



**DECEIVING ADVERSARY NETWORK
SCANNING EFFORTS USING HOST-BASED
DECEPTION**

GRADUATE RESEARCH PROJECT

Sherry B. Murphy, Major, USAF
AFIT/ICW/ENG/09-04

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/ICW/ENG/09-04

**DECEIVING ADVERSARY NETWORK SCANNING EFFORTS
USING HOST-BASED DECEPTION**

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Sherry B. Murphy, BS, MS

Major, USAF

June 2009

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED

**DECEIVING ADVERSARY NETWORK SCANNING EFFORTS
USING HOST-BASED DECEPTION**

Sherry B. Murphy, BS, MS

Major, USAF

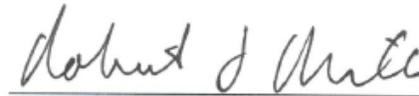
Approved:



Lt Col Jeffrey T. McDonald, USAF (Chairman)

9 JUN 09

date



Robert F. Mills, PhD (Member)

9 JUN 09

date

Abstract

In this research we demonstrate the usefulness of manipulating system traffic to deceive an attacker's operating system (OS) fingerprinting as part of their network scanning efforts. Specifically, we address whether host-based OS obfuscation has merit and application as an integral part of Air Force network defense and whether the technique warrants, further research and application development. We accomplish this objective through a literature review and a proof of concept evaluation of a selected OS obfuscation tool against selected OS fingerprinting tools under current Air Force network configuration. Our focus areas in the literature review include: how to characterize the scanning phase of an adversary attack, a survey of current OS fingerprinting and obfuscation tools, and description of current AF network concepts. To evaluate effectiveness of a candidate OS tool, we setup an experimental network environment that simulates adversarial network scanning.

Results of our study are: a) that current OS obfuscation tools designed for Windows OS are capable of providing some OS obfuscation on AF networks; b) that the current tools need to be evaluated for impacts on network maintenance tools and processes, to include future initiatives like IPv6; and c) that the current tools need to improve OS fingerprints and add options to force inconclusive results from fingerprinting tools.

Acknowledgements

This paper is dedicated to my wonderful husband for his sound advice and enduring love and to my wonderful daughter for her love and encouragement.

So many others are responsible for my success. I owe much to LtCol McDonald for patiently guiding me through my research; to Dr. Robert Mills for his guidance through the cyber program; to Sam Birch for offering insight into obfuscation; to Mr. Tim Lacey and Mr. Ryan Harris for setting up the backbone of my test network; to fellow students MSgt Wabiszewski, MSgt William Bai, Mr. Daniel Koranek, 2Lt Kyle Stewart, 2Lt Nick Fritts, and Maj Matt Larkowski, for helping me stand up two functional network domains.

Table of Contents

Abstract.....	iv
Acknowledgements.....	v
List of Figures.....	vii
List of Tables.....	ix
I. Introduction.....	1
Importance of the Topic.....	1
The Research Question.....	2
Organization of the Proposal.....	3
II. Literature Review.....	4
OS Fingerprinting in the Attack Process.....	4
Impacts of OS Obfuscation on Scanning Efforts.....	7
Challenges to OS Obfuscation.....	8
Current AF Network.....	10
III. Research Design.....	13
Goal.....	13
Threat Model.....	13
Defense Model.....	15
IV. Test Results.....	26
V. Discussion.....	29
Study Findings.....	29
Strengths and Weaknesses of the Study.....	30
VI. Conclusion.....	32
Summary.....	32
Future Research.....	32
Appendix A: Test Network Details.....	35
Appendix B: Fingerprinting Output Files before Obfuscation on Targets.....	36
Nmap Report with No Obfuscation on Targets – Polite mode.....	36
Nmap Report with No Obfuscation on Targets – Aggressive mode.....	39
p0f2 Output Data File with No Obfuscation on Targets.....	41
Appendix C: Fingerprinting Tool Output with Obfuscation on Targets.....	54
Nmap Output Data File with Obfuscation on Targets – Polite Mode.....	54
Nmap Output Data File with Obfuscation on Targets – Aggressive Mode.....	55
p0f2 Output Data File with Obfuscation on Targets.....	58
Bibliography.....	74
Vita.....	76

List of Figures

Figure	Page
Figure 1: FTP Banner Disclosing OS Information	10
Figure 2: Notional AF Network.....	11
Figure 3: Sample Fingerprint	16
Figure 4: Sample Footprint	17
Figure 5: Sample Scan Return	18
Figure 6: OSfuscate.....	19
Figure 7: Test Domains.....	22
Figure 8: TTL before Obfuscation.....	28
Figure 9: TTL after Obfuscation.....	28
Figure 10: Nmap Polite Scan Result for Server.....	36
Figure 11: Nmap Polite Scan Result for Vista Client.....	37
Figure 12: Nmap Polite Scan for XP Client.....	38
Figure 13: Nmap Aggressive Scan for XP Client.....	39
Figure 14: Nmap Aggressive Scan Results for Vista Client.....	40
Figure 15: Nmap Scan Results for XP Client	41
Figure 16: Nmap Polite Scan Results for Server with OSfuscation	54
Figure 17: Nmap Polite Scan Results for Vista Client with OSfuscation.....	54
Figure 18: Nmap Polite Scan Results for XP Client with OSfuscation.....	55
Figure 19: Nmap Aggressive Scan Results for Server with OSfuscation.....	55
Figure 20: Detailed OS Results for Nmap Aggressive Scan on Server with OSfuscation	56

Figure 21: Nmap Aggressive Scan Results for Vista Client with OSfuscation	56
Figure 22: Detailed OS Results for Nmap Aggressive Scan on Vista Client with OSfuscation	57
Figure 23: Nmap Aggressive Scan Results for XP Client with OSfuscation	57
Figure 24: Detailed OS Results for Nmap Aggressive Scan on XP Client with OSfuscation	58

List of Tables

Table 1: Summary of Attack Process.....	4
Table 2: OS Fingerprinting Tool Overview	6
Table 3: OSfuscate Registry Changes.....	19
Table 4: Test Scenario for Passive Fingerprinting.....	23
Table 5: Test Scenario Steps for Active Fingerprinting	24
Table 6: p0f2 Option Explanation.....	25
Table 7: Nmap Option Explanation	25
Table 8: Fingerprinting Results with No Obfuscation.....	26
Table 9: Test Results Emulating LINUX OS	27

DECEIVING ADVERSARY NETWORK SCANNING EFFORTS USING HOST-BASED DECEPTION

I. Introduction

“... for more than 15 years the US government and DoD networks have come under increasing pressure to attacks and probes from adversaries, as diverse as nation states, to the disgruntled individual or bored teenage hacker. And while we have detected illicit activity on our networks for more than 15 years and employ resources to offer a comprehensive multi-disciplinary approach to protecting our networks, we need to do more.”

-- General Kevin P. Chilton, Commander
United States Strategic Command, 2009

The number of reported cybersecurity attacks against federal agencies has more than tripled since 2006 (Hoover, 2009). In 2008, Federal agencies reported to the U.S. Computer Emergency Readiness Team that they had been victims of 18,050 cybersecurity attacks (Hoover, 2009). The opening phase of these attacks often involves attempts to gather data that will guide later stages of the attacks. One key piece of information that attackers need is the identity of the target system’s operating system. Various OS fingerprinting techniques have been developed and bundled in OS fingerprinting tools. Denying the hacker access to accurate OS information by defeating these tools represents an important first step to defeating adversary scanning efforts. In this research, we posit that host-based OS obfuscation may be an effective way to mitigate such tools and methods.

Importance of the Topic

Our nation is heavily reliant on computer networks for communication, economy, commerce, and military effectiveness. Our government, the private sector, and educational institutions spend significant resources towards the defense and research of

network defense. In just a 6 month period the US military spent at least \$100 million defending networks and responding to attacks that affected the Pentagon's networks (Levine, 2009). Another indicator of the significance of the nation's cyber-security came when President Obama ordered a 60-day review to examine how federal agencies use technology to protect secrets and data within 20 days of coming to office (Washington Post, 2009). Network protection is clearly critical to the nation's overall security posture.

To address these ever increasing malicious threats, one area of research has focused on determining the utility and feasibility of cyber deception (cydec). Network obfuscation, a key cydec technique, may offer hope to deter attackers and prevent successful attacks when deterrence fails. In 2008, Repik performed an initial assessment on the potential effectiveness of cydec in network defense. In his assessment he describes one possible cydec technique as "altering the signature of a computer so an adversary's tools identify the incorrect operating system, resulting in an ineffective attack" (Repik, 2008). In this study, we examined the potential benefits of host-level OS obfuscation on machines internal to the network. Based on findings from our experiment environment, we provide a key perspective on the efficacy of continued network obfuscation efforts.

The Research Question

In this research, we ask whether a clear benefit and feasibility exists for using OS obfuscation on AF networks to defeat OS fingerprinting techniques, to include whether sufficient tools are available to do OS obfuscation. Peers often mention the saying "security through obscurity" when the topic of obfuscation is being discussed. Obfuscation is "disarray, confusion resulting from failure to understand" (Wolfram

Mathematica, 2009). While obfuscation cannot stand alone or even stand as the first line defense as a network protection strategy, we believe that any denial of information to an attacker adds to the overall strength of our defenses. In this case, we seek to deny key pieces of information so that scanning efforts are obstructed and clearly revealed and evident.

Organization of the Proposal

The next section reviews key concepts foundational to this study: the attack process, deception basics, OS fingerprinting tools and techniques, OS obfuscation tools and techniques, and Air Force network initiatives that may affect OS obfuscation efforts. We present the design of the study and test plan is presented in Chapter III. In Chapter IV we present the test results from our experiment. We discuss our experiment findings and the strengths and weaknesses of the study in Chapter V. And in the final chapter we present our overall conclusions and areas of possible future analysis.

II. Literature Review

“By not perceiving our enemy yet perceiving ourselves, there will be partial victory and partial loss.”

--Sun-Tzu

OS Fingerprinting in the Attack Process

In order to defeat an attacker, we must look for opportunities to defeat any and all phases of the attack process. Though many network professionals offer different versions of the attack process, the general anatomy of the attack process is made up of five steps: reconnaissance, scanning, gaining access, maintaining access, and covering tracks and hiding. As Table 1 illustrates, in this paper we focused mainly on the scanning step, but for a more detailed look at the attack process we refer the reader to Repik’s work on defeating adversarial intelligence gathering in the network (Repik, 2008) or Counter Hack Reloaded by Skoudis (Skoudis & Liston, 2006).

Table 1: Summary of Attack Process

Step	Description	Goal
1. Reconnaissance	Gather information about potential targets	Acquire info: scope of the target’s activities, domain name, network blocks, reachable IP addresses, running services, system architecture, access control, & employed IDS
2. Scanning	Search target for openings and map network	Acquire info: reachable live hosts, network topology, open ports, services and software versions listening on open ports, and underlying operating system and associated vulnerabilities
3. Gaining Access	Use exploits against identified vulnerabilities to gain access	Gain access by breaking applications, OS, and/or databases, using network attacks
4. Maintaining Access	Maintain access and control of systems	Maintain access and control by using malicious software
5. Covering Tracks and Hiding	Maintain covert control & access to allow for longer presence & return avenue	Be covert by altering event logs, using hidden files and directories, naming files and processes inconspicuously, establish covert channels

Though reconnaissance efforts may result in the discovery of the target OS, the specific goal of determining the target OS is attributed to the scanning phase. One way to defeat or impede the attack process is to prevent the enemy from accurately perceiving us. In this case, we desire to characterize the impact of denying access to accurate information about the OS.

Operating systems have unique characteristics that when left unobscured can help an attacker to identify the operating system being used in the target system. Examples of these characteristics include the TCP/IP packet, response messages to queries, response messages to errors, predictability of sequence numbers, and banner information. Some specific attributes in a TCP/IP session are the values set for time-to-live (TTL), window size, Don't Fragment (DF) bit, and type of service (TOS) (Scambray, McClure, & Kurtz, 2001). By comparing the information gathered about the target OS to profiles established for various systems, a potential attacker can make educated guesses about the target OS (Skoudis & Liston, 2006).

OS information can be gathered through active and/or passive techniques. Tools that use passive fingerprinting techniques intercept and examine existing traffic to make guesses about the OS. As passive tools are dependent on existing traffic, this method may take longer to get a more accurate answer, but they are typically not detectable (Zalewski, 2006). On the other hand, we refer to tools that interact with the target to glean information about the OS as active methods. These active measures have proven to be very effective at accurately identifying the target OS, but can be detected by an intrusion detection systems (IDS) (Scambray, McClure, & Kurtz, 2001).

One very popular tool for OS fingerprinting that uses active techniques, Nmap, has timing options specifically designed to help avoid detection. By changing the timing, Nmap spreads out the appearance of log entries that result from the scan. Other than the “Normal” speed, Nmap has timing options ranging from a super-slow scan called “Paranoid” that sends one packet every 5 minutes to an accelerated mode called “Insane” for the attacker in a hurry (Skoudis & Liston, 2006).

