Scanning Networks

Module 3

Engineered by Hackers. Presented by Professionals.
Your identity is for sale on Internet black markets

The online black markets, called carding sites, deal in big batches of folks' Visa-card numbers, PIN numbers and more, Kerry Tomlinson, an investigative reporter with KATU TV News, told an audience on Nov. 4 during Scam Jam 2010, organized by the Better Business Bureau and held at Jantzen Beach Center.

About a dozen experts from agencies and groups including the FBI, U.S. Postal Inspection Service, Federal Trade Commission and Portland Crime Prevention spoke about scams.

One report you'll find describes http://www.shadowcrew.com, a global website with thousands of members who conducted their business anonymously, using nicknames and passwords, and running their online business through "proxy servers," separate computers that cover their trails by not revealing the true IP addresses on the crooks' computers. Shadowcrew operated for two years before being taken down after a yearlong undercover operation by the U.S. Secret Service.

"Shadowcrew members collectively trafficked in at least 1.5 million stolen credit card numbers that resulted in over $4 million in actual losses to credit card companies and financial institutions," says the report. It was written by Kimberly Kiefer Peretti, a senior counsel with the U.S. Department of Justice's Computer Crime & Intellectual Property Section.

http://www.thenewtribune.com
Module Objectives

- Definition and Types of Scanning
- Understanding CEH Scanning Methodology
- Checking Live Systems and Open Ports
- Understanding Scanning Techniques
- Different Tools Present to Perform Scanning
- Understanding Banner Grabbing and OS Fingerprinting
- Drawing Network Diagrams of Vulnerable Hosts
- Preparing Proxies
- Understanding Anonymizers
- Scanning Countermeasures
- Scanning Pen Testing
Scanning refers to a set of procedures for identifying hosts, ports, and services in a network.

Scanning is one of the components of intelligence gathering for an attacker to create a profile of the target organization.
**Types of Scanning**

**Port Scanning**
A series of messages sent by someone attempting to break into a computer to learn about the computer’s network services. Each message is associated with a "well-known" port number.

**Vulnerability Scanning**
The automated process of proactively identifying vulnerabilities of the computing systems present in a network.

**Network Scanning**
A procedure for identifying the active hosts on a network. Either for the purpose of attacking them or for network security assessment.
Ping scan involves sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply.

This scan is useful for **locating active devices** or determining if **ICMP** is passing through a **firewall**.

### Source | Destination | Summary
---|---|---
192.168.168.3 | 192.168.168.5 | ICMP: Echo
192.168.168.5 | 192.168.168.3 | ICMP: Echo Reply

**The ping scan output using Nmap:**

```
# nmap -sP -v 192.168.168.5
Starting nmap 5.21 (http://nmap.org) at 2010-07-11 16:30 EDT
Host 192.168.168.5 appears to be up.
MAC Address: 00:E0:48:12:CD:9A (Hewlett Packard)
Nmap finished: 1 IP address (1 host up) scanned in 0.889 seconds
Raw packets sent: 5 (30B) | Rcvd: 2 (25B)
```
Ping Sweep

Ping sweep is used to determine the **live hosts from a range of IP addresses** by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply.

Attacker use ping sweep to create **inventory of live systems** in a network.

---

**The ping sweep output using Nmap:**

```
nmap -sn -PE -PA 21, 23, 80, 3389 192.168.168.1-50
```

Starting Nmap 5.21 (http://nmap.org) at 2010-07-13 14:16 EDT
Nmap scan report for 192.168.168.1
Host is up (0.00s latency).
MAC Address: 00:A8:5A:E0:83:05 (Hewlett Packard)
Nmap scan report for 192.168.168.2
Host is up (0.016s latency).
MAC Address: 00:01:6B:0A:8E:15 (Foxconn)
Nmap scan report for 192.168.168.4
Host is up (0.00s latency).
MAC Address: 00:2A:B9:03:DD:80 (Dell)
Nmap scan report for 192.168.168.6
Host is up (0.00s latency).```
Ping Sweep Tools

Angry IP Scanner

SolarWinds Engineer's Toolset

http://www.angryip.org

http://www.solarwinds.com
Ping Sweep Tools

Colasoft Ping Tool
http://www.colasoft.com

Ping Scanner Pro
http://www.digilextechnologies.com

SolarWinds Standard Edition
http://www.solarwinds.com

Ultra Ping Pro
http://ultraping.netfirms.com

Utility Ping
http://www.wavget.com

PingInfoView
http://www.nirsoft.net

Visual Ping Tester
http://www.pingtester.net

PacketTrap pt360
http://www.packettrap.com
CEH Scanning Methodology

Check for Live Systems → Check for Open Ports → Banner Grabbing

Prepare Proxies ← Draw Network Diagrams ← Scan for Vulnerability
TCP uses a **three-way handshake** to establish a connection between server and client.

1. The Computer A (10.0.0.2) initiates a connection to the server (10.0.0.3) via a packet with only the **SYN** flag set.

2. The server replies with a packet with both the **SYN** and the **ACK** flag set.

3. For the final step, the client responds back to the server with a single **ACK** packet.

4. If these three steps are completed without complication, then a TCP connection is established between the client and the server.
TCP Communication Flags

SYN (Synchronize)
Used to initiate a connection between hosts

URG (Urgent)
It states that the data contained in the packet should be processed immediately

ACK (Acknowledgement)
Used to acknowledge the receipt of a packet

FIN (Finish)
It tells the remote system that there will be no more transmissions

PSH (Push)
Used to instruct the sending system to send all buffered data immediately

RST (Reset)
Used to reset a connection

Standard TCP communications are controlled by flags in the TCP packet header
Create **Custom Packet** using TCP Flags
Hping2 / Hping3

It is a command line packet crafter for the TCP/IP protocol

Tool for security auditing and testing firewall and networks

It runs on both Windows and Linux operating systems

hping3 is a scriptable TCL language command line tool compatible with hping2
Hping Commands

