer Air Force Base

Types of Scanning

- Port Scanning
- Network Scanning
- Vulnerability Scanning

Objectives of Network Scanning

- Discover live hosts
- Discover open ports
- Discover OS and system architecture
- Identify vulnerabilities and threats
- Detecting the associated network service of each port

Scanning Methodology

- Check for live systems (ping sweep)
- Check for open ports (3 way handshake)
- Scanning beyond IDS (packet fragmenting)
- Banner Grabbing
- Scan for vulnerability
- Draw Network Diagrams
- Prepare proxies
- Scanning Pen Testing

Case: Bloggers Write Text Backwards to Bypass Web Filters in China

Bloggers and journalists in China are using a novel approach to **bypass Internet filters** in their country – they write backwards or from right to left

The content therefore remains readable by human beings but defeats the **web filtering software**

China is implementing **'packet filtering'** to detect TCP packets containing controversial keywords such as Tibet, Democracy, Tiananmen, etc.

Port Scanning Countermeasures

- Firewalls to catch probes
- IDS to catch OS detection method
- Open only necessary ports
- Audit your own network with same tools

References

- CEH course work