



**Ofir Arkin**

**ofir@sys-security.com**

**Founder, The Sys-Security Group**



**Sys-Security Group**

Because security isn't trivial.



# Agenda

- **Release information**
- **History**
- **Xprobe I**
- **Strict Signature Matching**
  - Problems
  - Needs
- **Our 'Fuzzy' approach with Operating System Fingerprinting**
- **Practical Implementation**
- **Demo 😊**
- **Questions**

# Ofir Arkin

- **Founder, The Sys-Security Group**
- **Computer Security Researcher**
  - ICMP
  - TCP/IP
  - Voice over IP (VoIP)
  - Information Warfare
- **Computer Security Architect**
- **Published numerous papers and articles**

# Xprobe & Xprobe2 Creators



# Release Information

- **Paper: “Xprobe2 – A “Fuzzy” Approach to Remote Active Operating System Fingerprinting”**
- **Tool: Beta version of Xprobe2 (*must* use libpcap 0.7.1)**
- **All available from:**
  - <http://www.xprobe.org> [FW]
  - <http://www.xprobe2.org> [FW]
  - <http://www.sys-security.com>

# History – Xprobe I

- Xprobe v0.0.1 was **released** at the **Blackhat briefings in August 2001**
- Xprobe is a **remote active operating system fingerprinting tool** based on **Ofir Arkin's "ICMP Usage in Scanning" research project**

(<http://www.sys-security.com>)

- The tool (Xprobe I) presents **an alternative to other remote active operating system fingerprinting tools** which are **heavily dependent on the usage of the TCP protocol** for remote active operating system fingerprinting

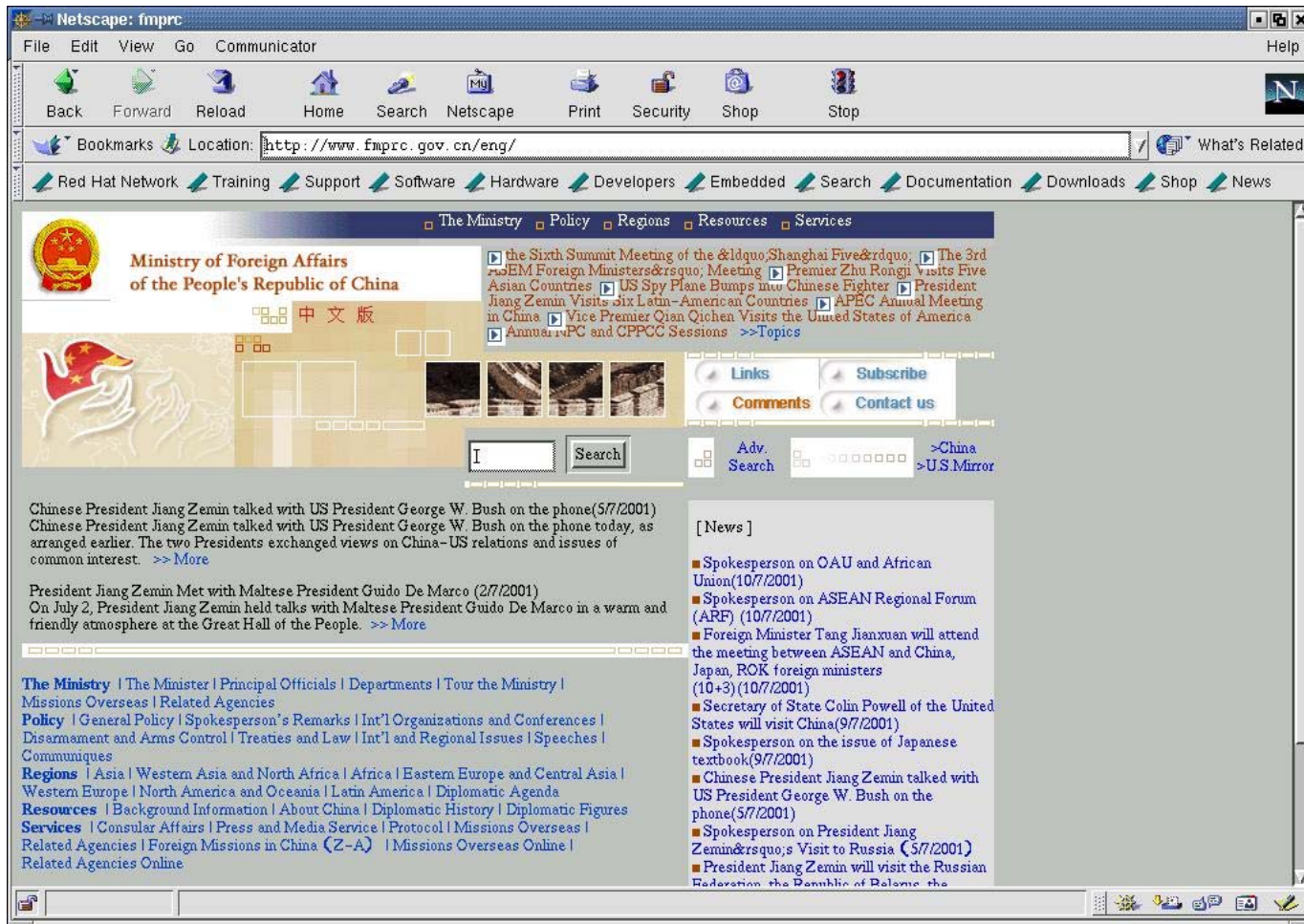
# History – Xprobe I

- The first versions of Xprobe combined various remote active operating system fingerprinting methods using the ICMP protocol, which were derived from the “ICMP Usage in Scanning” research project, into **a simple, fast, efficient and a powerful way** to detect a target host’s underlying operating system.
- Xprobe v1 **uses only ICMP related operating system fingerprinting tests**