As Table 2 depicts, a simple search of the internet yields several other options for OS fingerprinting tools:

Table 2: OS Fingerprinting Tool Overview

Name	Technique
Nmap by Fyodor	Active
p0f2 by Michael Zalewski	Passive
SinFP by GomoR	Active and passive
Xprobe/Xprobe2 by Ofir Arkin and Fyodor Yarochkin	Active
Ettercap by ALoR and NaGA	Passive
RING by Franck Veysset, et al	Active
Cheops (relies on QueSO by Apostels)	Active

Unlike the wide selection of OS fingerprinting tools returned from a brief Internet search, options for existing OS obfuscation tools are not as robust. One reason for this may be how difficult it is to make enough changes to deceive fingerprinting techniques, while at the same time leaving enough packet integrity so the system still works. Early work in OS obfuscation, once called fingerprint scrubbing, concentrated on obscuring OS information with future goals to try to spoof OS information (Smart, Malan, & Jahanian, 2000). The fingerprint scrubber was placed between the Internet and the network in front of end hosts or a set of network infrastructure components to block stack fingerprinting techniques (Smart, Malan, & Jahanian, 2000).

Given the scarcity of candidates, we found two OS obfuscation tools that are available for immediate use: OSfuscate (Crenshaw, 2008) and Morph (Wang, 2003). Morph runs on Linux systems while OSfuscate runs on Windows systems. Both tools allow the user to select an OS to emulate. Morph intercepts and changes the outbound packets while OSfuscate changes registry values. These changes are designed to stop fingerprinting tools from successfully matching the collected information to the OS profiles in the OS signature found in the fingerprinting tool databases.

Impacts of OS Obfuscation on Scanning Efforts

Denying accurate OS information about the target disrupts the attacker in several ways. On the most basic level, it prevents the attacker from exploiting default passwords established by the vendor in the event a system administrator failed to change it (Skoudis & Liston, 2006). Furthermore, if the target OS has been obfuscated, the target may be perceived as too hard of a target, especially if the hacker's goal is to use a specific exploit against a known vulnerability on a particular OS. An erroneous OS and patch level may cause the attacker to ignore the potential target. For instance, some organizations hack the registry of their own systems if they are unable to quickly patch the system. This action deceives focused network scans that look for systems to exploit based on a specific vulnerability (Birch, 2009).

Another potential benefit of OS obfuscation is that if the attacker is unsure of the OS, the attacker may not use a known effective exploit for fear it will have unintended effects on the target. Instead the attacker invests resources into researching or applying alternate attack methods with lower probability of success, or may simply move to another target. If the attacker assumes the wrong OS or is deceived into accepting false

OS indications and executes a plan against the wrong OS, the consequences can again put the attacker's success at risk. Applying exploits against the wrong OS can yield results from nothing happening all the way to a system crash (Lyon, 2009). For example, a buffer overflow exploit is OS independent, but the payload (written in machine language) must comply with the OS because it makes privileged calls to the OS (Skoudis & Liston, 2006). Linux interprets machine language differently than a Windows OS. Depending on the op codes, the first few bits of all computer commands that indicate what type of call is coming, the computer system could execute a benign command that does nothing, attempt to execute non-executable code causing the program to crash, or attempt to execute code the OS cannot handle causing a "blue screen of death." All of these unwanted results can increase chance of detection, heighten user and administrator alert, or deny access to the target: ultimately, each effect may disrupt an attack before it is ever launched.

Challenges to OS Obfuscation

When employing deception in traditional operations, we need to address a couple of issues: (1) how do we deceive the enemies but not ourselves, and (2) how much of our resources should we commit to the deception that would be used for other activities?

These same issues apply when employing deception in cyber. For example, system administrators use scanning and management tools to monitor the status and health of the network, troubleshoot problems, and ensure systems have the necessary patches loaded. If the hosts are reporting false OS information as a result of obfuscation tools, how will administrators have visibility into their networks and use the tools designed to automate maintenance actions across the network?

As described above, obfuscation offers the potential to complicate a potential attacker's attempts to identify the OS used within a defended network. The potential benefits of obfuscation, however, must be considered within the overall context of network operations. For example, many organizations develop and promulgate standard system configurations to reduce system operating costs and increase operating efficiencies. These standardization efforts could ultimately reduce the effectiveness of obfuscation if those standards become well known; in effect, can obfuscation fool anyone when the attacker already knows the published system standards?

Similarly, disgruntled employee posing an internal threat may already have knowledge of the organizations network and network access at some level. Against this threat OS obfuscation wouldn't be as beneficial.

As mentioned previously, we may categorize OS obfuscation as “security through obscurity”, and thereby attach negative connotations in regards to the strength of the security benefits it offers. However, “security through obscurity” is a concept that is widely used and accepted in other areas, as evidenced by investments in noise jamming where chaff and corner reflectors obfuscate aircraft location. The notion applies to even more mundane applications, such as the extensive use of camouflage on vehicles. Experts realize the value of that OS detection prevention, but they also know “security through obscurity” is never an adequate sole first line of defense (Scambray, McClure, & Kurtz, 2001). We do not advocate OS obfuscation as the sole first line of defense either, but we do recognize the possibility that it could contribute to an overall security posture. After all, which house would a robber steal from, the one with a locked door and an alarm sticker in the window or the one with a locked door without an alarm sticker?

Regardless if an alarm system is actually installed and active, criminal elements will probably go the path of least resistance. In the end, if the technique averts the full weight of force of a network attack, it may prove beneficial to the operational community.

Additionally, information about the OS may be leaked through other means such as in services banners (Lyons, 1998). For example, a telnet or ftp banner shows what OS is running unless the banner is removed or changed (Berrueta, 2003). Attackers can also gain OS information by sniffing DHCP queries from the target (Crenshaw, 2008). In such cases, no amount of OS obfuscation will help.

```
payfonez> telnet ftp.netscape.com 21
Trying 207.200.74.26...
Connected to ftp.netscape.com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

Figure 1: FTP Banner Disclosing OS Information

(Lyons, 1998)

As a final challenge, OS obfuscation is hard! Making enough changes to normal OS functions that trick an attacker while maintaining a stable system that functions, is no small task (Scambray, McClure, & Kurtz, 2001). Like other obfuscation areas, obfuscation tools must keep up with the many current and emerging fingerprinting techniques.

Current AF Network

AF networks follow a defense-in-depth approach. Each of them is tailored to meet the needs of their customer's unique requirements and operate within their budget. A typical configuration includes the following components: a firewall, intrusion detection

system, email server, proxy server, router, internet access, virtual private network access, Windows clients, router, anti-virus tools, and internet access. Currently, AF networks employ IPv4 as its internet protocol. Figure 1 represents a notional AF network.

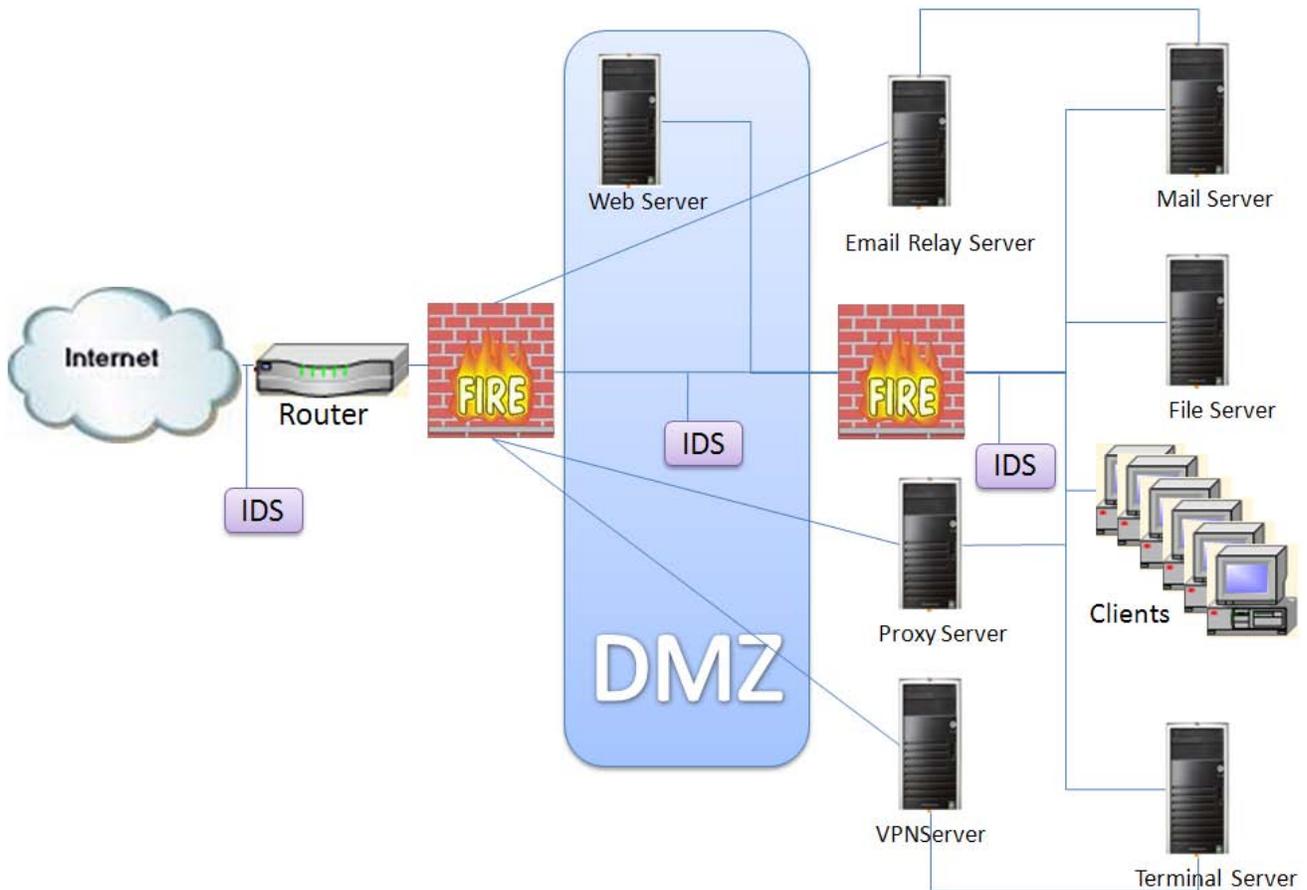


Figure 2: Notional AF Network

The AF has a few initiatives coming soon that may affect OS obfuscation tools. The mandatory use of IPv6 within the Department of Defense is slated to demonstrate IPv6 by June 2008; however it is estimated that it will take an additional 10 years to complete the transition. Also research is being conducted to evaluate the use of virtual machines and IP security (IPSec). This study did not evaluate OS obfuscation in

conjunction with these concepts but focused on the current AF network. Given these background areas, we now describe the details about our test environment.

III. Research Design

Goal

In order to address the feasibility of OS obfuscation tools, we simulate a “standard” AF network environment to examine the effectiveness of a currently available OS obfuscation tool against chosen OS fingerprinting tools. The selected OS obfuscation tool is OSfuscation and the selected OS fingerprinting tools are: Nmap (Network Mapper, an active OS fingerprinting tool) & p0f2 (passive OS fingerprinting version 2, a passive OS fingerprinting tool). As a good defense is tailored to the attacker; we now use threat modeling to look at the attacker.

Threat Model

The actions an attacker takes depend largely on the attacker’s goals, how important success of those goals is, and the perceived level of risk in mounting the attack. Looking at our systems from the perspective of the attacker helps us to anticipate and mitigate attack goals (Swiderski & Snyder, 2004). According to JTF-GNO, attackers want intelligence, counterintelligence, targeting information, operations information, technical information, financial and ID theft, intelligence preparation of the battlefield, and resources (bandwidth and processing power) (Joint Task Force Global Network Operations, 2009). Given this, the attacker profiled in this study desires to have the system remain active and presence undetected.

During the scanning phase of the attack, the attacker looks for entry points into the system and the trust level attained after gaining access through a particular entry point (Swiderski & Snyder, 2004). Knowing the OS helps the attacker identify entry points and is necessary to write a payload or use an existing vetted payload. It is our premise

that OS obfuscation can reduce attackers to guessing which OS(s) are used in a target network. This in turn could force attackers to use broader attack profiles and thereby increase the likelihood of drawing attention to their attacks. As such, obfuscation may ultimately reduce or prevent the success of their attacks.

In summary, OS obfuscation is most effective against an attacker that 1) lacks physical access, 2) does not have knowledge of the network configuration, 3) specifically targets an OS, 4) wants presence and actions to remain undetected, and 5) wants the system to remain up in order to access or manipulate information. Though the attacker may start from outside the network, our tests simulated an attacker already successfully inside the network to evaluate the obfuscation tool in a worst case scenario.

In a best case scenario, OS fingerprinting tools are employed outside of the network. From outside of the network, several active fingerprinting tools are ineffective. For example, in order for Nmap to return target information, it must be executed on the same network segment as the target or a reachable segment to and from the target. In regards to passive fingerprinting methods, the more data analyzed, the more accurate the OS guess. From the inside of the network, passive tools can be set up to intercept not only outbound traffic, but also internal traffic.

In order to gain internal access, the hacker must either hack a router or firewall, spoof traffic, and/or gain insider access (phishing, insider threat...). Simulating the attack from the inside was done to demonstrate a situation when OS fingerprinting tools are most effective.

Defense Model

To defend a network against the described attacker, we configure the established test environment to mask the OS of a server providing mail and domain controller services and two clients. Other defensive measures were to patch the systems and install the latest service packs on the clients and servers.

Tool Selection and Details

We chose Nmap and p0f2 as the active and passive fingerprinting tools for this test. Nmap is easy to use and updated frequently (Smart, Malan, & Jahanian, 2000). It's also well documented, the winner of the 2003 LinuxQuestions.org Members Choice Awards, and mentioned in several resources as a useful tool for hackers and administrators alike. p0f2 was voted #1 OS detection tool in 2006 (Nmap not part of the survey since it was an Nmap mailing list) (Lyon, 2006). Both tools were readily available at no cost.

Nmap ("Network Mapper") is an open source utility that can be used for network exploration and inventory, capturing host or service uptime, and security auditing. Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are running, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on all major OSs (Lyon, 2009).

Nmap sends out a series of packets to different ports on the target (Skoudis & Liston, 2006). Specifically it sends up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target (Lyons). Nmap analyzes the response attributes to generate a fingerprint.

Nmap also measures the predictability of the initial sequence number by sending several SYN-ACK packets to open ports and analyzing how the sequence number changes (Skoudis & Liston, 2006). The predictability of sequence numbers is another differing characteristic of OSs. Other packet probes sent out by Nmap are: SYN packet to open port, NULL packet to open port, SYN|FIN|URG|PSH packet to open port, ACK packet to open port, SYN packet to closed port, ACK packet to closed port, FIN|PSH|URG packet to closed port, and UDP packet to closed port (Skoudis & Liston, 2006).

Nmap has over 1,000 OS fingerprints in its database (Skoudis & Liston, 2006). A current list of OS profiles is maintained online at <http://nmap.org/svn/nmap-os-db><http://nmap.org/svn/nmap-os-db>. Figure 4 provides a representative sample fingerprint for Linux and Windows Vista (Lyons, 2009).