**ICMP Ping**
```
hping3 -l 10.0.0.25
```

**SYN scan on port 50-60**
```
hping3 -c 50-60 -s 10.0.0.25 -V
```

**ACK scan on port 80**
```
hping3 -A 10.0.0.25 -p 80
```

**FIN, PUSH and URG scan on port 80**
```
hping3 -F -p -U 10.0.0.25 -p 80
```

**UDP scan on port 80**
```
hping3 -c 10.0.0.25 -p 80
```

**Scan entire subnet for live host**
```
hping3 -c 10.0.1.x --rand-dest --I eth0
```

**Collecting Initial Sequence Number**
```
hping3 192.168.1.103 -Q -p 139 -s
```

**Intercept all traffic containing HTTP signature**
```
hping3 -9 HTTP -I eth0
```
Scanning Techniques

- SYN/ACK/FIN Scan
- Stealth Scan
- XMAS Scan
- NULL Scan
- IDLE Scan
- Inverse Mapping Scan
- TCP Connect Scan
TCP Connect / Full Open Scan

- TCP Connect scan detects when a port is open by completing the three-way handshake.
- TCP Connect scan establishes a full connection and tears it down by sending a RST packet.

**Diagram:**
- **Attacker** sends a SYN Packet + Port (n) to the **Target**.
- The Target responds with a SYN / ACK Packet.
- The Attacker sends an ACK + RST packet to tear down the connection.

**Legend:**
- SYN Packet
- ACK Packet
- RST Packet

**Note:**
- This diagram illustrates the sequence of packets in the three-way handshake process used in TCP Connect scans.
Stealth Scan (Half-open Scan)

Attackers use **stealth scanning techniques** to bypass firewall rules, logging mechanism, and hide themselves as usual network traffic.

1. The client sends a single **SYN** packet to the server on the appropriate port.

2. If the port is open then the server responds with a **SYN/ACK** packet.

3. If the server responds with an **RST** packet, then the remote port is in the "closed" state.

4. The client sends the **RST** packet to close the initiation before a connection can ever be established.
Xmas Scan

- Xmas scan sends a TCP frame to a remote device with URG, ACK, RST, SYN, and FIN flags set.
- FIN scan only with OS TCP/IP developed according to RFC 793.
- It will not work against any current version of Microsoft Windows.

The Xmas scan output using Nmap:

```
# nmap -sX -v 10.0.0.8

Starting nmap 5.21 (http://nmap.org) at 2010-07-11 16:30 EDT
Initiating XMAS Scan against 10.0.0.8 [1663 ports] at 21:18
The XMAS Scan took 1.55s to scan 1663 total ports
Host 10.0.0.8 appears to be up ... good.
Interesting ports on 10.0.0.8:
(The 1654 ports scanned but not shown below are in state: closed)
PORT     STATE      SERVICE
21/tcp    open|filtered  ftp
22/tcp    open|filtered  ssh
79/tcp    open|filtered  finger
110/tcp   open|filtered  POP3
514/tcp   open|filtered  Shell
```
FIN scan sends a TCP frame to a remote device with FIN flag set.

FIN scan only with OS TCP/IP developed according to RFC 793.

It will not work against any current version of Microsoft Windows.

In FIN scan, attackers send a TCP frame to a remote host with only FIN flags set.

nmap -sF 192.168.168.13

Starting Nmap 5.21 (http://nmap.org) at 2010-07-15 20:51 EST

Nmap scan report for 192.168.168.13
Host is up (0.000052s latency).
All 1000 scanned ports on 192.168.168.13 are closed
MAC Address: 00:15:58:A1:07:B2 (Foxconn)
Nmap done: 1 IP address (1 host up) scanned in 5.55 seconds.
**NULL Scan**

- **Attacker**: 10.0.0.6
- **Server**: 10.0.0.8:23

**TCP Packet with NO Flag Set**
- **No Response**: Port is open
- **RST/ACK**: Port is closed

- **NULL scan only works** if OS’ TCP/IP implementation is developed according to RFC 793
- **It will not work against any current version of Microsoft Windows**

```
nmap -sN 192.168.168.13
Starting Nmap 5.21 (http://nmap.org) at 2010-07-15 21:10 EST
Nmap scan report for 192.168.168.13 Host is up (0.00s latency).
All 1000 scanned ports on 192.168.168.13 are open|filtered
MAC Address: 00:15:58:A1:07:B2 (FoxConn)
Nmap done: 1 IP address (1 host up) scanned in 29.03 seconds
```

In NULL scan, attackers send a TCP frame to a remote host with NO Flags
Most network servers listen on TCP ports, such as **web servers on port 80** and **mail servers on port 25**. Port is considered “open” if an application is listening on the port.

One way to determine whether a port is open is to **send a "SYN" (session establishment) packet to the port**.

The target machine will send back a **"SYNACK" (session request acknowledgment) packet if the port is open, and an "RST (Reset) packet if the port is closed**.

A machine which receives an **unsolicited SYN|ACK packet** will respond with an RST. An unsolicited RST will be ignored.

Every IP packet on the Internet has a **"fragment identification" number**.

It is a TCP port scan method that allows sending spoofed packets to a computer through software tools such as **Nmap** and **Hping**.
IDLE Scan: Step 1

1. Send SYN/ACK packet to the zombie machine to **probe its IPID number**
2. Every IP packet on the Internet has a fragment identification number (IP ID), which is a 4 digit number that **increases every time a host sends IP packet**
3. Zombie not expecting a SYN/ACK packet will send **RST packet**, disclosing the IP ID
4. Analyze the RST packet from zombie machine to **extract IPID**
IDLE Scan: Step 2.1 (Open Port)

- Send SYN packet to the **target machine (port 80)** spoofing the IP address of the “zombie”

![Diagram showing the flow of packet transmission](image-url)

- **Attacker**
- **Zombie**
- **Target**

- SYN Packet to port 80 spoofing zombie IP address
- SYN/ACK Packet (if port is open)
- RST Packet
  - IPID=31338
The target will send **RST to the “zombie”** if the port is closed but zombie will not send anything back.
IDLE Scan: Step 3

Probe “zombie” IPID again

Attacker

IPID Probe SYN / ACK Packet

Response: IPID=31339
RST Packet

Zombie

IPID incremented by 2 since Step 1, so port 80 must be open
ICMP Echo Scanning

- This is not really port scanning, since ICMP does not have a port abstraction
- But it is sometimes useful to determine which hosts in a network are up by pinging them all
- `nmap -P cert.org/24 152.148.0.0/16`