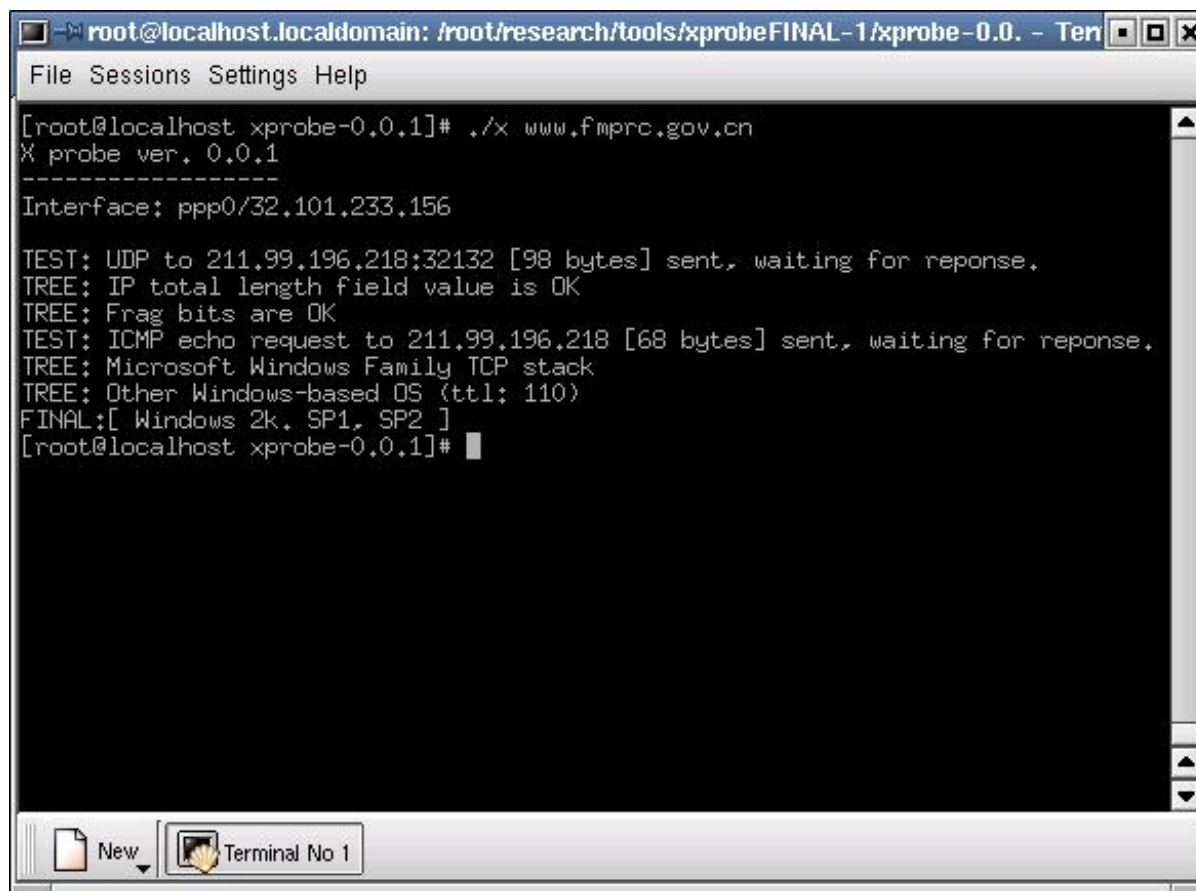
# History – Xprobe I

- The first versions of Xprobe **lacked the support of a signature database and relied on a static decision tree to produce the results.**
- The use of hard coded signatures within Xprobe instead of a database holding operating system fingerprinting signatures is **one of the main disadvantages of the tool**
- In spite of its disadvantages Xprobe I (current released version 0.0.2, non-released version 0.0.2p1) is a **fast, stealth and accurate** remote active operating system fingerprinting tool

# History – Xprobe I (an example from Defcon 9)



# History – Xprobe I (an example from Defcon 9)



```
root@localhost.localdomain: /root/research/tools/xprobeFINAL-1/xprobe-0.0. - Ten
File Sessions Settings Help

[root@localhost xprobe-0,0,1]# ./x www.fmprc.gov.cn
X probe ver. 0,0,1
-----
Interface: ppp0/32.101.233.156

TEST: UDP to 211.99.196.218:32132 [98 bytes] sent, waiting for reponse.
TREE: IP total length field value is OK
TREE: Frag bits are OK
TEST: ICMP echo request to 211.99.196.218 [68 bytes] sent, waiting for reponse.
TREE: Microsoft Windows Family TCP stack
TREE: Other Windows-based OS (ttl: 110)
FINAL:[ Windows 2k, SP1, SP2 ]
[root@localhost xprobe-0,0,1]#
```

10

# History – Xprobe I

- We were looking into integrating signature support to Xprobe.
- Since the usual strict signature matching approach, taken by other remote active operating system fingerprinting tools, **suffers from several design flaws and accuracy problems given the conditions the tools operate against**, we considered a different approach with signature matching

## Xprobe II

- I will be explaining how we aggregate different remote active operating system fingerprinting methods in order to identify the type of a remote operating system with a high precision rating utilizing a 'fuzzy' approach to remote active operating system fingerprinting.

# Strict Signature Matching

- The tools used today for remote active operating system fingerprinting (nmap, queso) **use a signature database to perform remote operating system recognition by utilizing strict signature matching and a fixed number of fingerprinting tests** to identify the type of a remote operating system.

# Strict Signature Matching – Problems

- **The strict signature matching technique**, by itself, is **not perfect**.
- It is **affected from a number of issues** reflected by the **topology of the targeted system/network** and the **nature of fingerprinting itself**, where we are merely ‘guessing’ the type of the remote operating system. Among these issues we can identify the following:

# Strict Signature Matching – Problems

- A packet might be **affected** in different ways **while in transit**. **Several field values within the packet might be changed by a networking device or even by a filtering device for different reasons. We can name several examples:**
  - A **packet shaping device** might change several field values within a packet (forcing TOS values, IP time-to-live values, discarding packets with malformed checksums, calculating checksums for zero-checksummed packets (UDP) etc).
  - A **router or a firewall might spoof responses for a targeted system they protect**. For example firewalls which spoof ICMP query replies for targeted systems they protect, or even performing the TCP 3-way handshake with an initiating system before handing the connection directly to a protected targeted system (some sort of a denial-of-service protection).
  - A **Scrubber** may be present between the sending system and the target system.

# Strict Signature Matching – Problems

- Potentially, these and other such problems, might affect the results produced by a remote active operating system fingerprinting tool **resulting with false and inaccurate results.**
- If a remote active operating system fingerprinting tool relies on certain IP packet field values, **which were changed or affected by the networking environment the packet traverses**, it is more than likely that the **strict signature matching process will fail** (or produce false results).

# Strict Signature Matching – Problems

- By introducing appropriate signature entries into our signature database **we can use this situation to our advantage**. The added entries within the signature database will match the modifications, and therefore we will be able to collect extra intelligence and knowledge about certain networking devices, filtering devices, or even networking topologies.
- Potentially we might be able to recognize a type of a packet filtering device (and sometimes its function, i.e. OpenBSD NAT, or Linux IP masquerade), a packet shaping device, etc.

# Strict Signature Matching – Problems

- In a real networking environment **systems should be firewalled**. If the traffic filtering is done correctly, then some inbound and outbound packets will be dropped by the firewall (i.e. not allowed in or out). **If a remote active operating system fingerprinting tool relies on the receipt of particular packet types and those packets were dropped by a firewall protecting the target system(s) chances are high that false results or no results at all will be produced.**
- If the packets sent by a remote active operating system fingerprinting tool **pass through a load balancing device along their way to the target machine some packets might be routed to a different machine rather than the destined target**. This might cause the signature matching process to fail.

# Strict Signature Matching – Problems

- **Some characteristics of a TCP/IP stack's behavior can be altered by a user:**
  - **Tunable parameters** of the TCP/IP stack might be changed e.g. the `sysctl` command on the various \*BSDs, the `ndd` command on Solaris, etc.
  - **Numerous patches exist** for some open source operating system's kernels that alter the way the particular operating system's TCP/IP stack responds to certain packets.[\[1\]](#)
- **If a remote active operating system fingerprinting tool is using some of the parameters which can be altered as part of its signature base, the signature match will most likely fail.**
- [\[1\]](#) One example is the IP Personality patch for Linux Kernel 2.4.x (<http://ippersonality.sourceforge.net/>)

# Strict Signature Matching – Problems

- If a remote active operating system fingerprinting tool **utilizes malformed packets to produce its results**, these malformed packets could be easily detected by a properly configured Network Intrusion Detection System (NIDS).
- **If one is ready to sacrifice the quality of the fingerprinting in order to avoid detection**, strict signature matching based remote active operating system fingerprinting tools may not allow you to do so if they rely on responses to malformed packets as part of an operating system signature.
- If a remote active operating system fingerprinting tool utilizes malformed packets to produce its results **these malformed packets might be dropped by a filtering device**, if the filtering device analyzes packets for non-legitimate contents. Therefore fingerprinting tests relying on these packets will fail and no results will be produced.

## Strict Signature Matching – Needs

- A certain **precision** of remote active operating system fingerprinting should be maintained **even if some particular tests fail or are rendered ineffective by the target network environment/topology.**
- The ability to **identify networking obstacles** such as filtering devices, load balancers, etc.
- The ability to **detect modifications made to the targeted machine's TCP/IP stack.**
- The ability to **detect Scrubber activity.**

# Strict Signature Matching – Needs

- If we are unable to identify the operating system type of the targeted machine, **we would like to limit the number of possible guesses/matches to a finite number.** **Having a list of possible matches would allow a knowledgeable auditor, in some cases, to either narrow down the list of possible matches or even take an educated guess at the correct operating system.**
- Often, **people discover new ways to fingerprint operating systems, or vendors alter their TCP/IP stacks making old-known fingerprints and/or fingerprinting methods fail against new operating systems or the altered TCP/IP stacks.** We wish to have a tool which will allow a user to easily **add or remove new modules of fingerprinting techniques**, based on any protocol, while maintaining and, still being able to use, the original modules and signature database. **This means we have to have an API for the tool.**

## Strict Signature Matching – Needs

- We wish to **maintain control on the ability to use (or not to use) malformed packets in our probes** and still be able to gather particular intelligence on a remote operating system's TCP/IP stack type.
- The ability to have **full control on each and every aspect of the fingerprinting tests** (i.e. number of repeated tests, number of packets sent, parameters used, etc.).