```

# Linux 2.6.15-28-server #1 SMP Thu May 10 10:40:27 UTC 2007 i686 GNU/Linux
(Ubuntu 6.06.1 LTS)
Fingerprint Linux 2.6.11 - 2.6.20
Class Linux | Linux | 2.6.X | general purpose
SEQ(SP=C8-D2%GCD=1-6%ISR=CE-D8%TI=Z%II=I%TS=7)
OPS(O1=M556ST11NW2%O2=M556ST11NW2%O3=M556NNT11NW2%O4=M556ST11NW2%O5=M556ST11N
W2%O6=M556ST11)
WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)
ECN(R=Y%DF=Y%T=3B-45%TG=40%W=16D0%O=M556NNSNW2%CC=N%Q=)
T1(R=Y%DF=Y%T=3B-45%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=Y%DF=Y%T=3B-45%TG=40%W=16A0%S=O%A=S+%F=AS%O=M556ST11NW2%RD=0%Q=)
T4(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(DF=N%T=3B-45%TG=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(DFI=N%T=3B-45%TG=40%CD=S)

# Version 6.0 (compilacion 6001: Service Pack 1)
Fingerprint Microsoft Windows Vista SP1
Class Microsoft | Windows | Vista | general purpose
SEQ(SP=F7-101%GCD=1-6%ISR=108-112%TI=I%II=I%SS=O|S%TS=7)
OPS(O1=M5B0ST11|M5B0NW8ST11%O2=M5B0ST11|M5B0NW8ST11%O3=M5B0NNT11|M5B0NW8NNT11
%O4=M5B0ST11|M5B0NW8ST11%O5=M5B0ST11|M5B0NW8ST11%O6=M5B0ST11)
WIN(W1=2000|FFFF%W2=2000|FFFF%W3=2000|FFFF%W4=2000|FFFF%W5=2000|FFFF%W6=2000)
ECN(R=Y%DF=Y%T=7B-85%TG=80%W=2000|FFFF%O=M5B0NNS|M5B0NW8NNS%CC=N|Y%Q=)
T1(R=Y%DF=Y%T=7B-85%TG=80%S=O%A=O|S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=7B-85%TG=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=7B-85%TG=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=7B-85%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=7B-85%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=7B-85%TG=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=7B-85%TG=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(DF=N%T=7B-85%TG=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(DFI=N%T=7B-85%TG=80%CD=Z)

```

Figure 4: Sample Footprint

After Nmap completes the scan, it matches the collected attributes against the database. Figure 5 provides a representative sample scan return on a subject that is used to match against the database of profiles:

```

OS:SCAN(V=4.85BETA4%D=3/27%OT=22%CT=1%CU=44663%PV=N%DS=0%G=Y%TM=49CD5E4B%P=
OS:i686-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=CD%TI=Z%CI=Z%II=I%TS=8)OPS(O1=M400
OS:CST11NW5%O2=M400CST11NW5%O3=M400CNNT11NW5%O4=M400CST11NW5%O5=M400CST11NW
OS:5%O6=M400CST11)WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)ECN(R
OS:=Y%DF=Y%T=40%W=8018%O=M400CNNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=8000%S=O%A=S+%F=AS%O=M400CST11NW5%RD=
OS:0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=
OS:Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%R
OS:IPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

```

Figure 5: Sample Scan Return

A detailed explanation on to how to read the profiles can be found at <http://nmap.org/book/osdetect-fingerprint-format.html>. Of interest to this study are the attributes changed by the OS obfuscation tool called, OSfuscate. Values present in the example are bolded and highlighted in yellow above and listed below in Table 3.

p0f2 works similarly to Nmap in that it analyzes packets from the target and matches the attribute values to a database of OS fingerprints. p0f2 fingerprints the OS on machines that connect to the machine it is running on--incoming connection (SYN mode--default), machines that its host machine connects to--outgoing connection (SYN+ACK mode), machines the host machine can't connect to--outgoing connection refused (RST+ mode), and machines whose communications p0f2 is set to observe--established connection (stray ACK mode) (Zalewski, the new p0f: 2.0.8, 2006). p0f2 fingerprinting accuracy gets better with time as more packets are available for collection and analysis.

Both Morph and OSfuscate were available for free. However, OSfuscate was used for the experiment because it operates on systems running a Windows OS, the OS of most AF systems. OSfuscate prompts the user to select an OS to emulate. Figure 6 is a screen capture of OSfuscate showing the available OS to emulate. OSfuscate makes changes to the following registry settings to match the selected OS. We list and describe

the registry settings in Table 3. In addition, the third column of Table 3 shows our correlation of the registry changes made by OSfuscate to values found in Nmap OS fingerprints.

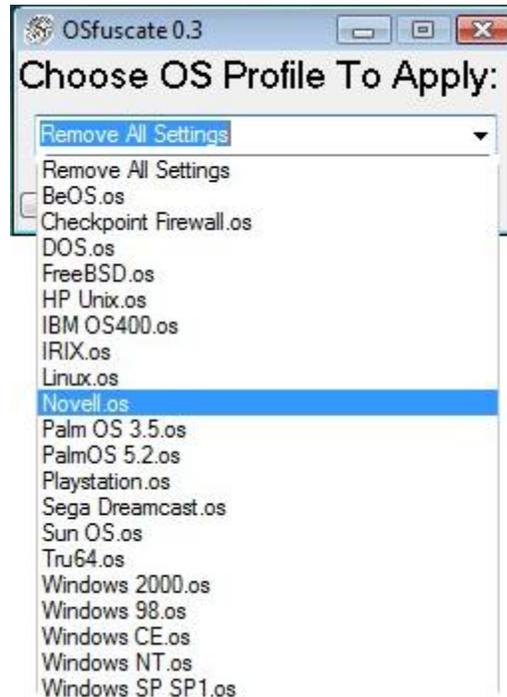


Figure 6: OSfuscate

Table 3: OSfuscate Registry Changes

In the registry under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

Registry Entry	Purpose	Nmap Abbrev
DefaultTTL	Specifies the default Time to Live (TTL) value in the header of outgoing IP packets. The TTL determines how long an IP packet that has not reached its destination can remain on the network before it is discarded.	T
Tcp1323Opts	Determines whether TCP uses the timestamping and window scaling features described in RFC 1323, TCP Extensions for High Performance	TS
EnablePMTUDiscovery	Determines whether TCP uses a fixed, default maximum transmission unit (MTU) or attempts to detect the actual MTU	No match found

Registry Entry	Purpose	Nmap Abbrev
TcpUseRFC1122Urgent Pointer	Specifies which mode TCP uses for urgent data. The two modes interpret the urgent pointer in the TCP header and the length of the urgent data differently. BSD or RFC 1122	F = U
TcpWindowSize	Determines the largest TCP receive window that the system offers. The receive window is the number of bytes a sender can transmit without receiving an acknowledgment.	W, W1-W6
SackOpts	Enables and disables the Selective Acknowledgment (SACK) feature. SACK is an optimizing feature that lets you acknowledge receipt of individual blocks of data in a continuous sequence, rather than just the last sequence number.	o = S
Interfaces*\MTU	Sets MTU is the size of the largest packet that can be transmitted over the underlying network, including the size of the transport header	o = M

(Purpose taken from Microsoft TechNet (**Microsoft, 2009**))

*Interface name

Test Environment

In setting up our test network environment, the basic structure of the test network followed the idea of defense in depth strategy in an attempt to model a notional AF network. Though virtual machines (i.e. VMware) could have been used, we chose not to do so to eliminate another variable that may have affected test results. Routers and firewalls provide layered protection (demilitarized zone-DMZ). Inside the network we configure two clients with OS obfuscation tool installed on them: Windows XP Professional SP 3 and Windows Vista SP1. In order to generate SMTP, UDP, and HTTP traffic, we configured a second network consisting of a domain controller, mail server, web server, and client.

In a traditional adversarial network scan, passive OS fingerprinting tools must be in a position to receive the packets. To accomplish this, the attacker must either entice the user to come to the attack machine or gain access to a router, switch, or firewall and work to get closer and closer to the final target. In our experiment we simulate the hacker's successful exploitation through the inside firewall and into the switch by dumping the spanned port traffic from the switch to the machines loaded with packet capture software and OS fingerprinting tools. Exploiting the routers and firewalls to gain access to the inside switch is no small feat but as stated earlier this is an ideal scenario for passive OS fingerprinting.

Figure 7 illustrates the configuration of the Windows clients, servers, and router, which simulate an AF network environment. As the attack was simulated for inside access, the firewall and IDS are not depicted in the figure. Other important information not displayed is the use of IPv4 (not IPv6), the lack of encryption on the connections (no IPSec), and no use of wireless technology. WireShark is the packet capture and analysis tool for the experiment.

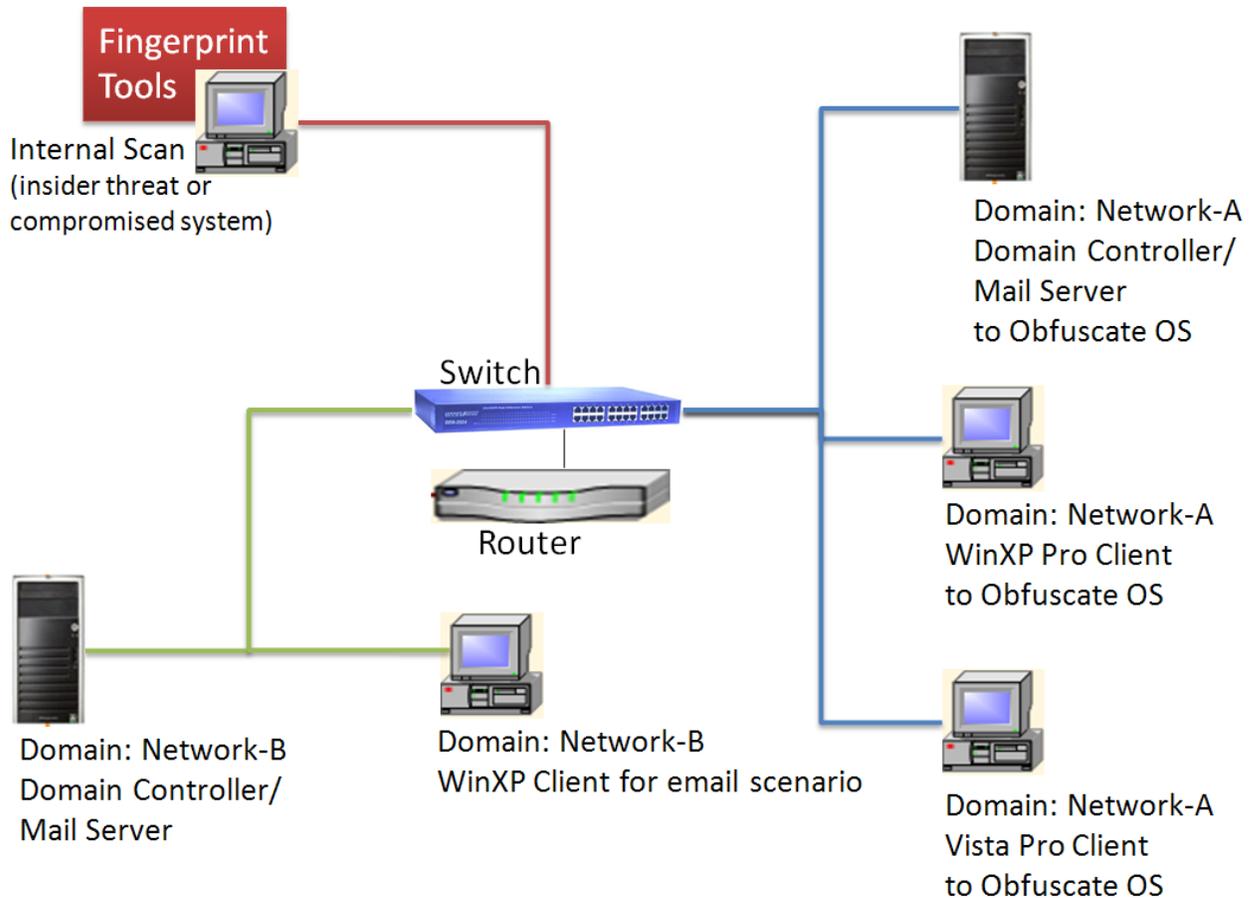


Figure 7: Test Domains

Success vs. Failure

We define a test instance as one scan against a target. In the case of our passive fingerprinting tool, one scan is the completion of the test scenario. A successful test instance means the fingerprinting tool could not correctly profile the target OS (to include inconclusive results), and a failure constitutes accurate OS identification by the fingerprinting tool. The reason an inconclusive result is considered a success is that it does not give any OS information away to the attacker. In fact, an inconclusive result is better than an incorrectly guessed OS because the attacker may attempt to run an exploit designed for the incorrect OS which could cause a system crash.

Scenario

The overall flow of the test was to first observe and collect OS fingerprinting scan results without OS obfuscation installed on any of the test machines. The next step was to observe and collect OS fingerprinting scan results with OS obfuscation running on the test machines. Since the passive and active tools use different methods to deduce the target OS, we use two different test steps to match the method. Complete the test steps first with no obfuscation on the target machines and then again after the OS on the target clients has been obfuscated. To generate traffic and create as consistent a scenario as possible, repeat the following tasks in the order is:

Table 4: Test Scenario for Passive Fingerprinting

Location	Action
On the Switch	Plug Attack Client into the span
From the attack client on Network-B	Logon on then start WireShark capture and p0f2: p0f -i 2 -o out.txt -V -N -l
From the control client on Network-B	Logon on as user1
<i>Perform the remaining steps 6 times at approximately 5 minutes separation between each start:</i>	
From the control client on Network-B	Annotate the time
	Send an email to user1@network-a.local and user2@network-a.local on the target network
From the XP client on domain Network-A	Log on as user1 and open Outlook
	Send an email to user2@network-a.local on the target network not using encryption or digital signing
	Send an email to user1@network-b.local on the control network not using encryption or digital signing
	Open the browser (IE7) and stop attempts to go to runonce Microsoft
	Navigate to www.network-b.local , click on the test link, click the back button, and close the browser
	Open the shared folder on A-DCX.Network-A.local called TestSharedFolder
	View the test.rtf file
	Close all programs and log off the system

Location	Action
From the Vista client on domain Network-A	Log on as user2 and open Outlook
	Send an email to user1@network-a.local on the target network not using encryption or digital signing
	Send an email to user1@network-b.local on the control network not using encryption or digital signing
	Open the browser (IE7) and stop attempts to go to runonce Microsoft
	Navigate to www.network-b.local , click on the test link, click the back button, and close the browser
	Open the shared folder on A-DCX.Network-A.local called TestSharedFolder
	View the test.rtf file
	Close all programs and log off the system
From the attack client on Network-B	Copy the p0f output file and add a line at the end of the output annotating completion of test scenario number (1-6)

Table 5: Test Scenario Steps for Active Fingerprinting

Location	Action
Switch	Plug the attack client into one of the VLANs
From the attack client on Network-B	Logon on and start WireShark capture
	Start an "aggressive" Nmap scan nmap -T4 -A -v -PE -PA21,23,80,3389 192.168.30.11, 192.168.30.2, 192.168.30.15
	Upon completion save the scan results
	Start a "polite" Nmap scan nmap -T2 -A -v -PE -PA21,23,80,3389 192.168.30.11, 192.168.30.2, 192.168.30.15
	Upon completion save the scan results

The next two tables list and describe the fingerprinting tool options used in the experiment. Each tool has several more options available. For the purposes of this experiment, we chose to use the Nmap default with two different timing options and a minimal option set for p0f2 that allowed for easier reading of the output.

Table 6: p0f2 Option Explanation

p0f2 Option	Explanation
-i 2	Identifies which device to listen on
-o out.txt	Specifies the output file
-V	Describe the status of all indicators in addition to the value
-N	Stops p0f2 from reporting distances and link media
-l	Outputs data in a line-per-record style

Table 7: Nmap Option Explanation

Nmap Option	Explanation
-T2	Polite (2) timing template used on slower networks or when evading an IDS by slowing down the scan
-T4	Aggressive (4) timing template
-A	This option enables additional advanced and aggressive options like OS detection (-O)
-v	Increases the verbosity level, causing Nmap to print more information about the scan in progress
-PE	ICMP echo request query to each target machine
-PA	TCP ACK packet destined for port 80
21, 23, 80, 3389	Specified ports 21 – ftp, 23 – telnet, 3389 – rdp, 80 - http

Assumptions and limitations

The placement of the packet capture tool assumes insider threat access or that an attacker has already gained access to a router, firewall, or internal system. Nmap and p0f2 employ probes that can operate through a firewall, but for testing purposes all traffic needed to be allowed to flow to the attack machine for maximum effectiveness.

The study did not incorporate wireless connections, IPv6 traffic, or IPSec to see if those concepts would work with OS obfuscation tools or to see if those concepts had any impact on the effectiveness of the OS obfuscation tool. The study also did not demonstrate OS obfuscation using smartcard authentication. Anti-virus software was not installed on any of the test machines.

IV. Test Results

OSfuscate successfully obfuscates the target OS against p0f2 and Nmap's aggressive scan, but is only partially successful against Nmap. The following tables present specific test instance results. We annotate successful fingerprinting with a check mark and a failure with an 'x'. The first table shows the fingerprinting tool results without obfuscation on the targets. The second table shows the fingerprinting tool results with obfuscation on the targets.

Table 8: Fingerprinting Results with No Obfuscation

	Server - No OSfuscate True OS:	Vista - No OSfuscate True OS:	Win XP - No OSfuscate True OS:
Nmap: Polite	MS Windows Server 2003 SP1 or SP2 (99%)	Microsoft Windows Vista SP0 or SP1, or Windows Server 2008 (99%)	Microsoft Windows XP SP2 or SP3, or Windows Server 2003 (99%)
Nmap: Aggressive	Microsoft Windows Server 2003 SP1 or SP2 (100%)	Microsoft Windows Vista SP0 or SP1, or Windows Server 2008 (100%)	Microsoft Windows XP SP2 or SP3, or Windows Server 2003 (100%)
p0f2: time elapsed 5	Windows 2000 SP4, XP SP1	- Unknown	Windows 2000 SP4, XP SP1
p0f2: time elapsed 10	Windows 2000 SP4, XP SP1	- Unknown	Windows 2000 SP4, XP SP1
p0f2: time elapsed 15	Windows 2000 SP4, XP SP1	- Unknown	Windows 2000 SP4, XP SP1
p0f2: time elapsed 20	Windows 2000 SP4, XP SP1	- Unknown	Windows 2000 SP4, XP SP1
p0f2: time elapsed 25	Windows 2000 SP4, XP SP1	- Unknown	Windows 2000 SP4, XP SP1
p0f2: time elapsed 30	Windows 2000 SP4, XP SP1	- Unknown	Windows 2000 SP4, XP SP1

Table 9: Test Results Emulating LINUX OS

	Server w/ OSfuscate	Vista w/ OSfuscate	XP w/ OSfuscate
Nmap: Polite	✓ Microsoft Windows XP SP2 (95%)	✗ Microsoft Windows Vista (95%)	✗ Microsoft Windows XP SP2 (95%)
Nmap: Aggressive	✓ No exact OS matches for host	✓ No exact OS matches for host	✓ No exact OS matches for host
p0f2: time elapsed 5 m	✓ Linux 2.0.3x (2)	- Unknown	✓ Linux 2.0.3x (2)
p0f2: time elapsed 10 m	✓ Linux 2.0.3x (2)	- Unknown	✓ Linux 2.0.3x (2)
p0f2: time elapsed 15 m	✓ Linux 2.0.3x (2)	- Unknown	✓ Linux 2.0.3x (2)
p0f2: time elapsed 20 m	✓ Linux 2.0.3x (2)	- Unknown	✓ Linux 2.0.3x (2)
p0f2: time elapsed 25 m	✓ Linux 2.0.3x (2)	- Unknown	✓ Linux 2.0.3x (2)
p0f2: time elapsed 30 m	✓ Linux 2.0.3x (2)	- Unknown	✓ Linux 2.0.3x (2)

Of interest, we observe that p0f2 did not fingerprint the Vista client with or without obfuscation enabled. As such, we don't consider the test instances using p0f2 against the Vista client as successful. We used the Windows version of p0f2 which is a version behind the UNIX version. p0f2 may have performed better if we had ran the most current version. We also note that in this experiment, Nmap's polite mode is more accurate than the aggressive mode. This finding is consistent with Nmap documentation that states though it takes less time to run an aggressive scan, some accuracy is sacrificed (Lyon, 2009). The creator of OSfuscation discloses on his web site that some of the fingerprints are better than others (Crenshaw, 2008). We speculate that OSfuscation may

perform better against Nmap if we chose one of the better fingerprints; however, a ranking of the fingerprints is not readily available.

The following sample packets captured using WireShark, show a portion of the TCP/IP packets before and after OSfuscate was applied. We highlighted the TTL values that were changed by OSfuscation.

```
Internet Protocol, Src: 192.168.30.11 (192.168.30.11), Dst: 192.168.71.2 (192.168.71.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 708
  Identification: 0x5212 (21010)
  Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 128
  Protocol: TCP (0x06)
```

Figure 8: TTL before Obfuscation