List Scan

- This type of scan simply generates and prints a list of IPs/Names without actually pinging or port scanning them
- A DNS name resolution will also be carried out
SYN/FIN Scanning Using IP Fragments

- It is not a new scanning method but a modification of the earlier methods.
- The TCP header is split up into several packets so that the packet filters are not able to detect what the packets intend to do.

```
C:\>nmap -sS -T4 -A -f -v 192.168.168.26
Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-29 13:05 India Standard Time
Initiating SYN Stealth Scan at 13:05
Scanning 192.168.168.26 [1000 ports]
Discovered open port 139/tcp on 192.168.168.26
Discovered open port 135/tcp on 192.168.168.26
Completed SYN Stealth Scan at 13:05, 1.16s elapsed (1000 total ports)
```
**UDP Scanning**

**Attacker**

Are you **open** on UDP Port 29?

No response if port is **Open**

If Port is Closed, an **ICMP Port unreachable** message is received

**Server**

---

**UDP Port Open**

- There is no **three-way TCP handshake** for UDP scan
- The system does not respond with a message when the port is **open**

---

**UDP Port Closed**

- If a UDP packet is sent to open port, the system responds with **ICMP port unreachable message**
- Spywares, Trojan horses, and other malicious applications use **UDP ports**
Attackers send TCP probe packets with various TCP flags (FIN, URG, PSH) set or with no flags. No response means the port is open and RST/ACK means the port is closed.
Attackers send an **ACK probe packet** with random sequence number, no response means port is filtered (stateful firewall is present) and **RST response means the port is not filtered**

```
nmap -sA -P0 10.10.0.25
Starting nmap 5.21 ([http://nmap.org](http://nmap.org)) at 2010-05-16 12:15 EST
All 529 scanned ports on 10.10.0.25 are: **filtered**
```
Scanning: **IDS Evasion Techniques**

1. Use fragmented IP packets

2. Spoof your IP address when launching attacks and sniff responses from server

3. Use source routing (if possible)

4. Connect to proxy servers or compromised trojaned machines to launch attacks
**IP Fragmentation Tools**

**Fragtest**
Determines exactly which types of the fragmented ICMP messages are processed and responded to by the remote host.

- **Syntax:** `fragtest TESTS ... host`

**fragroute**
Utility intercepts, modifies, and rewrites egress traffic destined for a specific host, according to a predefined rule set.

- **Syntax:** `fragroute [-f file] host`

For more information, visit:
- [http://linux.die.net](http://linux.die.net)
- [http://monkey.org](http://monkey.org)

---

**Fragmenting Probe Packets**
Nmap is a free open source utility for network exploration.

Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Attacker can use Nmap to extract information such as:

- Live hosts on the network
- Services (application name and version)
- Operating systems (and OS versions)
- Type of packet filters/firewalls
Scanning Tools

- Global Network Inventory Scanner
  [Website](http://www.magnetosoft.com)

- AWSPS: UDP Scanner
  [Website](http://www.atelierweb.com)

- Net Tools Suite Pack
  [Website](http://users.telenet.be)

- AWPTA
  [Website](http://www.atelierweb.com)

- Advanced Port Scanner
  [Website](http://www.radmin.com)

- MegaPing
  [Website](http://www.magnetosoft.com)

- Netifera
  [Website](http://netifera.com)

- Network Inventory Explorer
  [Website](http://www.10-strike.com)
Scanning Tools

Free Port Scanner
http://www.nsauditor.com

Infiltrator network security scanner
http://www.infiltration-systems.com

SuperScan
http://www.foundstone.com

Nscan
http://www.nscan.org

Komodia's PacketCrafter
http://www.komodia.com

xCAT Portscan
http://www.xcat-industries.nl

IP Tools
http://www.ks-soft.net

PhatScan
http://phatlinks.com
### Do Not Scan These IP Addresses

(Unless you want to get into trouble)