# Xprobe2

- Xprobe v2 brings about many of these features, and the solution to many of these needs. **We attempted to resolve most of these problems**, while sticking to our original goal of **creating one of the most advanced remote active operating system fingerprinting tool out there.**

# A Fuzzy Approach with Operating System Fingerprinting

- **Several approaches to ‘fuzzy’ matching can be used with a remote active operating system fingerprinting tool to match received results with a known fingerprints signature database:**
  - Fisher's Discriminate Function Analysis: this is a statistical solution which allows classifying a number of elements into groups based on ‘matching factors’. More details are available here: <http://www.statsoftinc.com/textbook/stdiscan.html> (this could be interesting to implement).
  - OCR recognition: several Optical Character Recognition methods have been implemented along the years. Most of them could be applicable to perform ‘fuzzy’ signature matching.
  - Matrix based fingerprints matching based on statistical calculation of scores for each test (one of the simplified forms of the OCR methods).
  - Other Mathematical algorithms

## A Fuzzy Approach with Operating System Fingerprinting

- The solution is based on a simple matrix representation of the scan (or scans), and the calculation of 'matches' by simply summing up scores for each 'signature' (OS).
- All tests are performed independently.
- The following is the abstract matrix we are using with Xprobe v2:

# A Fuzzy Approach with Operating System Fingerprinting

Upon initialization each fingerprinting test, which is implemented as an independent module, builds its own vector of possible 'test matches' for each OS (OS (OS(1), OS(2), ...OS(i))). This is done by reading the xprobe2.conf configuration file, which holds the fingerprints signature database, and looking for the "fingerprint" and "OS\_ID" entries

Once the fingerprinting test is executed the program examines the packet(s) received as a result of the fingerprinting test and places the appropriate 'score' (several values can be assigned) into the appropriate OS row.

initialization	OS	Operating System 1	Operating System 2	Operating System 3	...	Operating System $i$
→ Test 1	Test 1 (TTL)	score	score	score	...	score
	Test 2 (IP_ID)	score		score	...	score
	Test 3 (ICMP Port Unreachable)	score	score	score	...	score
	...				...	
	Test n	score	score	score		score
→ Sum of all tests	Totals	X	Y	Z	...	D

Once all tests are completed, we simply run through all the columns and calculate the summary for each OS. The top-score OS{x} (X, Y, Z, or D) will be declared as the final result.

# A Fuzzy Approach with Operating System Fingerprinting

- The `score` value can take one of the following values:
  - YES(3)
  - PROBABLY\_YES(2)
  - PROBABLY\_NO(1)
  - NO(0).
- Each test module assigns the appropriate `score` value according to the scheme implemented with the module. Having the score parameter able to be assigned different values introduces a certain degree of ‘fuzziness’ with Xprobe v2.
- This approach gives us probabilistic support since the highest score given for an OS (or OSs) is the most likely to produce an accurate match

# A Fuzzy Approach with Operating System Fingerprinting

- **The other ‘possible’ results could optionally be listed, as they may be useful to identify:**
  - A **slightly different TCP/IP stack** that produced similar test results for some of the fingerprinting tests used.
  - The **type of an intermediate device which alters some values within the packets sent and/or received** (e.g. if you use Linux’s IP masquerade abilities, it will overwrite certain settings within the IP headers of packets traversing through. This currently confuses the latest versions of nmap and xprobe).
  - The **type of the original operating system, even if the TCP/IP stack has been altered**. The alteration can be done by changing the default value of one, or more, tunable kernel parameters, by using a patch for the kernel, or by using a Scrubber. The TCP/IP stack alteration can also be aimed to ‘masquerade’ as some other operating system.
  - The ability to detect the original operating system holds true if some tests are not affected by the TCP/IP stack alternations and some are, taking into account that both signatures for the operating system without the alternation and for the operation system with the alternation should be present with the signature database.
  - A **filtering device spoofing responses for a system it is configured to defend**.

# A Fuzzy Approach with Operating System Fingerprinting

## ■ Pluggable Architecture

- A pluggable architecture was designed with Xprobe v2, where **different modules, representing new modules, improved modules, or your own way of TCP/IP stack fingerprinting tests might be introduced by any user using the program's API.**
- The core functionality of Xprobe v2 is designed in such a way that **each test is independent from each other** (the usage of the matrix), and when new modules are added, the functionality of the tool does not degrade. Instead, it just adds the appropriate test entry in the matrix.

# A Fuzzy Approach with Operating System Fingerprinting

- **Overcoming Failures of Certain Tests & Defeating Network Obstacles**
  - Having the ability to choose which fingerprinting tests and modules to use allows us to **overcome failures of certain tests**, since **they will not affect the “global picture”** (the final score for each operating system).
  - For example, one can choose to use NO(0) for failed tests, and PROBABLY\_NO(1), for platforms where responses are unknown.
  - **Even if a particular test fails all of the operating systems represented in the matrix will get the same score.**
  - This also suggests that **having more tests might produce a better overall result.**
  - The burden of deciding the weight each test has on an operating system lies on each individual module. This **gives module writers the freedom to assign score values according to their own take on remote active operating system fingerprinting.**

# A Fuzzy Approach with Operating System Fingerprinting

## ■ Control

- With Xprobe v2 a user has full control on which modules, probes and tests the tool will use when targeting a remote machine. This ability gives the experienced user more room to control the tool's exact behavior as well as flexibility no other remote active operating system fingerprinting tool provides today.
- The tool gives its users the ability to be **more accurate with matched results**, as with the appropriate usage of modules the discovery of “network obstacles” at the targeted network.

# A Fuzzy Approach with Operating System Fingerprinting

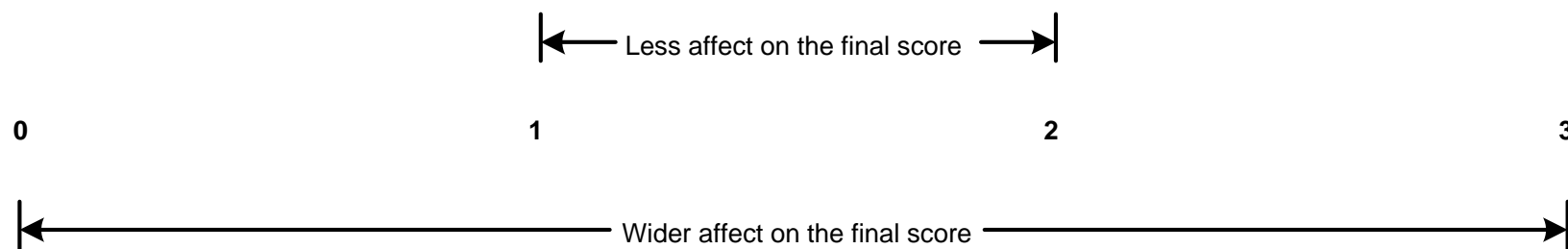
## ■ Dealing with Yes/No Tests

- The only issue that might affect the fingerprinting results, is a fingerprinting test which sends a packet and waits to see if the remote machine answers the probe or not. We define this type of fingerprinting test as “a Yes/No test”.
- With these type of tests, we have a problem to determine if **the remote machine did not produce an answer because it is not answering the particular probe as default, a tunable parameter was set to not answer the particular probe we are using, or because a filtering device is not allowing this type of probe (either inbound or outbound).**
- Using our fuzzy approach to remote active operating system fingerprinting we have the ability to control the affect of such a test on the overall result scheme.