```
Internet Protocol, Src: 192.168.30.11 (192.168.30.11), Dst: 192.168.71.2 (192.168.71.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 172
  Identification: 0x2c0b (11275)
  Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 64
  Protocol: TCP (0x06)
```

Figure 9: TTL after Obfuscation

V. Discussion

Study Findings

After analyzing the literature in the area of OS obfuscation and evaluating a real-world tool, we conclude from our experiment results that current OS obfuscation tools are developed enough to consistently mask OS information on systems running a Windows OS. Also, though it is known that many AF systems are running a Windows OS, not all are. Not all AF systems need to be obfuscated. As such, OS obfuscation implementation can be restricted to critical systems or on outbound gateway traffic masking packets after they leave the internal network. This placement may deconflict OS obfuscation from blue force system management tools used to maintain the network, and could also confuse passive OS fingerprinting tools monitoring traffic on web servers. Additionally, if the AF moves to a standards-based configuration instead of the current standard desktop environment, OS obfuscation would provide even more defense. This uncertainty makes OS obfuscation a good defensive tactic. OS obfuscation is not the first line of defense but it has a significant part in network defense. However, prior to implementing OS obfuscation on AF networks, system administrator tools and processes must be considered. If OS obfuscation deceives inventory, patch monitoring and installation, and configuration verification tools, it should not be implemented until those conflicts are mitigated.

In traditional deception applications, the goal is to create a believable lie. The same is true for cydec. The obfuscation tools allow the user to choose which OS to

emulate. In deciding which OS to emulate, make sure it makes sense. An attacker isn't going to believe you have a Sega Dreamcast on an AF network!

Initial analysis indicates that creating uncertainty in the mind of the attacker as opposed to convincing the attacker that a different OS is on the target, might be the optimum approach. This deception is done by using OS obfuscation to return inconclusive results to OS fingerprinting scans. If the attacker is fooled into believing the wrong OS, the attacker will execute exploits and payloads associated with the false OS thus creating undesirable effects for the user. Whereas reducing the attacker's OS fingerprinting efforts to just a guess increases the attacker's risk of detection and mission completion. If causing inconclusive results isn't possible, it is better to constantly change the mask (make fingerprint tool return a false OS on one scan and then another false OS for a later scan) than to return a wrong but consistent OS to avoid the same problem. Further research (i.e. Attack Trees and Value Focused Thinking) needs to be completed to determine the optimum approach.

Strengths and Weaknesses of the Study

The type of traffic generated for the experiment is similar to normal network traffic; however, it is significantly less in volume. This difference in traffic volume can negatively impact the success of fingerprinting tools and mask network degradation caused by the active fingerprinting tool. Since some of the fingerprints in OSfuscation work better than others, we could run tests emulating other OSs. In the execution of this experiment we made two errors. First, due to an error experienced while saving an Nmap scan, we re-ran the test of Nmap against the targets prior to OS obfuscation after we completed all obfuscation test instances and reversed OS obfuscation on all the targets

using the “Remove All Changes” feature in OSfuscation. As we have not tested the “Remove All Changes” feature in OSfuscation, this error introduced an unexpected variable: were all the obfuscation changes reversed? Given the results generated by our fingerprinting tools, we are confident in the integrity of the study.

VI. Conclusion

Summary

Attackers scan target networks to gather system information, find vulnerabilities and fine tune attacks. The OS of a target is intelligence that supports all three goals. Denying the attacker accurate OS information can stop or impede an attacker's mission success. Attackers use OS fingerprinting tools to gain this information. Host-based OS obfuscation can defeat those tools thus denying the attacker this piece to the attack puzzle. Current OS obfuscation tools designed for Windows OS are capable of providing some OS obfuscation for AF networks, but they need to be improved and evaluated for impacts on network maintenance tools and processes, to include future initiatives like IPv6.

Future Research

Several future research topics naturally evolve from this study. We recommend a study that tests OS obfuscation effectiveness under configurations that result from possible AF initiatives: IPv6, IPSec, virtual machines (i.e. VMware), and CAC authentication. The testers would evaluate OS obfuscation under each configuration separately then in combination. We also recommend using a passive fingerprinting tool that is more effective under non-obfuscated conditions. After conducting a survey of OSs used in the AF, a good study would be to evaluate Morph on Linux systems and research on how to do OS obfuscation for other OSs.

Another recommended study is to analyze how OS obfuscation affects system administrator network tools. A possible solution and additional study may be to

implement a key that triggers the unmasking of an obfuscated packet (Birch, 2009).

Recommendations

A logical next step to accomplish is to figure out what else on the system can change to obfuscate the OS, develop a tool that makes those changes, and ensure the tool works with future AF initiatives like IPv6. Instead of making registry edits, the tool should intercept all packets leaving the system, make the necessary changes to the packet, and send the packets on. The necessary changes would be defined by the user through an interface that allows the user to choose a particular OS to emulate; to choose to constantly change what OS to emulate; to choose not to emulate an OS but to force a fingerprinting tool to return inconclusive results; or to turn off obfuscation. Upon completion of or in conjunction with the development of the improved OS obfuscation tool, we recommend integrating the use of ‘chaff’, (introducing generated spoofed packets onto the network) with existing obfuscation techniques to further confuse fingerprinting tools. This tool could be used to modify all traffic leaving a network in order to defeat passive fingerprinting tools. For example, an attacker can install p0f2 on a web server and fingerprint the OS off of the incoming traffic. Given that tricking users into clicking links to bad servers is a commonly used (and successful) attack, obfuscating the OS could hinder reconnaissance and scanning efforts. It doesn’t completely protect the targets from the attacker though. Without knowledge of the OS, the attacker may choose to load a simple OS independent call home program that once on the target, fingerprints the target host’s OS. In tandem, researchers should use Attack Trees and/or Value Focused Thinking to determine the optimum way to implement OS obfuscation:

inconclusive OS fingerprinting results vs. a consistent false OS presentation vs. a changing false OS presentation.

Another research vector would be to look for other areas to apply obfuscation to that would be effective in defeating an attacker's scanning, as well as, reconnaissance efforts. Additional cydec concepts from Repik's work would be beneficial. Specifically researchers could explore Repik's decoy and dynamic IP concepts.

Appendix A: Test Network Details

- Switch: Cisco Catalyst 2950 configure for 2 VLANs and a span port
- Router: Cisco 2600 Series configure to provide communications between the two VLANs on the switch
- DNS configuration: Default root hints deleted and replaced with an entry pointing to the opposing domain controller, forwarder added to catch all other DNS domains and send DNS queries that the DNS server cannot resolve to the opposing DNS server (in this experiment the DNS server was on the Domain Controller)
- Software load per machine:
 - Domain A XP client (192.168.30.15): Windows XP Professional Version 2002, SP3, IE7, MSOffice 2007
 - Domain A Vista client (192.168.30.11): Windows Vista Business: SP1, MSOffice 2007, IE7
 - Domain A Server (192.168.30.2): Windows Server 2003 Standard Edition: SP2, Exchange 2003 Standard Version 6.5, with active directory, application server, file server, DNS server, and DHCP server roles
 - Domain B XP client: Windows XP Professional Version 2002: SP3, IE7, MSOffice 2007
 - Domain B Server: Windows Server 2003 Standard Edition: SP2, Exchange 2003 Standard Version 6.5, with active directory, application server, file server, DNS server, and DHCP server; serves web page with picture and link to a sample text file
 - Attack machine: Windows XP Professional Version 2002, SP3, WireShark Version 1.0.7, Zenmap 4.8Beta 8 (Windows GUI front end of Nmap), p0f2 2.04

Appendix B: Fingerprinting Output Files before Obfuscation on Targets

Nmap Report with No Obfuscation on Targets – Polite mode

The screenshot displays the Nmap scan results for the target `a-dcx.network-a.local (192.168.30.2)`. The interface is organized into several expandable sections:

- Comments:** This section is currently collapsed.
- Host Status:** This section is expanded and shows the following details:
 - State: up
 - Open ports: 29
 - Filtered ports: 0
 - Closed ports: 971
 - Scanned ports: 1000
 - Up time: Not available
 - Last boot: Not available
- Addresses:** This section is expanded and shows:
 - IPv4: 192.168.30.2
 - IPv6: Not available
 - MAC: 00:15:C5:67:80:66
- Hostnames:** This section is expanded and shows:
 - Name - Type: a-dcx.network-a.local - PTR
- Operating System:** This section is expanded and shows:
 - Name: Microsoft Windows Server 2003 SP1 or SP2
 - Accuracy: 99%

Decorative icons are present: a window icon next to the Host Status section and a bomb icon next to the Operating System section.

Figure 10: Nmap Polite Scan Result for Server

vista1.network-a.local (192.168.30.11)

Comments

Host Status

State:	up	
Open ports:	10	
Filtered ports:	0	
Closed ports:	990	
Scanned ports:	1000	
Up time:	3928	
Last boot:	(null)	

Addresses

IPv4: 192.168.30.11
IPv6: Not available
MAC: 00:15:C5:63:85:25

Hostnames

Name - Type: vista1.network-a.local - PTR

Operating System

Name: Microsoft Windows Vista SP0 or SP1, or Windows Server 2008

Accuracy:  99%

Figure 11: Nmap Polite Scan Result for Vista Client

[-] xp3.network-a.local (192.168.30.15)

- [+] **Comments**
- [-] **Host Status**
 - State: up 
 - Open ports: 3
 - Filtered ports: 0
 - Closed ports: 997
 - Scanned ports: 1000
 - Up time: Not available 
 - Last boot: Not available
- [-] **Addresses**
 - IPv4: 192.168.30.15
 - IPv6: Not available
 - MAC: 00:15:C5:67:2F:B0
- [-] **Hostnames**
 - Name - Type: xp3.network-a.local - PTR
- [-] **Operating System**
 - Name: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
 - Accuracy:  99%

Figure 12: Nmap Polite Scan for XP Client

Nmap Report with No Obfuscation on Targets – Aggressive mode

a-dcx.network-a.local (192.168.30.2)

- Comments**
- Host Status**
 - State: up 
 - Open ports: 30
 - Filtered ports: 0
 - Closed ports: 970
 - Scanned ports: 1000 
 - Up time: Not available
 - Last boot: Not available
- Addresses**
 - IPv4: 192.168.30.2
 - IPv6: Not available
 - MAC: 00:15:C5:67:80:66
- Hostnames**
 - Name - Type: a-dcx.network-a.local - PTR
- Operating System**
 - Name: Microsoft Windows Server 2003 SP1 or SP2
 - Accuracy: 

Figure 13: Nmap Aggressive Scan for XP Client

[-] vista1.network-a.local (192.168.30.11)

- [+] **Comments**
- [-] **Host Status**

State:	up	
Open ports:	10	
Filtered ports:	0	
Closed ports:	990	
Scanned ports:	1000	
Up time:	1029462	
Last boot:	(null)	
- [-] **Addresses**

IPv4:	192.168.30.11
IPv6:	Not available
MAC:	00:15:C5:63:85:25
- [-] **Hostnames**

Name - Type:	vista1.network-a.local - PTR
--------------	------------------------------
- [-] **Operating System**

Name:	Microsoft Windows Vista SP0 or SP1, or Windows Server 2008
Accuracy:	<div style="border: 1px solid black; background-color: green; width: 100%; text-align: center; color: white; padding: 2px;">100%</div>

Figure 14: Nmap Aggressive Scan Results for Vista Client

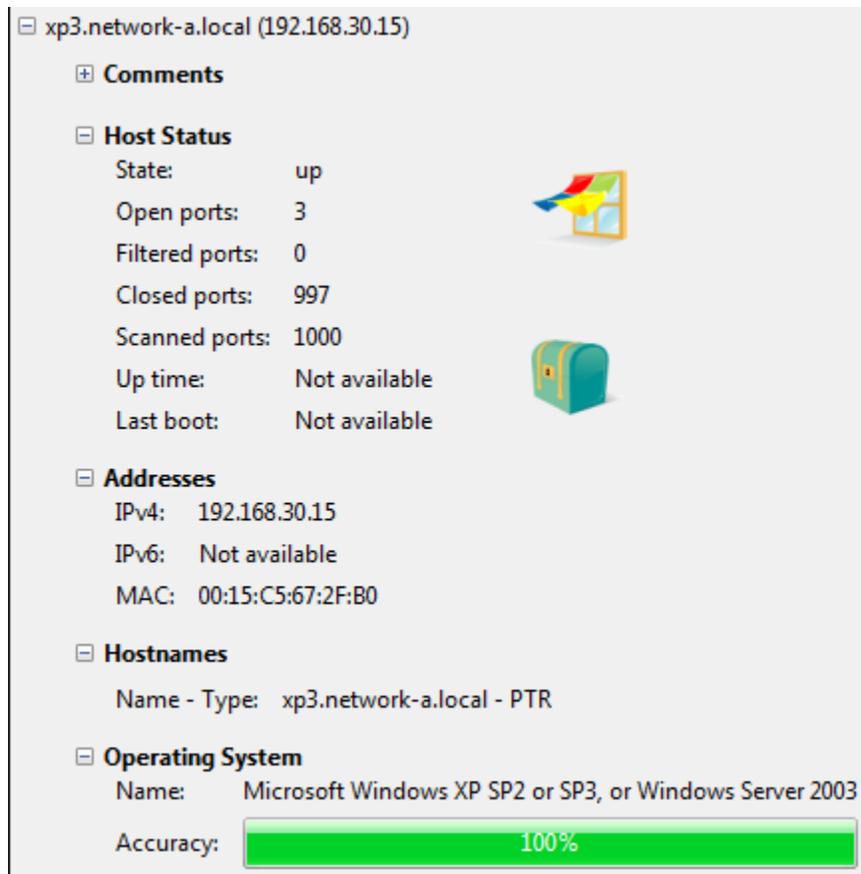


Figure 15: Nmap Scan Results for XP Client

p0f2 Output Data File with No Obfuscation on Targets