<table>
<thead>
<tr>
<th>RANGE 128</th>
<th>RANGE 130</th>
<th>RANGE 132</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.37.0.0 Army Yuma Proving Ground</td>
<td>129.53.0.0 - 129.53.255.255 66SPTG-SCB</td>
<td>132.3.0.0 Williams Air Force Base</td>
</tr>
<tr>
<td>128.38.0.0 Naval Surface Warfare Center</td>
<td>129.54.0.0 Vandenberg Air Force Base, CA</td>
<td>132.5.0.0 - 132.5.255.255 49th Fighter Wing</td>
</tr>
<tr>
<td>128.43.0.0 Defence Research Establishment-Ottawa</td>
<td>129.92.0.0 Air Force Institute of Technology</td>
<td>132.6.0.0 Ankara Air Station</td>
</tr>
<tr>
<td>128.47.0.0 Army Communications Electronics Command</td>
<td>129.99.0.0 NASA Ames Research Center</td>
<td>132.7.0.0 - 132.7.255.255 SSG/SIAC</td>
</tr>
<tr>
<td>128.49.0.0 Naval Ocean Systems Center</td>
<td>129.131.0.0 Naval Weapons Center</td>
<td>132.9.0.0 28th Bomb Wing</td>
</tr>
<tr>
<td>128.50.0.0 Department of Defense</td>
<td>129.163.0.0 NASA Johnson Space Center</td>
<td>132.10.0.0 319 Comm Sq</td>
</tr>
<tr>
<td>128.51.0.0 Department of Defense</td>
<td>129.164.0.0 NASA IVV</td>
<td>132.11.0.0 Hellenikon Air Base</td>
</tr>
<tr>
<td>128.56.0.0 U.S. Naval Academy</td>
<td>129.165.0.0 NASA Goddard Space Flight Center</td>
<td>132.12.0.0 Myrtle Beach Air Force Base</td>
</tr>
<tr>
<td>128.60.0.0 Naval Research Laboratory</td>
<td>129.167.0.0 NASA Marshall Space Flight Center</td>
<td>132.13.0.0 Bentwaters Royal Air Force</td>
</tr>
<tr>
<td>128.63.0.0 Army Ballistics Research Laboratory</td>
<td>129.168.0.0 NASA Lewis Research Center</td>
<td>132.14.0.0 Air Force Concentration</td>
</tr>
<tr>
<td>128.80.0.0 Army Communications Electronics Command</td>
<td>129.190.0.0 Naval Underwater Systems Center</td>
<td>132.15.0.0 Kadena Air Base</td>
</tr>
<tr>
<td>128.102.0.0 NASA Ames Research Center</td>
<td>129.198.0.0 Air Force Flight Test Center</td>
<td>132.16.0.0 Kunsan Air Base</td>
</tr>
<tr>
<td>128.149.0.0 NASA Headquarters</td>
<td>129.209.0.0 Army Ballistics Research Laboratory</td>
<td>132.17.0.0 Lindsey Air Station</td>
</tr>
<tr>
<td>128.154.0.0 NASA Wallops Flight Facility</td>
<td>129.229.0.0 U.S. Army Corps of Engineers</td>
<td>132.18.0.0 McGuire Air Force Base</td>
</tr>
<tr>
<td>128.155.0.0 NASA Langley Research Center</td>
<td>129.251.0.0 United States Air Force Academy</td>
<td>132.19.0.0 100CS (NET-MILDENHAM)</td>
</tr>
<tr>
<td>128.156.0.0 NASA Lewis Network Control Center</td>
<td>RANGE 130</td>
<td>132.20.0.0 35th Communications Sq</td>
</tr>
<tr>
<td>128.157.0.0 NASA Johnson Space Center</td>
<td>130.40.0.0 NASA Johnson Space Center</td>
<td>132.21.0.0 Plattsburgh Air Force Base</td>
</tr>
<tr>
<td>128.158.0.0 NASA Ames Research Center</td>
<td>130.90.0.0 Mather Air Force Base</td>
<td>132.22.0.0 23Communications Sq</td>
</tr>
<tr>
<td>128.159.0.0 NASA Ames Research Center</td>
<td>130.109.0.0 Naval Coastal Systems Center</td>
<td>132.24.0.0 Dover Air Force Base</td>
</tr>
<tr>
<td>128.160.0.0 Naval Research Laboratory</td>
<td>130.124.0.0 Honeywell Defense Systems Group</td>
<td>132.25.0.0 786 CS/SCBM</td>
</tr>
<tr>
<td>128.161.0.0 NASA Ames Research Center</td>
<td>130.165.0.0 U.S.Army Corps of Engineers</td>
<td>132.27.0.0 - 132.27.255.255 39CS/SCSM</td>
</tr>
<tr>
<td>128.183.0.0 NASA Goddard Space Flight Center</td>
<td>130.167.0.0 NASA Headquarters</td>
<td>132.28.0.0 14TH COMMUNICATION</td>
</tr>
<tr>
<td>128.202.0.0 50th Space Wing</td>
<td>RANGE 131</td>
<td>132.30.0.0 Lajes Air Force Base</td>
</tr>
<tr>
<td>128.216.0.0 MacDill Air Force Base</td>
<td>131.6.0.0 Langley Air Force Base</td>
<td>132.31.0.0 Loring Air Force Base</td>
</tr>
<tr>
<td>128.217.0.0 NASA Kennedy Space Center</td>
<td>131.10.0.0 Barksdale Air Force Base</td>
<td>132.33.0.0 60CS/SCSNM</td>
</tr>
<tr>
<td>128.236.0.0 U.S. Air Force Academy</td>
<td>131.17.0.0 Sheppard Air Force Base</td>
<td>132.34.0.0 Cannon Air Force Base</td>
</tr>
<tr>
<td>RANGE 129</td>
<td>131.21.0.0 Hahn Air Base</td>
<td>132.35.0.0 Altus Air Force Base</td>
</tr>
<tr>
<td>129.23.0.0 Strategic Defense Initiative Organization</td>
<td>131.32.0.0 37 Communications Squadron</td>
<td>132.37.0.0 75 ABW</td>
</tr>
<tr>
<td>129.29.0.0 United States Military Academy</td>
<td>131.35.0.0 Fairchild Air Force Base</td>
<td>132.38.0.0 Goodfellow AFB</td>
</tr>
<tr>
<td>129.50.0.0 NASA Marshall Space Flight Center</td>
<td>131.36.0.0 Yokota Air Base</td>
<td>132.39.0.0 K.I. Sawyer Air Force Base</td>
</tr>
</tbody>
</table>
| 129.51.0.0 Patrick Air Force Base                   | 131.37.0.0 Elmendorf Air Force Base                        | For a complete list, see the file: IP ADDRESSES YOU SHOULD NOT SCAN
Scanning Countermeasures

Configure firewall and IDS rules to detect and block probes

Block unwanted ports at the firewall

Use custom rule set to lock down the network

Hide sensitive information from public view
Scanning Countermeasures

Filter inbound ICMP message types and all outbound ICMP type 3 unreachable messages at **border routers and firewalls**.

If a commercial firewall is in use, ensure that:

1. **The latest service pack** is installed
2. The **Antispoofing rules** have been correctly defined
3. Fastmode services are not used in **Check Point Firewall-1** environments

Ensure that routing and filtering mechanisms cannot be bypassed using **specific source ports** or source-routing techniques.

Understand the network configuration and its accessible ports by launching **TCP and UDP port scans** along with ICMP probes against your own IP address space.
War Dialing

1. War dialing involves the use of a program in conjunction with a modem to penetrate the modem-based systems.

2. Companies do not control the dial-in ports as strictly as the firewall and machines with attached modems.

3. A tool that identifies the phone numbers that can successfully make a connection with a computer modem.

4. It generally works by using a predetermined list of common user names and passwords in an attempt to gain access to the system.
It does not matter how strongly you have locked the front door to your network if you have left the back door wide open.