# A Fuzzy Approach with Operating System Fingerprinting

- If we assess that a particular Yes/No test has a high probability of being blocked at the network perimeter, at the host level where the host might have been hardened, or not being answered by the majority of systems we can narrow the range of assigned values for this particular test.
- Instead of using the YES(3) or No(0) score values we will be assigning the score values of PROBABLY\_YES(2), for a successful attempt, and PROBABLY\_NO(1) for an unsuccessful attempt. With this being done we minimize the unreliable test results affect on the overall results, assuming other tests will be taken.

# A Fuzzy Approach with Operating System Fingerprinting



# A Fuzzy Approach with Operating System Fingerprinting

- Although currently we are using only four (4) different values for the score parameter, we are planning in the future to use a wider score parameter value range with more appropriate values for these type of conditions.
- As a rule of thumb we need to understand, and adjust, to the environment(s) we are operating in. Targeting machines over the Internet and auditing your own networks internally are two totally different scenarios.
- One also needs to have an intimate knowledge with different TCP/IP stacks in order to fully understand how those will respond when probed with different fingerprinting tests. This person will have the ability to take a full advantage of the modular architecture of Xprobe v2 and from its own test results when they are not conclusive.

# A Fuzzy Approach with Operating System Fingerprinting

- For example, some operating systems are lacking the appropriate tunable parameter for controlling some behavioral aspects of their TCP/IP stack. We can name Sun Solaris 2.3-2.9 and the lack of ability to configure the TCP/IP stack not to answer ICMP Echo requests and ICMP Address Mask requests. In this case, if, eventually, the remote machine is found to be a Sun Solaris machine but the Address Mask test failed, than there is a filtering device that disallowed this type of messages between us and the target.
- Or, HP Printers which are not identified by their module number (i.e. HP Laser Jet 4) but by their ROM and EEPROM version (I guess some one needs to fix his fingerprinting database now...)

# The Practical Implementation

- Xprobe v2 is **primarily implemented based on operating system fingerprinting tests developed for the original Xprobe tool.** These are remote active operating system fingerprinting tests based on the ICMP protocol which were discovered during Ofir Arkin's "ICMP Usage in Scanning" research project.
- However, **new tests have been added based on our own research or other remote operating system fingerprinting tools implementations.**
- Please refer to the original Xprobe article and design notes documentation [\[1\]](#) for more information on the original Xprobe remote operating system fingerprinting tests.
- [\[1\]](#) X – Remote ICMP based OS fingerprinting Techniques, Ofir Arkin & Fyodor Yarochkin August 2001. Available from: <http://www.sys-security.com>.

# The Practical Implementation

- A user is **not limited to using only the fingerprinting test modules available with the program; he may write his own modules** with his own remote operating system fingerprinting tests reflecting his own take on fingerprinting since **an API is provided with Xprobe v2.**
- Please refer to the Xprobe2 paper and documentation for more information on our API

## Sample Xprobe2 Run

- The sample run was produced utilizing a Linux kernel 2.4.18-based machine running Xprobe2 targeting a Microsoft Windows XP Professional machine on the same local LAN.
- The following is the sample run Xprobe2 have produced:

```
carman:~/tmp/xprobe2/src # ./xprobe2 -v 192.168.1.200
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
[+] Target is 192.168.1.200
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 192.168.1.200 is up (Guess probability: 100%)
[+] Target: 192.168.1.200 is alive
[+] Primary guess:
[+] Host 192.168.1.200 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2" (Guess
probability: 68%)
[+] Other guesses:
[+] Host 192.168.1.200 Running OS: "Microsoft Windows XP Professional" (Guess probability: 68%)
[+] Host 192.168.1.200 Running OS: "Microsoft Windows ME" (Guess probability: 63%)
[+] Host 192.168.1.200 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above" (Guess
probability: 59%)
[+] Host 192.168.1.200 Running OS: "NetBSD 1.5.2" (Guess probability: 59%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

# Sample Xprobe2 Run

- The first two modules to be initialized and used, 'ICMP Echo' and 'TTL distance', are reachability tests. With the first test, an ICMP echo request is sent to the target machine. The goal is to elicit an ICMP echo reply back from the target system:

```
11:40:37.046355 192.168.1.13 > 192.168.1.200: icmp: echo request (ttl 64, id 477, len 41)
```

```
4500 0029 01dd 0000 4001 f4d1 c0a8 010d
c0a8 01c8 0800 b6be dd59 0000 5850 524f
4245 322d 7072 6f62 65
```

```
11:40:37.046587 192.168.1.200 > 192.168.1.13: icmp: echo reply (ttl 128, id 1817, len 41)
```

```
4500 0029 0719 0000 8001 af95 c0a8 01c8
c0a8 010d 0000 bebe dd59 0000 5850 524f
4245 322d 7072 6f62 6500 0000 0000 fce5
84a7
```

## Sample Xprobe2 Run

- With the second reachability test a TCP SYN packet is sent to the target system. The goal is to elicit a response from the target system, a TCP SYN/ACK (when the TCP port is opened) or a TCP RST packet (when the TCP port is closed):

```
11:40:37.049343 192.168.1.13.5557 > 192.168.1.200.65535: S [tcp sum ok] 1:1(0)
win 512 (DF) (ttl 80, id 5774, len 40)
      4500 0028 168e 4000 5006 901c c0a8 010d
      c0a8 01c8 15b5 ffff 0000 0001 0000 0000
      5002 0200 1407 0000
11:40:37.049581 192.168.1.200.65535 > 192.168.1.13.5557: R [tcp sum ok] 0:0(0)
ack 2 win 0 (ttl 128, id 1818, len 40)
      4500 0028 071a 0000 8006 af90 c0a8 01c8
      c0a8 010d ffff 15b5 0000 0000 0000 0002
      5014 0000 15f4 0000 0000 0000 0000 57de
      88ff
```

## Sample Xprobe2 Run

- If no answer is received, a second TCP SYN packet will be sent targeting a different TCP port on the targeted system, with the same idea in mind. Only if these attempts will not produce a reply from the target system, a UDP datagram will be sent to the target system in an attempt to elicit an ICMP Port Unreachable error message.
- All test within the second reachability module work in a traceroute like manner.
- The rest of the modules which are currently available with Xprobe v2 are fingerprinting modules which are based on the fingerprinting tests we have used for the original Xprobe v1.

# Sample Xprobe2 Run

- The results are being examined and compared with the fingerprinting database, and scores are being calculated according to each fingerprinting module.
- The Operating System Fingerprint that Xprobe2 returns is the most probable match, taken from the sum of all scores. The answer also reflects other possibilities:

```
[+] Primary guess:  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2"  
(Guess probability: 68%)  
[+] Other guesses:  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows XP Professional"  
(Guess probability: 68%)  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows ME" (Guess probability: 63%)  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above"  
(Guess probability: 59%)  
[+] Host 192.168.1.200 Running OS: "NetBSD 1.5.2" (Guess probability: 59%)
```

45

# Sample Xprobe2 Run