```

<Wed May 20 14:17:01 2009> 192.168.71.2:6693 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:01 2009> 192.168.71.2:6693 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:15 2009> 192.168.30.15:2924 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:15 2009> 192.168.30.15:2925 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:19 2009> 192.168.30.15:2931 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:19 2009> 192.168.30.15:2930 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:19 2009> 192.168.30.15:2932 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:19 2009> 192.168.30.15:2936 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:19 2009> 192.168.30.15:2938 - Windows 2000 SP4, XP SP1
<Wed May 20 14:17:19 2009> 192.168.30.15:2939 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:05 2009> 192.168.30.15:2942 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:05 2009> 192.168.30.15:2943 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:05 2009> 192.168.30.15:2945 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:05 2009> 192.168.30.15:2947 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:05 2009> 192.168.30.15:2948 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:05 2009> 192.168.30.15:2949 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:06 2009> 192.168.30.15:2951 - Windows 2000 SP4, XP SP1
<Wed May 20 14:18:06 2009> 192.168.30.15:2952 - Windows 2000 SP4, XP SP1
  
```


<Wed May 20 14:19:56 2009> 192.168.30.11:56154 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:19:56 2009> 192.168.30.11:56155 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:19:56 2009> 192.168.30.11:56156 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:19:56 2009> 192.168.30.11:56157 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:19:56 2009> 192.168.30.11:56158 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:19:56 2009> 192.168.30.11:56159 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:20:08 2009> 192.168.71.11:2221 - Windows 2000 SP4, XP SP1
<Wed May 20 14:20:08 2009> 192.168.71.11:2222 - Windows 2000 SP4, XP SP1
<Wed May 20 14:20:15 2009> 192.168.30.2:7900 - Windows 2000 SP4, XP SP1
<Wed May 20 14:20:15 2009> 192.168.30.2:7900 - Windows 2000 SP4, XP SP1
<Wed May 20 14:20:21 2009> 192.168.30.11:56160 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:20:21 2009> 192.168.30.11:56160 - UNKNOWN
[8192:127:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:20:38 2009> 192.168.30.11:56161 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:20:38 2009> 192.168.30.11:56162 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:04 2009> 192.168.30.11:56163 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:07 2009> 192.168.30.11:56165 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:27 2009> 192.168.30.11:56166 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:27 2009> 192.168.30.11:56167 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:27 2009> 192.168.30.11:56168 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:27 2009> 192.168.30.11:56169 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:27 2009> 192.168.30.11:56170 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:21:31 2009> 192.168.30.15:2959 - Windows 2000 SP4, XP SP1
<Wed May 20 14:21:39 2009> 192.168.30.11:56171 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:23:55 2009> 192.168.71.2:6719 - Windows 2000 SP4, XP SP1
<Wed May 20 14:23:55 2009> 192.168.71.2:6719 - Windows 2000 SP4, XP SP1
<Wed May 20 14:23:57 2009> 192.168.30.15:2961 - Windows 2000 SP4, XP SP1
<Wed May 20 14:23:57 2009> 192.168.30.15:2962 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:01 2009> 192.168.30.15:2965 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:01 2009> 192.168.30.15:2966 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:01 2009> 192.168.30.15:2967 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:01 2009> 192.168.30.15:2971 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:01 2009> 192.168.30.15:2973 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:01 2009> 192.168.30.15:2974 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:06 2009> 192.168.30.15:2977 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:06 2009> 192.168.30.15:2978 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:06 2009> 192.168.30.15:2980 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:06 2009> 192.168.30.15:2982 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:06 2009> 192.168.30.15:2983 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:06 2009> 192.168.30.15:2984 - Windows 2000 SP4, XP SP1
<Wed May 20 14:24:07 2009> 192.168.30.15:2986 - Windows 2000 SP4, XP SP1

<Wed May 20 14:30:06 2009> 192.168.30.15:3022 - Windows 2000 SP4, XP SP1
<Wed May 20 14:30:06 2009> 192.168.30.15:3023 - Windows 2000 SP4, XP SP1
<Wed May 20 14:30:06 2009> 192.168.30.15:3024 - Windows 2000 SP4, XP SP1
<Wed May 20 14:30:10 2009> 192.168.71.11:2232 - Windows 2000 SP4, XP SP1
<Wed May 20 14:30:53 2009> 192.168.30.15:3026 - Windows 2000 SP4, XP SP1
<Wed May 20 14:30:53 2009> 192.168.30.15:3026 - Windows 2000 SP4, XP SP1
<Wed May 20 14:31:10 2009> 192.168.30.15:3029 - Windows 2000 SP4, XP SP1
<Wed May 20 14:32:08 2009> 192.168.71.11:2234 - Windows 2000 SP4, XP SP1
<Wed May 20 14:32:08 2009> 192.168.71.11:2235 - Windows 2000 SP4, XP SP1
<Wed May 20 14:32:31 2009> 192.168.30.2:7961 - Windows 2000 SP4, XP SP1
<Wed May 20 14:32:31 2009> 192.168.30.2:7961 - Windows 2000 SP4, XP SP1
<Wed May 20 14:33:16 2009> 192.168.30.11:56214 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:31 2009> 192.168.30.15:3030 - Windows 2000 SP4, XP SP1
<Wed May 20 14:33:35 2009> 192.168.30.11:56215 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:35 2009> 192.168.30.11:56216 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:35 2009> 192.168.30.11:56217 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56218 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56219 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56220 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56221 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56222 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56223 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56224 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56225 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:36 2009> 192.168.30.11:56226 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:38 2009> 192.168.30.11:56227 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:38 2009> 192.168.30.11:56228 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:38 2009> 192.168.30.11:56229 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:38 2009> 192.168.30.11:56230 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:49 2009> 192.168.30.11:56231 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:49 2009> 192.168.30.11:56232 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:49 2009> 192.168.30.11:56233 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:50 2009> 192.168.30.11:56234 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:50 2009> 192.168.30.11:56235 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]
<Wed May 20 14:33:50 2009> 192.168.30.11:56236 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:??:?]

<Wed May 20 14:44:26 2009> 192.168.30.11:56332 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:26 2009> 192.168.30.11:56333 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:27 2009> 192.168.30.15:3159 - Windows 2000 SP4, XP SP1
<Wed May 20 14:44:27 2009> 192.168.30.15:3159 - Windows 2000 SP4, XP SP1
<Wed May 20 14:44:28 2009> 192.168.30.11:56334 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56335 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56336 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56337 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56338 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56339 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56340 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:28 2009> 192.168.30.11:56341 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:44:44 2009> 192.168.30.15:3161 - Windows 2000 SP4, XP SP1
<Wed May 20 14:44:44 2009> 192.168.30.15:3161 - Windows 2000 SP4, XP SP1
<Wed May 20 14:44:59 2009> 192.168.30.15:3164 - Windows 2000 SP4, XP SP1
<Wed May 20 14:45:10 2009> 192.168.71.11:2238 - Windows 2000 SP4, XP SP1
<Wed May 20 14:45:13 2009> 192.168.30.15:3165 - Windows 2000 SP4, XP SP1
<Wed May 20 14:45:32 2009> 192.168.30.15:3167 - Windows 2000 SP4, XP SP1
<Wed May 20 14:45:37 2009> 192.168.30.11:56342 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56343 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56344 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56345 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56346 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56347 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56348 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:37 2009> 192.168.30.11:56349 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:38 2009> 192.168.30.11:56350 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:38 2009> 192.168.30.11:56351 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:38 2009> 192.168.30.11:56352 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:40 2009> 192.168.30.11:56353 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:40 2009> 192.168.30.11:56354 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:40 2009> 192.168.30.11:56355 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:40 2009> 192.168.30.11:56356 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]

<Wed May 20 14:45:44 2009> 192.168.30.11:56357 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:44 2009> 192.168.30.11:56358 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:44 2009> 192.168.30.11:56359 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56360 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56361 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56362 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56363 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56364 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56365 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56366 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:45 2009> 192.168.30.11:56367 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:46 2009> 192.168.30.11:56368 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:46 2009> 192.168.30.11:56369 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:46 2009> 192.168.30.11:56370 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:46 2009> 192.168.30.11:56371 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:46 2009> 192.168.30.11:56372 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:45:46 2009> 192.168.30.11:56373 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:00 2009> 192.168.30.2:8063 - Windows 2000 SP4, XP SP1
<Wed May 20 14:46:00 2009> 192.168.30.2:8063 - Windows 2000 SP4, XP SP1
<Wed May 20 14:46:13 2009> 192.168.30.11:56374 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:13 2009> 192.168.30.11:56374 - UNKNOWN
[8192:127:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:18 2009> 192.168.30.11:56375 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:40 2009> 192.168.30.11:56376 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:40 2009> 192.168.30.11:56377 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:40 2009> 192.168.30.11:56378 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]
<Wed May 20 14:46:40 2009> 192.168.30.11:56379 - UNKNOWN
[8192:128:1:52:M1460,N,W2,N,N,S:.:?:?]

Appendix C: Fingerprinting Tool Output with Obfuscation on Targets

Nmap Output Data File with Obfuscation on Targets – Polite Mode

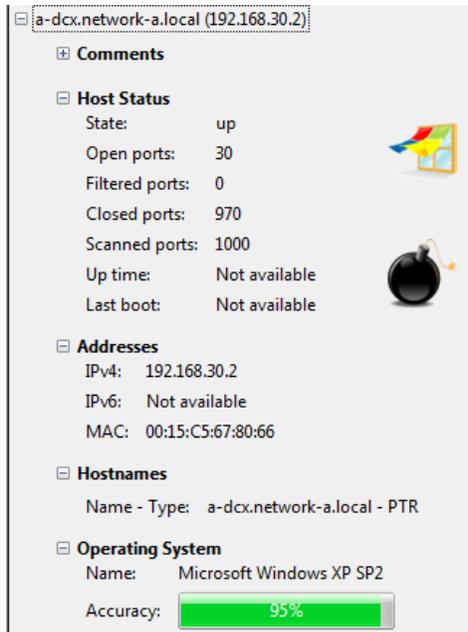


Figure 16: Nmap Polite Scan Results for Server with OSfuscation

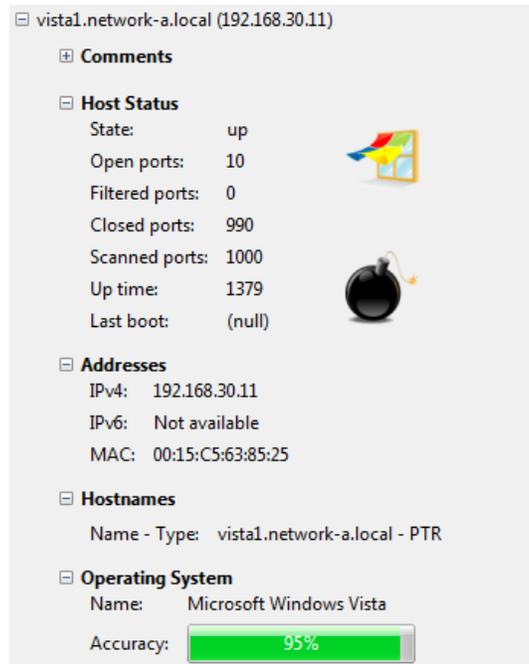


Figure 17: Nmap Polite Scan Results for Vista Client with OSfuscation

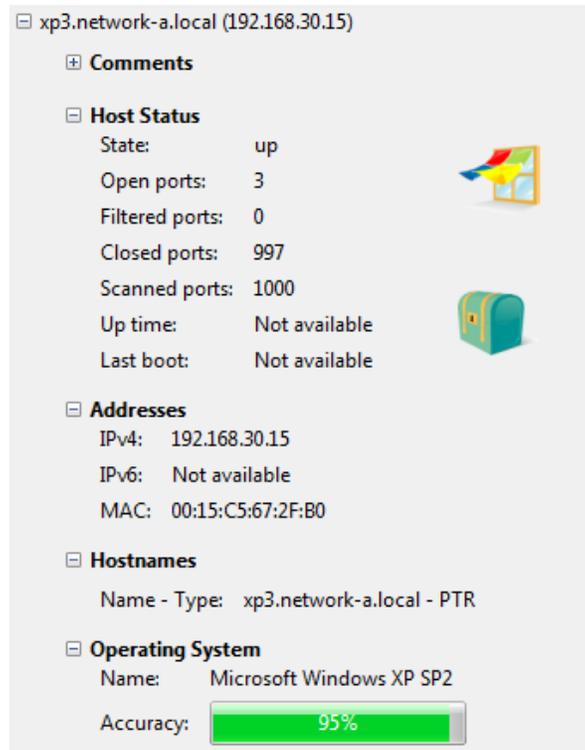


Figure 18: Nmap Polite Scan Results for XP Client with OSfuscation

Nmap Output Data File with Obfuscation on Targets – Aggressive Mode

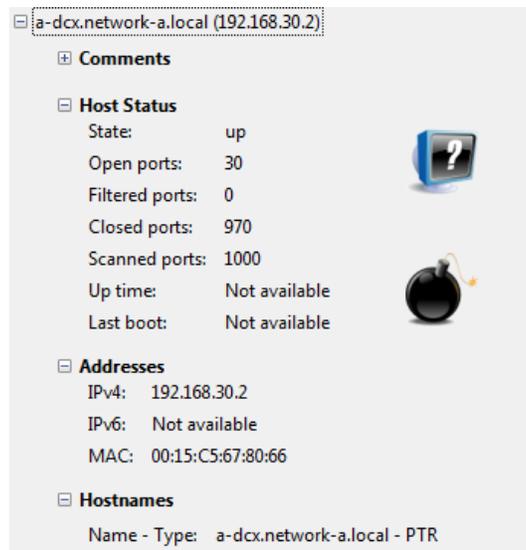


Figure 19: Nmap Aggressive Scan Results for Server with OSfuscation

MAC Address: 00:15:C5:67:80:66 (Dell)

No exact OS matches for host (If you know what OS is running on it, see [http://www.tcpipfingerprints.com](#))

```
OS:SCAN (V=4.85BETA8%D=5/20%OT=25%CT=1%CU=43125%PV=Y%DS=1%G=Y%M=0015C5%TM=4A
OS:148CB6%P=i686-pc-windows-windows) SEQ (SP=FA%GCD=1%ISR=106%TI=I%CI=I%II=I%
OS:SS=S%TS=U) SEQ (SP=FB%GCD=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=U) SEQ (SP=F9%GCD
OS:=1%ISR=106%TI=I%CI=I%II=I%SS=S%TS=U) OPS (O1=M5B4NW0%O2=M5B4NW0%O3=M5B4NW0
OS:%O4=M5B4NW0%O5=M5B4NW0%O6=M5B4) WIN (W1=4000%W2=4000%W3=4000%W4=4000%W5=40
OS:00%W6=4000) ECN (R=Y%DF=N%T=40%W=4000%O=M5B4NW0%CC=N%Q=) T1 (R=Y%DF=N%T=40%S
OS:=O%A=S+%F=AS%RD=0%Q=) T2 (R=Y%DF=N%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=) T3 (R=Y
OS:%DF=N%T=40%W=4000%S=O%A=S+%F=AS%O=M5B4NW0%RD=0%Q=) T4 (R=Y%DF=N%T=40%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=) T5 (R=Y%DF=N%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=) T6 (R
OS:=Y%DF=N%T=40%W=0%S=A%A=O%F=R%O=%RD=0%Q=) T7 (R=Y%DF=N%T=40%W=0%S=Z%A=S+F=
OS:AR%O=%RD=0%Q=) U1 (R=Y%DF=N%T=40%IPL=B0%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G) IE (R=Y%DFI=S%T=40%CD=Z)
```

Figure 20: Detailed OS Results for Nmap Aggressive Scan on Server with OSfucscation

[-] vista1.network-a.local (192.168.30.11)

- [-] **Comments**
- [-] **Host Status**
 - State: up
 - Open ports: 10
 - Filtered ports: 0
 - Closed ports: 990
 - Scanned ports: 1000
 - Up time: 2346
 - Last boot: (null)
- [-] **Addresses**
 - IPv4: 192.168.30.11
 - IPv6: Not available
 - MAC: 00:15:C5:63:85:25
- [-] **Hostnames**
 - Name - Type: vista1.network-a.local - PTR

Figure 21: Nmap Aggressive Scan Results for Vista Client with OSfucscation

MAC Address: 00:15:C5:63:85:25 (Dell)

No exact OS matches for host (If you know what OS is running on it, see <http://www.nmap.org> TCP/IP fingerprint:

```
OS:SCAN (V=4.85BETA8%D=5/20%OT=135%CT=1%CU=39512%PV=Y%DS=1%G=Y%M=0015C5%TM=4
OS:A148CB6%P=i686-pc-windows-windows) SEQ (SP=105%GCD=1%ISR=102%TI=I%CI=I%II=
OS:I%SS=S%TS=7) SEQ (SP=106%GCD=1%ISR=102%TI=I%CI=I%II=I%SS=S%TS=7) SEQ (SP=104
OS:%GCD=1%ISR=101%TI=I%CI=I%II=I%SS=S%TS=7) OPS (O1=NW8ST11%O2=NW8ST11%O3=NW8
OS:NNT11%O4=NW8ST11%O5=NW8ST11%O6=ST11) WIN (W1=2000%W2=2000%W3=2000%W4=2000%
OS:W5=2000%W6=2000) ECN (R=Y%DF=Y%T=40%W=2000%O=NW8NNS%CC=N%Q=) T1 (R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=) T2 (R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=) T3
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=) T4 (R=Y%DF=Y%T=40%W=0%S=A%A=O%
OS:F=R%O=%RD=0%Q=) T5 (R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=) T6 (R=Y%DF=Y
OS:%T=40%W=0%S=A%A=O%F=R%O=%RD=0%Q=) T7 (R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%R
OS:D=0%Q=) U1 (R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIIPCK=G%RUCK=G%RUD=G) I
OS:E (R=Y%DFI=N%T=40%CD=Z)
```

Figure 22: Detailed OS Results for Nmap Aggressive Scan on Vista Client with OSfuscation

xp3.network-a.local (192.168.30.15)

- Comments
- Host Status
 - State: up
 - Open ports: 3
 - Filtered ports: 0
 - Closed ports: 997
 - Scanned ports: 1000
 - Up time: Not available
 - Last boot: Not available
- Addresses
 - IPv4: 192.168.30.15
 - IPv6: Not available
 - MAC: 00:15:C5:67:2F:B0
- Hostnames
 - Name - Type: xp3.network-a.local - PTR

Figure 23: Nmap Aggressive Scan Results for XP Client with OSfuscation

MAC Address: 00:15:C5:67:2F:B0 (Dell)
 No exact OS matches for host (If you know what OS is running on it, see <http://www.nmap.org>)
 TCP/IP fingerprint:
 OS:SCAN(V=4.0|BETA8|D=5/20|OT=135|CT=1|CU=42862|PV=Y|DS=1|G=Y|M=0015C5|TM=4
 OS:A148CB6|P=i686-pc-windows-windows) SEQ(SP=106|GCD=1|ISR=108|TI=I|CI=I|II=
 OS:I|SS=S|TS=U) OPS(O1=M5B4NW0|O2=M5B4NW0|O3=M5B4NW0|O4=M5B4NW0|O5=M5B4NW0|O
 OS:6=M5B4) WIN(W1=4000|W2=4000|W3=4000|W4=4000|W5=4000|W6=4000) ECN(R=Y|DF=N|
 OS:T=40|W=4000|O=M5B4NW0|CC=N|Q=) T1(R=Y|DF=N|T=40|S=O|A=S+|F=AS|RD=0|Q=) T2(
 OS:R=Y|DF=N|T=40|W=0|S=Z|A=S|F=AR|O=|RD=0|Q=) T3(R=Y|DF=N|T=40|W=4000|S=O|A=
 OS:S+|F=AS|O=M5B4NW0|RD=0|Q=) T4(R=Y|DF=N|T=40|W=0|S=A|A=O|F=R|O=|RD=0|Q=) T5
 OS:(R=Y|DF=N|T=40|W=0|S=Z|A=S+|F=AR|O=|RD=0|Q=) T6(R=Y|DF=N|T=40|W=0|S=A|A=O
 OS:|F=R|O=|RD=0|Q=) T7(R=Y|DF=N|T=40|W=0|S=Z|A=S+|F=AR|O=|RD=0|Q=) U1(R=Y|DF=
 OS:N|T=40|IPL=B0|UN=0|RIPL=G|RID=G|RIPCK=G|RUCK=G|RUD=G) IE(R=Y|DFI=S|T=40|C
 OS:D=Z)

Figure 24: Detailed OS Results for Nmap Aggressive Scan on XP Client with OSfufusion

p0f2 Output Data File with Obfuscation on Targets

```
<Wed May 20 19:40:03 2009> 192.168.30.14:46839 - UNKNOWN
[2048:49:0:44:M1460:..:??]
<Wed May 20 19:40:13 2009> 192.168.30.14:46749 - UNKNOWN
[3072:42:0:44:M1460:..:??]
<Wed May 20 19:40:28 2009> 192.168.71.2:7664 - Windows 2000 SP4, XP SP1
<Wed May 20 19:40:28 2009> 192.168.71.2:7664 - Windows 2000 SP4, XP SP1
<Wed May 20 19:40:28 2009> 192.168.30.14:46751 - SunOS 4.1.x
<Wed May 20 19:40:38 2009> 192.168.30.15:1073 - Linux 2.0.3x (2)
<Wed May 20 19:40:38 2009> 192.168.30.15:1074 - Linux 2.0.3x (2)
<Wed May 20 19:40:43 2009> 192.168.30.14:46752 - SunOS 4.1.x
<Wed May 20 19:40:49 2009> 192.168.30.15:1081 - Linux 2.0.3x (2)
<Wed May 20 19:40:49 2009> 192.168.30.15:1080 - Linux 2.0.3x (2)
<Wed May 20 19:40:49 2009> 192.168.30.15:1082 - Linux 2.0.3x (2)
<Wed May 20 19:40:49 2009> 192.168.30.15:1087 - Linux 2.0.3x (2)
<Wed May 20 19:40:49 2009> 192.168.30.15:1089 - Linux 2.0.3x (2)
<Wed May 20 19:40:49 2009> 192.168.30.15:1090 - Linux 2.0.3x (2)
<Wed May 20 19:40:58 2009> 192.168.30.14:46750 - UNKNOWN
[1024:48:0:44:M1460:..:??]
<Wed May 20 19:41:11 2009> 192.168.30.15:1097 - Linux 2.0.3x (2)
<Wed May 20 19:41:11 2009> 192.168.30.15:1098 - Linux 2.0.3x (2)
<Wed May 20 19:41:11 2009> 192.168.30.15:1100 - Linux 2.0.3x (2)
<Wed May 20 19:41:11 2009> 192.168.30.15:1102 - Linux 2.0.3x (2)
<Wed May 20 19:41:11 2009> 192.168.30.15:1103 - Linux 2.0.3x (2)
<Wed May 20 19:41:12 2009> 192.168.30.15:1104 - Linux 2.0.3x (2)
<Wed May 20 19:41:13 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 19:41:17 2009> 192.168.30.15:1106 - Linux 2.0.3x (2)
<Wed May 20 19:41:17 2009> 192.168.30.15:1107 - Linux 2.0.3x (2)
<Wed May 20 19:41:17 2009> 192.168.30.15:1108 - Linux 2.0.3x (2)
<Wed May 20 19:41:28 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 19:41:36 2009> 192.168.30.2:1557 - Linux 2.0.3x (2)
<Wed May 20 19:41:36 2009> 192.168.30.2:1557 - Linux 2.0.3x (2)
```

<Wed May 20 19:41:43 2009> 192.168.30.14:46751 - UNKNOWN
[3072:50:0:44:M1460:.:?:?]
<Wed May 20 19:41:54 2009> 192.168.30.15:1111 - Linux 2.0.3x (2)
<Wed May 20 19:41:54 2009> 192.168.30.15:1111 - Linux 2.0.3x (2)
<Wed May 20 19:41:58 2009> 192.168.30.14:46752 - UNKNOWN
[3072:58:0:44:M1460:.:?:?]
<Wed May 20 19:42:13 2009> 192.168.30.14:46749 - UNKNOWN
[3072:38:0:44:M1460:.:?:?]
<Wed May 20 19:42:14 2009> 192.168.30.11:49205 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:42:28 2009> 192.168.30.14:46750 - UNKNOWN
[3072:42:0:44:M1460:.:?:?]
<Wed May 20 19:42:29 2009> 192.168.30.15:1115 - Linux 2.0.3x (2)
<Wed May 20 19:42:43 2009> 192.168.30.14:46751 - UNKNOWN
[2048:57:0:44:M1460:.:?:?]
<Wed May 20 19:42:46 2009> 192.168.30.15:1116 - Linux 2.0.3x (2)
<Wed May 20 19:42:58 2009> 192.168.30.14:46752 - UNKNOWN
[3072:38:0:44:M1460:.:?:?]
<Wed May 20 19:43:13 2009> 192.168.30.11:49206 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:13 2009> 192.168.30.11:49207 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:13 2009> 192.168.30.14:46749 - UNKNOWN
[3072:54:0:44:M1460:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49208 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49209 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49210 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49211 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49212 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49213 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49214 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49215 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49216 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:14 2009> 192.168.30.11:49217 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:16 2009> 192.168.30.11:49218 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:16 2009> 192.168.30.11:49219 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:16 2009> 192.168.30.11:49220 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:16 2009> 192.168.30.11:49221 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49222 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49223 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49224 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]

<Wed May 20 19:43:22 2009> 192.168.30.11:49225 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49226 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49227 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49228 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49229 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49230 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49231 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:22 2009> 192.168.30.11:49232 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:23 2009> 192.168.30.11:49233 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:23 2009> 192.168.30.11:49234 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:25 2009> 192.168.30.11:49235 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:25 2009> 192.168.30.11:49236 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:25 2009> 192.168.30.11:49237 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:28 2009> 192.168.30.14:46750 - UNKNOWN
[2048:49:0:44:M1460:.:?:?]
<Wed May 20 19:43:41 2009> 192.168.30.2:1568 - Linux 2.0.3x (2)
<Wed May 20 19:43:41 2009> 192.168.30.2:1568 - Linux 2.0.3x (2)
<Wed May 20 19:43:44 2009> 192.168.30.14:46749 - UNKNOWN
[1024:56:0:44:M1460:.:?:?]
<Wed May 20 19:43:45 2009> 192.168.30.11:49238 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:45 2009> 192.168.30.11:49238 - UNKNOWN
[8192:63:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:59 2009> 192.168.30.14:46750 - UNKNOWN
[2048:53:0:44:M1460:.:?:?]
<Wed May 20 19:43:59 2009> 192.168.30.11:49239 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:43:59 2009> 192.168.30.11:49240 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:44:09 2009> 192.168.71.11:2375 - Windows 2000 SP4, XP SP1
<Wed May 20 19:44:09 2009> 192.168.71.11:2376 - Windows 2000 SP4, XP SP1
<Wed May 20 19:44:14 2009> 192.168.30.14:46751 - UNKNOWN
[3072:38:0:44:M1460:.:?:?]
<Wed May 20 19:44:23 2009> 192.168.30.11:49241 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:44:24 2009> 192.168.30.11:49242 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:44:24 2009> 192.168.30.11:49243 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:44:28 2009> 192.168.30.15:1118 - Linux 2.0.3x (2)
<Wed May 20 19:44:28 2009> 192.168.30.15:1119 - Linux 2.0.3x (2)
<Wed May 20 19:44:29 2009> 192.168.30.14:46752 - UNKNOWN
[1024:40:0:44:M1460:.:?:?]
<Wed May 20 19:44:32 2009> 192.168.30.11:49244 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]