- Do your modems reveal banners with their identity?
- Is there unknown open access to a legacy system?
- Do your modems still have default manufacturer passwords?
- Are your authorized modems susceptible to a break-in with a wardialer?
- Are you at risk by not conducting regular audits across your organization?
- Has someone inside your organization attached a modem to your network?
War Dialing Tools

- THC Scan
  http://freeworld.thc.org

- PAW / PAWS
  http://www.wyae.de

- iWar
  https://www.softwink.com

- ShokDial
  http://www.w00w00.org

- TeleSweep Secure®
  http://www.securelogix.com

- ToneLoc
  http://www.oldschoolphreak.com

- Plax Network Suite
  http://www.bestsecuritytips.com

- Visual NetTools
  http://www.airgrab.com
War Dialing Countermeasures

- Develop and implement security policies
- Conduct a manual reconnaissance of your network
- Use phone numbers in a range completely different from your internal PBX numbers
- Document floor plans and all your equipment
- Check your auto answer configurations on your modem
- Log all successful and failed login attempts
War Dialing Countermeasures: SandTrap Tool

Sandtrap can **detect war dialing attempts** and notify the administrator immediately being called, connected, via HTTP POST to a web server.
CEH Scanning Methodology

Check for Live Systems → Check for Open Ports → Banner Grabbing

Prepare Proxies ← Draw Network Diagrams ← Scan for Vulnerability
OS fingerprinting is the method to determine the operating system running on a remote target system. There are two types of OS fingerprinting: Active and Passive.

**Active**
- Specially crafted packets are sent to remote OS and the response is noted.
- The responses are then compared with a database to determine the OS.
- Response from different OS's varies due to differences in TCP/IP stack implementation.

**Passive**
- Passive banner grabbing uses sniffing techniques to capture packets flowing from system.
- Captured packets are then analyzed for OS information.
- It is also based on the differential implementation of the stack and the various ways an OS responds to it.
Active Banner Grabbing Using Telnet

This technique probes **HTTP servers** to determine the **Server field** in the HTTP response header.
Banner Grabbing Tool: ID Serve

- ID Serve is used to identify the make, model, and version of any web site's server software.
- It is also used to identify non-HTTP (non-web) Internet servers such as FTP, SMTP, POP, NEWS, etc.

![ID Serve Software Interface](image)

- ID Serve is a tool used for identifying the specifics of a web server's software.
- It can identify both HTTP and non-HTTP servers, including FTP, SMTP, POP, and NEWS.

Example usage:
1. Enter or paste an Internet server URL or IP address (e.g., www.juggyboy.com).
2. Query the server.
3. Server query processing results.
4. The server identified itself as AppleIDiskServer.1G3010.

Source: http://www.grc.com

---

Certified Ethical Hacker

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ATHENA
TRUNG TÂM BÀO TÀO AN NINH MẠNG & QUẢN TRỊ MẠNG
WWW.ATHENA.EDU.VN
GET REQUESTS

You might want to try these additional get requests for banner grabbing:

- GET
- GET /
- GET / HTTP/999.99
- GET / HTTP/1.0
- GET / HTTP/1.0
- GET / HTTP/999.99
- GET / http/999.99
- GET / http/999.99
- GET / HTTP/Q.9
- GET / HTTP/5.0
- GET / HTTP/5.0
- GET / HTTP/1.1
- GET / HTTP/1.1.0
- GET / HTTP/1.2
- GET / HTTP/2.1
- GET / HTTP/1.0
- GET / HTTP/1.0X
- GET / HTTP/
- GET/HTTP/1.0
- GET / HTTP/1.0
- GET / HTTP/1.0
- GET / HTTP/1.0
- GET / HTTP/1.0
- GET / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0
- HEAD / HTTP/1.0

Take a look at: GET REQUESTS

KNOWN_TESTS.htm file
Netcraft reports a site's operating system, web server, and netblock owner together with, if available, a **graphical view of the time** since last reboot for each of the computers serving the site.

**Results for microsoft.com**

<table>
<thead>
<tr>
<th>Site</th>
<th>Site Report</th>
<th>First seen</th>
<th>Netblock</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.microsoft.com">www.microsoft.com</a></td>
<td>August 1995</td>
<td>Microsoft Corp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>support.microsoft.com</td>
<td>October 1997</td>
<td>Microsoft Corp</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>technet.microsoft.com</td>
<td>August 1999</td>
<td>Microsoft Corp</td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td>msn.microsoft.com</td>
<td>September 1998</td>
<td>Microsoft Corp</td>
<td>Windows Server 8</td>
<td></td>
</tr>
<tr>
<td>office.microsoft.com</td>
<td>November 1998</td>
<td>Microsoft Corp</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>update.microsoft.com</td>
<td>February 2005</td>
<td>Microsoft Corp</td>
<td>Windows Server 2008</td>
<td></td>
</tr>
<tr>
<td>go.microsoft.com</td>
<td>November 2001</td>
<td>Microsoft Corp</td>
<td>Windows Server 2003</td>
<td></td>
</tr>
<tr>
<td>windows.microsoft.com</td>
<td>June 1998</td>
<td>Microsoft Corp</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>social.technet.microsoft.com</td>
<td>August 2008</td>
<td>Microsoft Corp</td>
<td>Windows Server 2008</td>
<td></td>
</tr>
</tbody>
</table>

http://www.netcraft.com
Banner Grabbing Countermeasures: Disabling or Changing Banner

IIS users can use these tools to disable or change banner information:

- IIS Lockdown Tool
  - http://microsoft.com

ServerMask
- http://www.port80software.com

Apache 2.x with `mod_headers` module - use a directive in `httpd.conf` file to change banner information
- Header set Server "New Server Name"

Apache 1.3.x users have to edit definitions in `httpd.h` and recompile Apache to get the same result

Alternatively, change the `ServerSignature` line to `ServerSignature off` in `httpd.conf` file
Hiding File Extensions

- Hiding file extensions is a good practice to mask the technology generating dynamic pages
- Apache users can use `mod_negotiation` directives
- IIS users use tools such as PageXchanger to manage the file extensions
Hiding File Extensions from Webpages

File extensions provide information about the underlying server technology, attackers can use this information to search vulnerabilities and launch attacks.

Change application mappings such as .asp with .htm or .foo, etc. to disguise the identity of the servers.

IIS users use tools such as PageXchanger to manage the file extensions.