```
[+] Primary guess:  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2"  
(Guess probability: 68%)  
[+] Other guesses:  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows XP Professional"  
(Guess probability: 68%)  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows ME" (Guess probability: 63%)  
[+] Host 192.168.1.200 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above"  
(Guess probability: 59%)  
[+] Host 192.168.1.200 Running OS: "NetBSD 1.5.2" (Guess probability: 59%)
```

- **With our example, Microsoft Windows XP and Microsoft Windows 2000 have received the same score. This is due to the fact that they share a very similar TCP/IP stack.**

**So how this works on the wire?**

## **Xprobe2 Demo**

**When thinking of a great, unbiased, accurate, cool  
broadcast service, for me there is only one...**

# Islamic Republic of IRAN – Broadcasting

Islamic Republic of Iran Broadcasting - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.irib.com/

WWW.IRIB.COM Islamic Republic Of IRAN Broadcasting

Arabic English فارسی

HINDI Live Radio-Special program

ایران - مهان - اقتصادی علمی فرهنگی - ورزشی - آب و هوا

دیدار خاویز سولانا با رئیس جمهوری

عمان؛ ممله به عراق نابفردانه است

World Service

Kol-David

The Latest Archive of Hebrew Radio

www.sahartv.com

LIVE

The Latest Report

WWW.IRIB.COM/TV

پخش

Internet

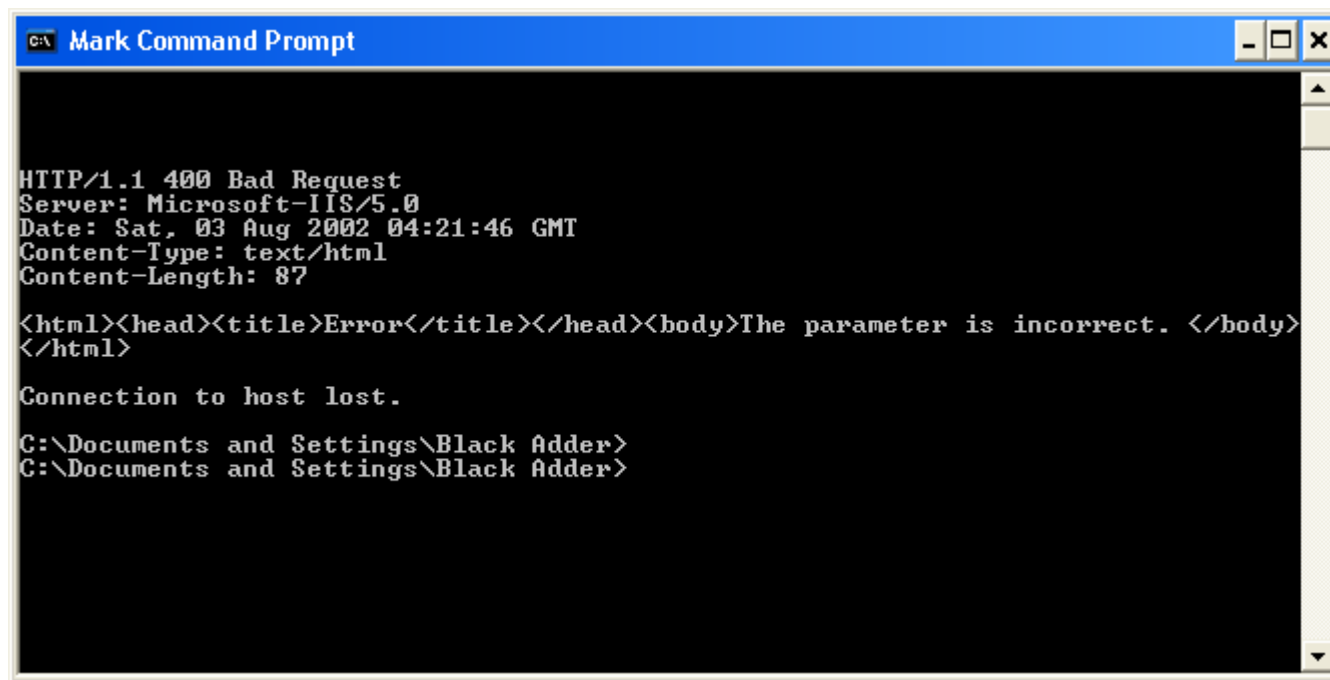
```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.irib.com
```

```
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
```

```
[+] Target is www.irib.com
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 62.220.119.50 is up (Guess probability: 100%)
[+] Target: 62.220.119.50 is alive
[+] Primary guess:
[+] Host 62.220.119.50 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2" (Guess probability: 68%)
[+] Other guesses:
[+] Host 62.220.119.50 Running OS: "Microsoft Windows XP Professional" (Guess probability: 68%)
[+] Host 62.220.119.50 Running OS: "OS X 10.1.5" (Guess probability: 63%)
[+] Host 62.220.119.50 Running OS: "Microsoft Windows ME" (Guess probability: 63%)
[+] Host 62.220.119.50 Running OS: "NetBSD 1.5.2" (Guess probability: 63%)
[+] Host 62.220.119.50 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above" (Guess probability: 59%)
[+] Host 62.220.119.50 Running OS: "Sun Solaris 5 (SunOS 2.5)" (Guess probability: 59%)
[+] Host 62.220.119.50 Running OS: "Sun Solaris 6 (SunOS 2.6)" (Guess probability: 59%)
[+] Host 62.220.119.50 Running OS: "Sun Solaris 7 (SunOS 2.7)" (Guess probability: 59%)
[+] Host 62.220.119.50 Running OS: "Sun Solaris 8 (SunOS 2.8)" (Guess probability: 59%)
[+] Host 62.220.119.50 Running OS: "FreeBSD 3.4" (Guess probability: 59%)
[+] Host 62.220.119.50 Running OS: "Linux Kernel 2.2.x" (Guess probability: 54%)
[+] Host 62.220.119.50 Running OS: "Linux Kernel 2.4.0 - 2.4.4" (Guess probability: 54%)
[+] Host 62.220.119.50 Running OS: "Microsoft Windows 98/98SE" (Guess probability: 54%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

50

# Islamic Republic of IRAN – Broadcasting



```
C:\ Mark Command Prompt

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sat, 03 Aug 2002 04:21:46 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

Connection to host lost.

C:\Documents and Settings\Black Adder>
C:\Documents and Settings\Black Adder>
```

**Looking for a nice comfortable dungeon in a near by  
jail?**

# Iran Yellow Pages

The screenshot shows a web browser window titled "iran index" displaying the homepage of Iran Yellow Pages. The browser's address bar shows "http://www.iranyellowpages.com/". The website features a blue header with the "Iran Yellow Pages" logo and a navigation menu. The main content area is titled "Iran Yellow Pages.com" and includes a date and time stamp: "Tue, July 30, 2002 12:52". Below the title, there are navigation buttons for "Home Page", "Full Page", "Half Page", and "Links". A "Category Browser" section lists various categories such as Accommodation, Food & Dining, Health & Medicine, Legal & Financial, Recreation & Sports, Retail & Shopping, Computers & Electronics, Business & Economy, Art & Entertainment, and Automotive. A search bar is located on the left side of the page. The browser's status bar at the bottom indicates "Internet".

53

```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.iranyellowpages.com
```

```
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
```

```
[+] Target is www.iranyellowpages.com
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 203.115.112.147 is up (Guess probability: 100%)
[+] Target: 203.115.112.147 is alive
[+] Primary guess:
[+] Host 203.115.112.147 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above" (Guess probability: 77%)
[+] Other guesses:
[+] Host 203.115.112.147 Running OS: "Microsoft Windows NT 4 Service Pack 3 and Below" (Guess probability: 68%)
[+] Host 203.115.112.147 Running OS: "Microsoft Windows ME" (Guess probability: 68%)
[+] Host 203.115.112.147 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2" (Guess probability: 63%)
[+] Host 203.115.112.147 Running OS: "Microsoft Windows XP Professional" (Guess probability: 63%)
[+] Host 203.115.112.147 Running OS: "Microsoft Windows 98/98SE" (Guess probability: 59%)
[+] Host 203.115.112.147 Running OS: "NetBSD 1.5.2" (Guess probability: 59%)
[+] Host 203.115.112.147 Running OS: "Linux Kernel 2.4.5 and above" (Guess probability: 54%)
[+] Host 203.115.112.147 Running OS: "Linux Kernel 2.4.0 - 2.4.4" (Guess probability: 54%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

# Iran Yellow Pages

```
carman:~/tmp/xprobe2/src # telnet 203.115.112.147 80
Trying 203.115.112.147...
Connected to 203.115.112.147.
Escape character is '^]'.

```

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Fri, 02 Aug 2002 01:26:36 GMT
Content-Type: text/html
Content-Length: 87

```

```
<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html>Connection closed by foreign host. carman:~/tmp/xprobe2/src #

```

**Bored while in Jail? Maybe some more reading?**

# Tehran Times

**THURSDAY**  
August 1, 2002

**tehrantimes.com**  
International Daily

[www.worldinformation.com](http://www.worldinformation.com)

tehrantimes.com [Advertise](#) [Archives](#) [Contact Us](#) [Feedback](#) [Advanced Search](#)

**NEWS**

- Politics
- Domestic
- International
- Social
- Sports
- Science
- Weather
- Economy
- Culture
- Religion
- Feature
- Other News

**NEWS**

**Skhamkhani Strongly Backs IRGC's Statement**

*TEHRAN TIMES POLITICAL DESK*

TEHRAN - Issuing statements about the concerns of the Islamic Revolution is part of the duty of the Islamic Republic Guards Corps (IRGC), Defense Minister Ali Shamkhani said on Wednesday.

[FULL STORY](#)

**Search Last Seven Issues**

[Search](#)

Visit our [Advanced Search](#) to search past editions.

[Help](#)

**Custom News**

Use this link to customize TehranTimes according to your interest

**Edit Custom News**

Click to change your news profiles

**In other news**

[ISAF Says Was Aware of Afghan Bomb Plot a Week Ago](#)

[Lebanese Office Worker Kills Eight](#)

**SPECIAL**

- Learning
- It's Worth
- Knowing

**Views**

- Opinion
- Perspectives
- Events

**Done** **Internet**

57

```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.tehrantimes.com
```

```
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
```

```
[+] Target is www.tehrantimes.com
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 208.158.112.245 is up (Guess probability: 50%)
[+] Target: 208.158.112.245 is alive
[+] Primary guess:
[+] Host 208.158.112.245 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above"
(Guess probability: 77%)
[+] Other guesses:
[+] Host 208.158.112.245 Running OS: "Microsoft Windows NT 4 Service Pack 3 and Below"
(Guess probability: 68%)
[+] Host 208.158.112.245 Running OS: "Microsoft Windows ME" (Guess probability: 68%)
[+] Host 208.158.112.245 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2" (Guess probability: 63%)
[+] Host 208.158.112.245 Running OS: "Microsoft Windows XP Professional" (Guess probability: 63%)
[+] Host 208.158.112.245 Running OS: "Microsoft Windows 98/98SE" (Guess probability: 59%)
[+] Host 208.158.112.245 Running OS: "NetBSD 1.5.2" (Guess probability: 59%)
[+] Host 208.158.112.245 Running OS: "Linux Kernel 2.4.5 and above" (Guess probability: 54%)
[+] Host 208.158.112.245 Running OS: "Linux Kernel 2.4.0 - 2.4.4" (Guess probability: 54%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

58

# Tehran Times

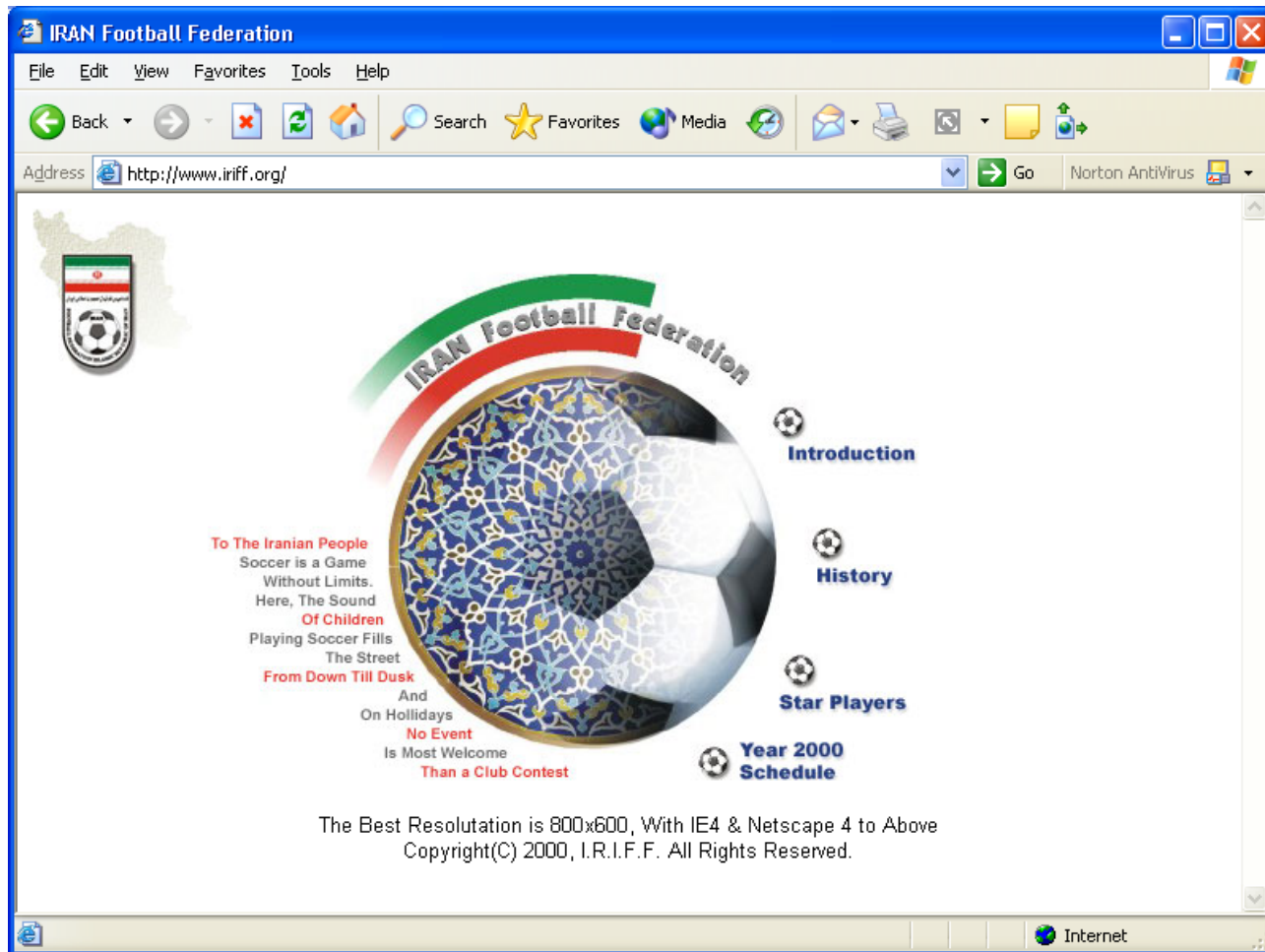
```
carman:~/tmp/xprobe2/src # xprobe -v 208.158.112.245
X probe ver. 0.0.2
-----
Interface: ppp0/64.24.37.117

LOG: Target: 208.158.112.245
LOG: Netmask: 255.255.255.255
LOG: probing: 208.158.112.245
LOG: [send]-> UDP to 208.158.112.245:32132
LOG: [98 bytes] sent, waiting for response.
TREE: IP total length field value is OK
TREE: Frag bits are OK
LOG: [send]-> ICMP echo request to 208.158.112.245
LOG: [68 bytes] sent, waiting for response.
TREE: Microsoft Windows Family TCP stack
TREE: Other Windows-based OS (ttl: 116)
TREE: Other Windows-based OS (98/98SE/NTsp3-/NTsp4+)
LOG: [send]-> ICMP time stamp request to 208.158.112.245
LOG: [68 bytes] sent, waiting for response.
Receive timeout. Quitting..
TREE: Windows NTsp3-!Windows NTsp4+
LOG: [send]-> ICMP address mask request to 208.158.112.245
LOG: [48 bytes] sent, waiting for response.
LOG: Receive timeout. Quitting..