Apache users can use mod_negotiation directives.

Doing without file extensions altogether is an even better idea.
CEH Scanning Methodology

1. Check for Live Systems
2. Check for Open Ports
3. Banner Grabbing
4. Prepare Proxies
5. Draw Network Diagrams
6. Scan for Vulnerability
Vulnerability scanning identifies **vulnerabilities and weaknesses of a system** and network in order to determine how a system can be exploited.
Nessus: Screenshot

http://www nessus.org

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Vulnerability Scanning Tool: SAINT

SAINT is also known as Security Administrator's Integrated Network Tool

Attackers can detect the network vulnerabilities on any remote target in a non-intrusive manner

It gathers information regarding what type of OS is running and which ports are open

4 Steps to a SAINT™ Scan
1. FIND TARGETS
2. PORT SCAN
3. HTTP VULN. CHECK
4. REPORT

- EXECUTIVE SUMMARY
- DETAILED TECHNICAL REPORTS
- RECOMMENDED FIXES
- TREND ANALYSIS

http://www.saintcorporation.com
Network Vulnerability Scanners

- Retina
  http://www.eeye.com

- Core Impact
  http://www.coresecurity.com

- MBSA
  http://technet.microsoft.com

- Shadow Security Scanner
  http://www.safety-lab.com

- Nsauditor
  http://www.nsauditor.com

- Network Security Inspector
  http://www.sunbeltsoftware.com

- OpenVAS
  http://www.openvas.org

- Security Manager Plus
  http://www.manageengine.com
CEH Scanning Methodology

Check for Live Systems → Check for Open Ports → Banner Grabbing

Prepare Proxies → Draw Network Diagrams → Scan for Vulnerability
LANsurveyor

VisioLANsurveyor automatically discovers your network and produces comprehensive and easy-to-view network maps that can be exported into Microsoft Office.

- Automatically discovers and diagrams network topology
- Generates network maps in Microsoft Office® Visio®
- Detects new devices and modifications in network topology
- Performs inventory management for hardware and software assets
- Directly addresses PCI compliance and other regulatory requirements

Attackers use mapping tools for drawing network diagrams of vulnerable host to launch attack.
LANsurveyor: Screenshot

http://www.solarwinds.com
Network Mappers

LANState
http://www.10-strike.com

CartoReso
http://cartoreso.campus.ecp.fr

Insightix Visibility
http://www.insightix.com

Lan-Secure Switch Center
http://www.lan-secure.com

FriendlyPinger
http://www.kilievich.com

HP OpenView Network Node Manager
https://h10078.www1.hp.com

Ipsonar
http://www.lumeta.com

NetMapper
http://www.opnet.com
CEH Scanning Methodology

- Check for Live Systems
- Check for Open Ports
- Banner Grabbing
- Prepare Proxies
- Draw Network Diagrams
- Scan for Vulnerability
Proxy Servers

- Proxy is a network computer that can serve as an intermediary for connecting with other computers.

As a firewall, a proxy protects the local network from outside access.

Proxy servers can afford some protection against hacking attacks.

As an IP addresses multiplexer, a proxy allows the connection of a number of computers to the Internet when having only one IP address.

Specialized proxy servers can filter out the unwanted content, such as ads or 'unsuitable' material.

Proxy servers can be used (to some extent) to anonymize web surfing.
Why Attackers Use **Proxy Servers**?

1. To hide the *source IP address* so that an attacker can hack without any legal corollary.
2. Attacker appears in a victim server's log files with a *fake source address of the proxy* rather than with the attacker's actual address.
3. To *remotely access intranets* and other *website resources* that are normally off limits.
4. To *interrupt all the requests* sent by an attacker and transmit them to a third destination, hence victims will only be able to identify the proxy server address.
5. To *use multiple proxy servers* for scanning and attacking, making it difficult for administrators to trace the real source of attack.
Use of Proxies for Attack

Direct attack/ No proxies

Logged Proxy

Attacker

Target

Attacker

Target

Attacker

Target

Attacker

Target
How Does MultiProxy Work?

List of Proxy Servers

- 164.58.28.250:80
- 194.muja.pitt.washtcct.dsl.att.net:80
- web.khi.is:80
- customer-148-223-48-114.uninet.net.mx:80
- 163.24.133.117:80
- paubrasil.mat.unb.br:8080
- 164.58.10.25:80
- bpup014.hgo.se:3128
- bpup007.hgo.se:3128
- www.reprokopia.se:8000
- 193.188.95.146:8080
- 193.220.22.246:80
- gennet.gennet.ee:80
- pandora.teimes.gr:8080
- mail.thaweb.co.uk:8000
- mail.thenew.co.uk:8888
- 194.6.1.219:80
- 194.79.113.83:8080
- ntbkp.nattec.co.il:8080
- 195.103.8.10:8080
- pools1-31.adsl.nordnet.fr:80
- pools1-98.adsl.nordnet.fr:80
- 195.167.64.193:80
- server.astragats.com:8080
- los.micr.com.pl:80
- 195.47.14.193:80
- mail.voltage.co.za:8080
- 196.23.147.34:80
- 196.40.43.34:80
- lvosweb.levgeasteock.com:8000

MultiProxy running at 127.0.0.1:8088

Target

Internet
Free Proxy Servers

A search in Google lists thousands of free proxy servers
Proxy Workbench

- Proxy workbench is a proxy server that resides inside the network and monitors the connection, supports proxy chaining.

How to run:
- Install proxy workbench
- Configure the client to use this proxy IP to connect to port 8080

User → Proxy Server → Internet

http://www.tcpiq.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Proxifier Tool: Create Chain of Proxy Servers

Proxifier is a program that allows network applications that do not support working through proxy servers to operate through an HTTPS or SOCKS proxy or a chain of proxy servers.

http://www.proxifier.com
SocksChain transmits the TCP/IP applications through a chain of proxy servers.
TOR (The Onion Routing)

**Anonymity**
Provides anonymous communication over Internet

**Privacy**
Ensures the privacy of both sender and recipient of a message

**Security**
Provides multiple layers of security to a message

**Tor Proxy**
The initiating onion router, called a "Tor client" determines the path of transmission

**Proxy Chain**
Uses cooperating proxy routers throughout the network

**Encryption**
Encrypts and decrypts all data packets using public key encryption
TOR Proxy
Chaining Software
HTTP Tunneling Techniques

HTTP Tunneling technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls.