FINAL:[ Windows NTsp4+ ]
```

**Bored while in Jail? Had enough reading? Maybe join an out-of-the-cell activities like the following**

# Iran Football Association



```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.iriff.org
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com

[+] Target is www.iriff.org
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 205.178.180.168 is up (Guess probability: 100%)
[+] Target: 205.178.180.168 is alive
[+] Primary guess:
[+] Host 205.178.180.168 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above"
(Guess probability: 77%)
[+] Other guesses:
[+] Host 205.178.180.168 Running OS: "Microsoft Windows NT 4 Service Pack 3 and Below"
Guess probability: 68%)
[+] Host 205.178.180.168 Running OS: "Microsoft Windows ME" (Guess probability: 68%)
[+] Host 205.178.180.168 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2"
(Guess probability: 63%)
[+] Host 205.178.180.168 Running OS: "Microsoft Windows XP Professional"
(Guess probability: 63%)
[+] Host 205.178.180.168 Running OS: "Microsoft Windows 98/98SE" (Guess probability: 59%)
[+] Host 205.178.180.168 Running OS: "NetBSD 1.5.2" (Guess probability: 59%)
[+] Host 205.178.180.168 Running OS: "Linux Kernel 2.4.5 and above" (Guess probability: 54%)
[+] Host 205.178.180.168 Running OS: "Linux Kernel 2.4.0 - 2.4.4" (Guess probability: 54%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

# Iran Football Association

```
carman:~/tmp/xprobe2/src # telnet www.iriff.org 80
Trying 205.178.180.168...
Connected to www.iriff.org.
Escape character is '^]'.
```

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Fri, 02 Aug 2002 01:54:00 GMT
Content-Type: text/html
Content-Length: 87
```

```
<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html>Connection closed by foreign host. carman:~/tmp/xprobe2/src #
```

**After one long “organized” vacation one needs a real  
vacation**

# Iran Hotels

IranHotels, the site to find Hotels in Iran

File Edit View Favorites Tools Help

Address <http://www.iranhotels.com/>

IranHotels  
اولین مجموعه هتلهای ایرانی در اینترنت

RESERVATION CENTER

English

NEW SEARCH

IranHotels

IranHotels RESERVATION CENTER is the only and the first online inquiry system with live to search for Iranian Hotels and get travel services for Iran. With IranHotels RESERVATION CENTER, you will be available to contact hotels and tour operators in Iran directly, so we do not leave your travel plans in the hands of a computer.

**The best offer...**  
Get the best offer using IranHotels RESERVATION CENTER. All registered

hotels and agencies by IranHotels can get your request. So you can choose between several offers from different hotels and agencies in Iran. Be sure, every hotel will give you its best possible offer, because only you can check and see the different offers.

**Eram Hotel**

**Become a member**  
Add your Hotel  
Find by IranHotels what you need to have success on the world wide web. Register your own domain and get your WEBSITE by IranHotels Server. Your hotel will be included in our database free.

**WEBSITE FOR IRANIAN HOTELS**

**Hotels**

City: All

star category: All

Hotel:

Search

**Travel services**  
IRAN has opened the doors to all visitors from all over the world. Tour operators and travel agencies can help you to organize your trip to IRAN.

Select a country to search for tour operators and travel agencies specializes in travel and tour to IRAN

Iran Search

Internet

```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.iranhotels.com
```

```
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
```

```
[+] Target is www.iranhotels.com
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 62.26.131.13 is up (Guess probability: 100%)
[+] Target: 62.26.131.13 is alive
[+] Primary guess:
[+] Host 62.26.131.13 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2"
(Guess probability: 77%)
[+] Other guesses:
[+] Host 62.26.131.13 Running OS: "Microsoft Windows XP Professional" (Guess probability: 77%)
[+] Host 62.26.131.13 Running OS: "Microsoft Windows ME" (Guess probability: 72%)
[+] Host 62.26.131.13 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above"
(Guess probability: 68%)
[+] Host 62.26.131.13 Running OS: "Microsoft Windows 98/98SE" (Guess probability: 63%)
[+] Host 62.26.131.13 Running OS: "NetBSD 1.5.2" (Guess probability: 63%)
[+] Host 62.26.131.13 Running OS: "Linux Kernel 2.4.5 and above" (Guess probability: 59%)
[+] Host 62.26.131.13 Running OS: "Linux Kernel 2.4.0 - 2.4.4" (Guess probability: 59%)
[+] Host 62.26.131.13 Running OS: "Linux Kernel 2.2.x" (Guess probability: 59%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

# Iran Hotels

```
carman:~/tmp/xprobe2/src # telnet www.iranhotels.com 80
Trying 62.26.131.13...
Connected to www.iranhotels.com.
Escape character is '^]'.

```

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 02 Aug 2002 02:00:21 GMT
Content-Type: text/html
Content-Length: 79

```

```
<html><head><title>Error</title></head><body>Falscher Parameter.
</body></html>Connection closed by foreign host. carman:~/tmp/xprobe2/src #

```

## Some Re-Visits

# Wimbledon

Welcome to GoTennis : It's Tennis, on the Net! - Microsoft Internet Explorer

Address: http://www.wimbledon.org/

**GOTENNIS** "It's Tennis, on the Net™"

**US Open 2002** TennisTours.com **I ♥ TENNIS** Get a Tour Package >>

Welcome - Already a member? Sign in Friday, August 02, 2002

Home | Tennis Travel | Event Calendar | Pro Shop | Tickets & Tours | Global Sites | Player Services | Fan Zone

US Open Tickets & Tour Packages My Home | Discuss | Get Our Newsletter | Find a Pro

## Haas Squeeks Past Sampras

**GoTennis Today**

- Roddick-Lapenanti Match Gets Loud & Ugly
- Anna K. Moves Into Acura Classic Quarters
- Safin Squeeks Past Rios In Toronto Masters Thriller
- Rafter: It's A Boy!

**Scoreboard**

- Toronto Masters
- Acura Classic
- Match Odds

**Live Scores**

**Daily Netcast**

- Listen :: WTA
- Listen :: ATP

**Pro Shop**

- Racquets
- Men's Shoes
- Women's Shoes
- Men's Apparel
- Women's Apparel
- Tennis Bags
- Wimbledon Shop
- US Open Shop
- Great Prices!

**Babolat Racquet Line**

**ATP Tour Info**

1 Hewitt	524
2 Safin	397
3 Henman	378
4 Costa	340
5 Agassi	332

[Full Rankings >>](#)

**Men's Profiles**

**GoTennis = Your US Open Store >>**

- US Open Gear & Apparel
- Tour Packages (Hotel, Tickets & Shuttle)
- Tickets For All Levels & Sessions

**Latest Headlines**

- Sampras storms back to beat Lee at Masters, will face Haas**  
TORONTO (August 01, 2002 12:21 AM EDT) - Pete Sampras, seeking his first tournament title in over two years, beat Hyung-taik Lee 3-6, 7-6 (5), 6-2 Wednesday night in a second-round match in the Tennis

**Ask the Experts...**

**Ask The Coach**  
Van Der Meer

**Courtside**

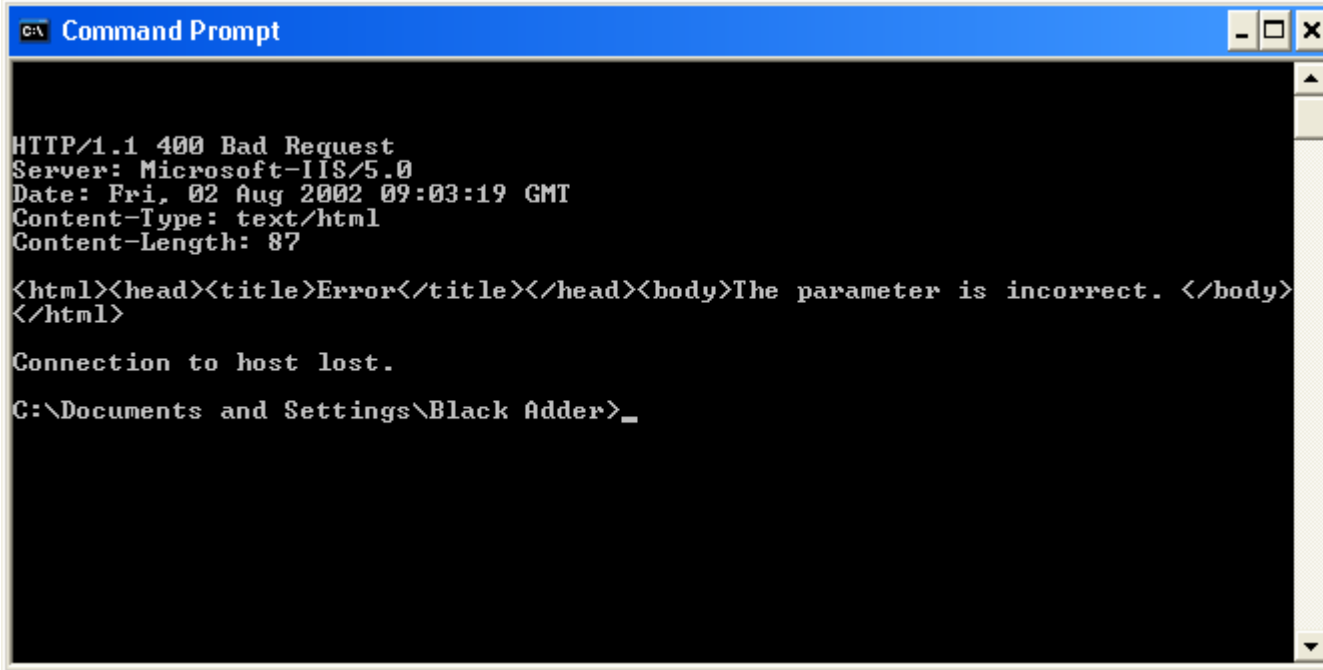
```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.wimbeldon.org
```

```
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
```

```
[+] Target is www.wimbeldon.org
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 63.110.130.171 is up (Guess probability: 100%)
[+] Target: 63.110.130.171 is alive
[+] Primary guess:
[+] Host 63.110.130.171 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2" (Guess probability: 77%)
[+] Other guesses:
[+] Host 63.110.130.171 Running OS: "Microsoft Windows XP Professional" (Guess probability: 77%)
[+] Host 63.110.130.171 Running OS: "Microsoft Windows ME" (Guess probability: 72%)
[+] Host 63.110.130.171 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above" (Guess probability:
68%)
[+] Host 63.110.130.171 Running OS: "Microsoft Windows 98/98SE" (Guess probability: 63%)
[+] Host 63.110.130.171 Running OS: "NetBSD 1.5.2" (Guess probability: 63%)
[+] Host 63.110.130.171 Running OS: "Linux Kernel 2.4.5 and above" (Guess probability: 59%)
[+] Host 63.110.130.171 Running OS: "Linux Kernel 2.4.0 - 2.4.4" (Guess probability: 59%)
[+] Host 63.110.130.171 Running OS: "Linux Kernel 2.2.x" (Guess probability: 59%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

70

# Wimbledon



```
C:\ Command Prompt

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 02 Aug 2002 09:03:19 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

Connection to host lost.

C:\Documents and Settings\Black Adder>_
```

# State Family Planning Commission of China

The screenshot shows the website of the State Family Planning Commission of China, viewed in Microsoft Internet Explorer. The browser's address bar displays <http://www.sfpc.gov.cn/EN/>. The website features a blue header with the title "State Family Planning Commission of China" and a map of China. Below the header, there is a "Fresh News" section with a list of articles, a "Project Initiatives" section with icons for various programs, and a left sidebar with navigation links.

**Navigation Links (Left Sidebar):**

- Homepage
- Panorama
- Data
- Institutional Chart
- International Cooperation
- FAQ
- Links
- Contact
- Chinese

**Fresh News (Main Content):**

**High Incidence of Birth Defects to Be Effectively Controlled by 2010**

- ▶ [China regrets US fund move](#)
- ▶ [Statement by the Spokesperson of the State Family Planning Commission of China on U.S. Decision not to Grant Funding to UNFPA](#)
- ▶ [Family planning policy helps reduce poverty](#)
- ▶ [Population work sees progress](#)
- ▶ [World Population Day: China talks about sex, health, life](#)
- ▶ [National Family Planning & Reproductive Health Survey \(2001\)](#)
- ▶ [AIDS may kill 1 in 4 workers in some nations](#)
- ▶ [China Opens First Website on AIDS Prevention](#)
- ▶ [Fewer women want to become mothers](#)
- ▶ [The 8th National Population Science Symposium cum-Representative Conference Held at Beijing](#)
- ▶ [SFPC Minister Zhang Visits Marie Stopes](#)
- ▶ [Minister Zhang Discusses Bilateral Cooperation with British Minister of International Development](#)
- ▶ [Minister Zhang on China's Population and Family](#)

**Project Initiatives (Right Sidebar):**

- Reproductive Health
- Gender (Gender equality/ Women's Empowerment)
- STDs HIV AIDs
- Adolescent
- Family
- Migrants

```
carman:~/tmp/xprobe2/src # ./xprobe2 -v www.sfpc.gov.cn
```

```
XProbe2 v.0.1 Copyright (c) 2002 fygrave@tigerteam.net, ofir@sys-security.com
```

```
[+] Target is www.sfpc.gov.cn
[+] Loading modules.
[+] Following modules are loaded:
    [x]ICMP echo (ping)
    [x]TTL distance
    [x]ICMP echo
    [x]ICMP Timestamp
    [x]ICMP Address
    [x]ICMP Info Request
    [x]ICMP port unreachable
[+] 7 modules registered
[+] Initializing scan engine
[+] Running scan engine
[+] Host: 159.226.187.2 is up (Guess probability: 50%)
[+] Target: 159.226.187.2 is alive
[+] Primary guess:
[+] Host 159.226.187.2 Running OS: "Microsoft Windows 2000/2000SP1/2000SP2"
(Guess probability: 72%)
[+] Other guesses:
[+] Host 159.226.187.2 Running OS: "Microsoft Windows XP Professional" (Guess probability: 72%)
[+] Host 159.226.187.2 Running OS: "Microsoft Windows ME" (Guess probability: 68%)
[+] Host 159.226.187.2 Running OS: "NetBSD 1.5.2" (Guess probability: 63%)
[+] Host 159.226.187.2 Running OS: "Microsoft Windows NT 4 Service Pack 4 and Above"
(Guess probability: 63%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

73

# State Family Planning Commission of China

```
carman:~ # telnet www.sfpc.gov.cn 80
Trying 159.226.187.2...
Connected to www.sfpc.gov.cn.
Escape character is '^]'.
```

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 02 Aug 2002 06:56:18 GMT
Content-Type: text/html
Content-Length: 87
```

```
<html><head><title>Error</title></head><body>The parameter is incorrect.
</body></html>Connection closed by foreign host.
```

# The fingerprinting Database

- A full description of how to add signatures and what the different keywords symbolize will be published next week

# Credits

- **Meder Kydyraliev** (Help with programming)
  
- Also thanks to **Cat & Major** for allowing me to get on the G00n network last night

# Further Reading

- Arkin Ofir, “ICMP Usage in Scanning” research project

<http://www.sys-security.com>

- Arkin Ofir, “ICMP Usage in Scanning” version 3.0, June 2001

<http://www.sys-security.com/html/projects/icmp.html>

- Arkin Ofir & Fyodor Yarochkin, “X – Remote ICMP based OS fingerprinting Techniques”, August 2001 (This paper describes the first generation of Xprobe).

[http://www.sys-security.com/archive/papers/X\\_v1.0.pdf](http://www.sys-security.com/archive/papers/X_v1.0.pdf)

- Arkin Ofir & Fyodor Yarochkin, “ICMP based remote OS TCP/IP stack fingerprinting techniques”, Phrack Magazine, Volume 11, Issue 57, File 7 of 12, Published August 11, 2001.

<http://www.sys-security.com/archive/phrack/p57-0x07>

# Questions?