This is made possible by sending data through HTTP (port 80).

End Users use HTTP-Tunnel to transmit or receive data through Firewall.

Previously inaccessible servers and services.

Racks of HTTP Tunnel Servers receive and relay the data.
Why do I Need HTTP Tunneling?

- If the organization has blocked all the ports in your firewall and only allows port 80/443 and you want to use FTP to connect to some remote server on the Internet.
- In this case, you can send your packets via http protocol.

_Inside the network:_
- FTP Client Software
- HTTP Tunneling client running on local port
- FTP data is encapsulated in http packet

_Outside the network:_
- Remote server running FTP
- FTP data is unwrapped
- Firewall rules only allow port 80 and 443
- Http tunneling server software running

TCP Ports:
- Port 23
- Port 21
- Port 79
- Port 25
- Port 110
- Port 500
- Port 69
- Port 80
- Port 443
Super Network Tunnel Tool

It is a **two-way http tunnel** software connecting two computers. It works like **VPN tunneling** but uses http protocol to establish a connection.

http://www.networktunnel.net
Http tunnel for Windows

- Http tunnel creates a bidirectional virtual data connection tunneled in HTTP requests. The HTTP requests can be sent via an HTTP proxy if so desired.
- This can be useful for users behind the restrictive firewalls.
- If WWW access is allowed through an HTTP proxy, it is possible to use http tunnel and, say, telnet or PPP to connect to a computer outside the firewall.

On the server, you must run hts. If you want to redirect all port 80 (http) traffic to port 23 (telnet), it would go something like:

```bash
hts -F server.test.com:23 80
```

On the client you would run htc. If you are going through a proxy, the -P option is needed otherwise omit it.

```bash
htc -P proxy.corp.com:80 -F 22 server.test.com:80
```

Then telnet localhost and it will redirect the traffic out to port 80 on the proxy server and on to port 80 of the server, then to port 23.
Additional HTTP Tunneling Tools

HTTP-Tunnel

HTTPPort

http://www.http-tunnel.com

website unavailable
SSH Tunneling

Using OpenSSH you can tunnel all of the traffic from your local box to a remote box that you have an account on.

```
ssh -f user@juggyboy.com -L 2000:juggyboy.com:25 -N
```

- `-f` = background mode
- `user@juggyboy.com` = user name and server you are logging into
- `-N` = Do not execute the command on the remote system

This essentially forwards the local port 2000 to port 25 on juggyboy.com encrypted. Simply point your E-mail client to use localhost:2000 as the SMTP server.
SSL Proxy Tool

SSLproxy is a transparent proxy that can translate between encrypted and unencrypted data transport on socket connections.

It also has a non-transparent mode for automatic encryption-detection on netbios.

http://www.obdev.at

When should I use SSLProxy?

To launch exploits using SSL product
To evade IDS systems
To cover the attack path

Attacker

Target

Establish SSL tunnel to send exploits
Internet

Exploits → SSLProxy → IDS → SSL Protocol
How to Run SSL Proxy?

**Window 1: Client – Hacker Machine Run:**

```bash
sslproxy -L 127.0.0.1 -155 -R <some remote IP> -r 443 -c dummycert.pem -p ssl2
```

**Window 2: Client - Connect to 12.0.0.1 port 55 and send your exploits**

- Example: `telnet 127.0.0.1 55`
- Then type `GET /`
Proxy Tools

- Proxy Commander
  http://www.dlao.com

- GProxy
  http://gpass1.com

- Protoport Proxy Chain
  http://www.protoport.com

- Proxy+
  http://www.proxyplus.cz

- FastProxySwitch
  http://affinity-tools.com

- ProxyFinder
  http://www.proxy-tool.com

- ProxyFinder Enterprise
  http://www.proxy-tool.com

- Proxy-Pro Professional GateKeeper
  http://www.sysgenic.com
Proxy Tools

- ezProxy
  http://psw.oclc.org

- SurfStream
  http://software-files-lcnet.com

- Proxy Switcher
  http://www.proxyswitcher.com

- JAP Anonymity and Privacy
  http://anon.inf.tu-dresden.de

- ProxyBag
  http://www.alcenia.com

- CC Proxy Server
  http://www.yzsoft.net

- Proxyswitcher Lite
  http://www.proxyswitcher.com

- Free Proxy
  http://www.sysgenic.com
Anonymizers

- An anonymizer removes all the identifying information from the user’s computers while the user surfs the Internet.
- Anonymizers make activity on the Internet untraceable.
- Anonymizer tools allow you to bypass Internet censored websites.

Why use Anonymizer?

- Privacy and anonymity
- Bypass IDS and Firewall rules
- Protects from online attacks
- Accesses Government restricted content
Types of Anonymizers

Networked Anonymizers

They transfer communications through a network of Internet computers between you and the destination.

**Advantage:** Complication of the communications makes traffic analysis complex.

**Disadvantage:** Any multi-node network communications have some degree of risk at each node for compromise of confidentiality.

Single-point Anonymizers

They pass your surfing through a single web site to protect your identity.

**Advantage:** User’s IP address and related identifying information are protected by the arms-length communications.

**Disadvantage:** It offers less resistance to the sophisticated traffic analysis.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
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.

"If it bothers you that the China government does it, it should bother you when your cable company does it."
Manual Conversion

- Manual text conversion is a type of classical steganography, where text in natural language is jumbled according to a predefined pattern known to both sender and receiver.
- It can be used to bypass keyword based Internet filtering but is not effective against URL or DNS filtering techniques.

This tool can convert an ordinary Chinese classical text from horizontal to vertical patterns to avoid firewall rules.

**Tool:** Vertical Text Converter
(http://www.cshbl.com)
Psiphon is a censorship circumvention system that allows users to bypass firewalls and access blocked sites in countries where the Internet is censored.

It uses a secure, encrypted HTTP tunnel connection to receive requests from psiphonite to psiphonode who in turn then transports the results back to the requested psiphonite.

It acts as a web proxy for authenticated psiphonites, the first service that even works on mobile browsers.

It bypass the content-filtering systems of countries like China, North Korea, Iran, Saudi Arabia, Egypt and others.
How Psiphon Works?

Internet Uncensored Countries

Psiphon Tool

Using HTTPS

Internet Censored Countries

Psiphon user in China

Blocked

Google

YouTube

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Psiphon: Screenshot

http://psiphon.ca
How to Check if Your Website is Blocked in China or Not?

"How do I find out if web users in China can access my website at xyz.com?"

If you get a "Packets lost" error or there is a time-out while connecting to your site, chances are that the site is restricted.

Just Ping
(http://www.just-ping.com)

Watch Mouse
(http://www.watchmouse.com)
Google sets a cookie on users’ system with a **unique identifier** that enables them to track users’ web activities such as:
1. Search Keywords and habits
2. Search results
3. Websites visited

Google cookies expire in two years

Information from Google cookies can be used as **evidence** in a court of law

This is what Google's log might look like when you search for "PORSCHE"


**http://www.google.com/search?q=PORSCHE** - MSIE 8.0; Windows NT 7.0 -
Spoofing IP Address

IP spoofing refers to the procedure of an attacker changing his or her IP address so that he or she appears to be someone else.

When the victim replies to the address, it goes back to the spoofed address and not to the attacker’s real address.

IP spoofing using Hping2:

Hping2 www.juggyboy.com -a 7.7.7.7

You will not be able to complete the three-way handshake and open a successful TCP connection by spoofing an IP address.
IP Spoofing Detection Techniques: Direct TTL Probes

- Sending a packet to the claimed host will result in a reply, if the TTL in the reply is not the same as the packet being checked, it is a spoofed packet.

- This technique is successful when attacker is in a different subnet.
IP Spoofing Detection Techniques: IP Identification Number

- Sending a probe packet to the claimed host will result in a reply, if the IP ID number in the reply is not in the near value as the packet being checked, it is a spoofed packet.
- This technique is successful even if the attacker is in the same subnet.

Attacker (Spoofed Address 10.0.0.5)

Sending a packet with spoofed 10.0.0.5 IP – IP ID 2586

Target

Sending a packet to 10.0.0.5 IP

Reply from real 10.0.0.5 IP – IP ID 515
IP Spoofing Detection Techniques: TCP Flow Control Method

- If attacker is sending spoofed packets, he will not receive the target’s ACK-packets and will not respond with SYN+ACK packet.
- If the attacker does not stop sending packets after the initial window size is exhausted, most probably the packets are spoofed.

Diagram:
- Attacker (Spoofed Address 10.0.0.5)
- Sending a SYN packet with spoofed 10.0.0.5 IP
- Sending ACK packet to real 10.0.0.5 IP
- Target
IP Spoofing Countermeasures

- **Encryption**
  Encrypt all network traffic

- **Limit Access**
  Limit access to configuration information on a machine

- **Egress Filtering**
  Use filters to prevent packets from leaving your network

- **Ingress Filtering**
  Use router filters to prevent packets from entering your network

- **Sequence Number**
  Use random initial sequence numbers
Scanning Penetration Testing

1. Check for Live Systems
2. Check for Open Ports
3. Banner Grabbing
4. Prepare Proxies
5. Draw Network Diagrams
6. Scan for Vulnerability
The objective of penetration testing a network for scanning attempts is to determine the network security posture by identifying live systems, discovering open ports, associated services and grabbing system banners from a remote location simulating a network hacking attempt.

The penetration testing report will help system administrators to:

- Close unused ports
- Calibrate firewall rules
- Disable unnecessary services
- Troubleshoot service configuration errors
- Hide or customize banners
Scanning Pen Testing

1. Perform Host discovery
   - Use tools such as Angry IP Scanner, Nmap, Netscan, etc.

2. Perform Port scanning
   - Use tools such as Nmap, Netscan Tools Pro, UDP Scanner, etc.

3. Perform Banner Grabbing/OS Fingerprinting
   - Use tools such as Telnet, Netcraft, Xprobe, Satori, etc.

- Check for the live hosts using tools such as Angry IP Scanner, SolarWinds Engineer’s toolset, Colasoft Ping, Utility Ping, Nmap, Netscan, etc.
- Check for open ports using tools such as Nmap, Netscan Tools Pro, Net Tools Suite Pack, UDP Scanner, etc.
- Perform banner grabbing/OS fingerprinting using tools such as Telnet, Netcraft, Xprobe, Satori, etc.
Scanning Pen Testing

Scan for vulnerability

- Use tools such as Nessus, SAINT, GFI LANGuard, Core Impact, etc.

Draw network diagrams

- Use tools such as LAN surveyor, Ipsonar, CartoReso, etc.

Prepare proxies

- Use tools such as Proxifier, SocksChain, SSL Proxy, Proxy+, etc.

Document all the findings

Scan for vulnerabilities using tools such as Nessus, SAINT, GFI LANGuard, Core Impact, Nsauditor, MBSA, etc.

Draw network diagrams of the vulnerability hosts using tools such as LAN surveyor, Ipsonar, CartoReso, NetMapper, etc.

Prepare proxies using tools such as Proxifier, SocksChain, SSL Proxy, Proxy+, Gproxy, ProxyFinder, etc.

Document all the findings
Module Summary

- Scanning is one of the three components of intelligence gathering for an attacker.
- The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network.
- FTP bounce scanning is a type of port scanning which makes use of the Bounce attack vulnerability in FTP servers.
- War dialing involves the use of a program in conjunction with a modem to penetrate the modem-based systems of an organization by continually dialing in.
- OS fingerprinting is the method to determine the operating system that is running on the target system.
- Proxy is a network computer that can serve as an intermediary for connecting with other computers.
- A chain of proxies can be created to evade the traceback of the attacker.
The only problem with Microsoft is that they have no taste. They have absolutely no taste. And what that means is, I don't mean it in a small way I mean't it in a big way.

- Steve Jobs,
  CEO, Apple Inc.