```

<Wed May 20 19:44:44 2009> 192.168.30.14:46840 - UNKNOWN
[2048:49:0:44:M1460:..:??]
<Wed May 20 19:44:54 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 19:45:09 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 19:45:10 2009> 192.168.71.11:2377 - Windows 2000 SP4, XP SP1
<Wed May 20 19:45:24 2009> 192.168.30.14:46751 - UNKNOWN
[3072:54:0:44:M1460:..:??]
<Wed May 20 19:45:39 2009> 192.168.30.14:46752 - UNKNOWN
[2048:45:0:44:M1460:..:??]
<Wed May 20 19:45:54 2009> 192.168.30.14:46840 - UNKNOWN
[2048:49:0:44:M1460:..:??]
<Wed May 20 19:46:04 2009> 192.168.30.14:46749 - UNKNOWN
[3072:50:0:44:M1460:..:??]
<Wed May 20 19:46:05 2009> 192.168.71.2:7685 - Windows 2000 SP4, XP SP1
<Wed May 20 19:46:05 2009> 192.168.71.2:7685 - Windows 2000 SP4, XP SP1
<Wed May 20 19:46:08 2009> 192.168.30.15:1120 - Linux 2.0.3x (2)
<Wed May 20 19:46:08 2009> 192.168.30.15:1121 - Linux 2.0.3x (2)
<Wed May 20 19:46:16 2009> 192.168.30.15:1124 - Linux 2.0.3x (2)
<Wed May 20 19:46:16 2009> 192.168.30.15:1125 - Linux 2.0.3x (2)
<Wed May 20 19:46:17 2009> 192.168.30.15:1126 - Linux 2.0.3x (2)
<Wed May 20 19:46:17 2009> 192.168.30.15:1130 - Linux 2.0.3x (2)
<Wed May 20 19:46:17 2009> 192.168.30.15:1132 - Linux 2.0.3x (2)
<Wed May 20 19:46:17 2009> 192.168.30.15:1133 - Linux 2.0.3x (2)
<Wed May 20 19:46:19 2009> 192.168.30.14:46839 - UNKNOWN
[3072:50:0:44:M1460:..:??]
<Wed May 20 19:46:22 2009> 192.168.30.15:1136 - Linux 2.0.3x (2)
<Wed May 20 19:46:22 2009> 192.168.30.15:1137 - Linux 2.0.3x (2)
<Wed May 20 19:46:22 2009> 192.168.30.15:1139 - Linux 2.0.3x (2)
<Wed May 20 19:46:22 2009> 192.168.30.15:1141 - Linux 2.0.3x (2)
<Wed May 20 19:46:22 2009> 192.168.30.15:1142 - Linux 2.0.3x (2)
<Wed May 20 19:46:22 2009> 192.168.30.15:1143 - Linux 2.0.3x (2)
<Wed May 20 19:46:23 2009> 192.168.30.15:1145 - Linux 2.0.3x (2)
<Wed May 20 19:46:23 2009> 192.168.30.15:1146 - Linux 2.0.3x (2)
<Wed May 20 19:46:23 2009> 192.168.30.15:1147 - Linux 2.0.3x (2)
<Wed May 20 19:46:29 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 19:46:44 2009> 192.168.30.14:46750 - UNKNOWN
[3072:50:0:44:M1460:..:??]
<Wed May 20 19:46:52 2009> 192.168.30.2:1588 - Linux 2.0.3x (2)
<Wed May 20 19:46:52 2009> 192.168.30.2:1588 - Linux 2.0.3x (2)
<Wed May 20 19:46:59 2009> 192.168.30.14:46751 - UNKNOWN
[2048:49:0:44:M1460:..:??]
<Wed May 20 19:46:59 2009> 192.168.30.15:1149 - Linux 2.0.3x (2)
<Wed May 20 19:46:59 2009> 192.168.30.15:1149 - Linux 2.0.3x (2)
<Wed May 20 19:47:14 2009> 192.168.30.14:46752 - UNKNOWN
[2048:45:0:44:M1460:..:??]
<Wed May 20 19:47:25 2009> 192.168.30.15:1152 - Linux 2.0.3x (2)
<Wed May 20 19:47:29 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 19:47:37 2009> 192.168.30.15:1153 - Linux 2.0.3x (2)
<Wed May 20 19:47:42 2009> 192.168.30.11:49245 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:47:42 2009> 192.168.30.11:49246 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:47:42 2009> 192.168.30.11:49247 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:47:43 2009> 192.168.30.11:49248 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:47:43 2009> 192.168.30.11:49249 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]

```

<Wed May 20 19:47:43 2009> 192.168.30.11:49250 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:43 2009> 192.168.30.11:49251 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:43 2009> 192.168.30.11:49252 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:43 2009> 192.168.30.11:49253 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:43 2009> 192.168.30.11:49254 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:43 2009> 192.168.30.11:49255 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:44 2009> 192.168.30.14:46749 - UNKNOWN
[3072:50:0:44:M1460:.:?:?]
<Wed May 20 19:47:45 2009> 192.168.30.11:49256 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:45 2009> 192.168.30.11:49257 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:45 2009> 192.168.30.11:49258 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:45 2009> 192.168.30.11:49259 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49260 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49261 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49262 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49263 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49264 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49265 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:49 2009> 192.168.30.11:49266 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:50 2009> 192.168.30.11:49267 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:50 2009> 192.168.30.11:49268 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:50 2009> 192.168.30.11:49269 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:50 2009> 192.168.30.11:49270 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:50 2009> 192.168.30.11:49271 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:50 2009> 192.168.30.11:49272 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:51 2009> 192.168.30.11:49273 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:51 2009> 192.168.30.11:49274 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:51 2009> 192.168.30.11:49275 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:47:59 2009> 192.168.30.14:46750 - UNKNOWN
[2048:41:0:44:M1460:.:?:?]
<Wed May 20 19:48:07 2009> 192.168.30.2:1595 - Linux 2.0.3x (2)
<Wed May 20 19:48:07 2009> 192.168.30.2:1595 - Linux 2.0.3x (2)

```

<Wed May 20 19:48:11 2009> 192.168.30.11:49276 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:11 2009> 192.168.30.11:49276 - UNKNOWN
[8192:63:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:14 2009> 192.168.30.14:46751 - UNKNOWN
[3072:58:0:44:M1460:.:??:?]
<Wed May 20 19:48:29 2009> 192.168.30.14:46752 - SunOS 4.1.x
<Wed May 20 19:48:37 2009> 192.168.30.11:49277 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:39 2009> 192.168.30.11:49278 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:39 2009> 192.168.30.11:49279 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:39 2009> 192.168.30.11:49280 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:39 2009> 192.168.30.11:49281 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:48:44 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 19:48:59 2009> 192.168.30.14:46750 - UNKNOWN
[1024:40:0:44:M1460:.:??:?]
<Wed May 20 19:49:14 2009> 192.168.30.14:46749 - UNKNOWN
[1024:52:0:44:M1460:.:??:?]
<Wed May 20 19:49:29 2009> 192.168.30.14:46750 - UNKNOWN
[2048:49:0:44:M1460:.:??:?]
<Wed May 20 19:49:44 2009> 192.168.30.14:46751 - SunOS 4.1.x
<Wed May 20 19:49:59 2009> 192.168.30.14:46752 - UNKNOWN
[1024:52:0:44:M1460:.:??:?]
<Wed May 20 19:50:14 2009> 192.168.30.14:46749 - UNKNOWN
[2048:57:0:44:M1460:.:??:?]
<Wed May 20 19:50:27 2009> 192.168.71.2:7707 - Windows 2000 SP4, XP SP1
<Wed May 20 19:50:27 2009> 192.168.71.2:7707 - Windows 2000 SP4, XP SP1
<Wed May 20 19:50:29 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 19:50:40 2009> 192.168.30.15:1157 - Linux 2.0.3x (2)
<Wed May 20 19:50:41 2009> 192.168.30.15:1159 - Linux 2.0.3x (2)
<Wed May 20 19:50:41 2009> 192.168.30.15:1160 - Linux 2.0.3x (2)
<Wed May 20 19:50:41 2009> 192.168.30.15:1164 - Linux 2.0.3x (2)
<Wed May 20 19:50:41 2009> 192.168.30.15:1166 - Linux 2.0.3x (2)
<Wed May 20 19:50:41 2009> 192.168.30.15:1167 - Linux 2.0.3x (2)
<Wed May 20 19:50:44 2009> 192.168.30.14:46751 - UNKNOWN
[2048:37:0:44:M1460:.:??:?]
<Wed May 20 19:50:53 2009> 192.168.30.15:1170 - Linux 2.0.3x (2)
<Wed May 20 19:50:53 2009> 192.168.30.15:1171 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1173 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1175 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1176 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1177 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1179 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1180 - Linux 2.0.3x (2)
<Wed May 20 19:50:54 2009> 192.168.30.15:1181 - Linux 2.0.3x (2)
<Wed May 20 19:50:59 2009> 192.168.30.14:46752 - UNKNOWN
[1024:40:0:44:M1460:.:??:?]
<Wed May 20 19:51:09 2009> 192.168.30.2:1610 - Linux 2.0.3x (2)
<Wed May 20 19:51:09 2009> 192.168.30.2:1610 - Linux 2.0.3x (2)
<Wed May 20 19:51:14 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 19:51:18 2009> 192.168.30.15:1183 - Linux 2.0.3x (2)
<Wed May 20 19:51:18 2009> 192.168.30.15:1183 - Linux 2.0.3x (2)
<Wed May 20 19:51:28 2009> 192.168.30.11:49282 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]

```

<Wed May 20 19:51:29 2009> 192.168.30.14:46750 - UNKNOWN
[2048:37:0:44:M1460:.:?:?]
<Wed May 20 19:51:38 2009> 192.168.30.15:1186 - Linux 2.0.3x (2)
<Wed May 20 19:51:44 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 19:51:51 2009> 192.168.30.15:1187 - Linux 2.0.3x (2)
<Wed May 20 19:51:56 2009> 192.168.30.11:49283 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49284 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49285 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49286 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49287 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49288 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49289 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49290 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49291 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49292 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49293 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:56 2009> 192.168.30.11:49294 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:58 2009> 192.168.30.11:49295 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:58 2009> 192.168.30.11:49296 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:58 2009> 192.168.30.11:49297 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:58 2009> 192.168.30.11:49298 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:51:59 2009> 192.168.30.14:46750 - UNKNOWN
[1024:44:0:44:M1460:.:?:?]
<Wed May 20 19:52:01 2009> 192.168.30.11:49299 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:01 2009> 192.168.30.11:49300 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:01 2009> 192.168.30.11:49301 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:02 2009> 192.168.30.11:49302 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:02 2009> 192.168.30.11:49303 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:02 2009> 192.168.30.11:49304 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:02 2009> 192.168.30.11:49305 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:02 2009> 192.168.30.11:49306 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:02 2009> 192.168.30.11:49307 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]

```

<Wed May 20 19:52:02 2009> 192.168.30.11:49308 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:03 2009> 192.168.30.11:49309 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:03 2009> 192.168.30.11:49310 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:03 2009> 192.168.30.11:49311 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:03 2009> 192.168.30.11:49312 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:03 2009> 192.168.30.11:49313 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:03 2009> 192.168.30.11:49314 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:14 2009> 192.168.30.14:46841 - UNKNOWN
[1024:48:0:44:M1460:.:?:?]
<Wed May 20 19:52:23 2009> 192.168.30.2:1616 - Linux 2.0.3x (2)
<Wed May 20 19:52:23 2009> 192.168.30.2:1616 - Linux 2.0.3x (2)
<Wed May 20 19:52:25 2009> 192.168.30.14:46749 - UNKNOWN
[3072:50:0:44:M1460:.:?:?]
<Wed May 20 19:52:30 2009> 192.168.30.11:49315 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:30 2009> 192.168.30.11:49315 - UNKNOWN
[8192:63:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:40 2009> 192.168.30.14:46751 - UNKNOWN
[3072:54:0:44:M1460:.:?:?]
<Wed May 20 19:52:48 2009> 192.168.30.11:49316 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:55 2009> 192.168.30.14:46752 - UNKNOWN
[2048:41:0:44:M1460:.:?:?]
<Wed May 20 19:52:57 2009> 192.168.30.11:49317 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:57 2009> 192.168.30.11:49318 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:58 2009> 192.168.30.11:49319 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:52:58 2009> 192.168.30.11:49320 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:53:10 2009> 192.168.30.14:46750 - UNKNOWN
[3072:46:0:44:M1460:.:?:?]
<Wed May 20 19:53:25 2009> 192.168.30.14:46841 - SunOS 4.1.x
<Wed May 20 19:53:35 2009> 192.168.30.14:46749 - UNKNOWN
[1024:56:0:44:M1460:.:?:?]
<Wed May 20 19:53:50 2009> 192.168.30.14:46751 - UNKNOWN
[2048:53:0:44:M1460:.:?:?]
<Wed May 20 19:54:05 2009> 192.168.30.14:46752 - UNKNOWN
[3072:38:0:44:M1460:.:?:?]
<Wed May 20 19:54:20 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 19:54:35 2009> 192.168.30.14:46749 - UNKNOWN
[1024:44:0:44:M1460:.:?:?]
<Wed May 20 19:54:44 2009> 192.168.30.15:1189 - Linux 2.0.3x (2)
<Wed May 20 19:54:50 2009> 192.168.30.14:46750 - UNKNOWN
[1024:52:0:44:M1460:.:?:?]
<Wed May 20 19:55:02 2009> 192.168.30.15:1191 - Linux 2.0.3x (2)
<Wed May 20 19:55:02 2009> 192.168.30.15:1192 - Linux 2.0.3x (2)
<Wed May 20 19:55:05 2009> 192.168.30.14:46751 - UNKNOWN
[1024:56:0:44:M1460:.:?:?]

```

```

<Wed May 20 19:55:20 2009> 192.168.30.14:46752 - UNKNOWN
[2048:57:0:44:M1460:..:??]
<Wed May 20 19:55:35 2009> 192.168.30.14:46749 - UNKNOWN
[3072:42:0:44:M1460:..:??]
<Wed May 20 19:55:50 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 19:56:05 2009> 192.168.30.14:46751 - UNKNOWN
[1024:56:0:44:M1460:..:??]
<Wed May 20 19:56:09 2009> 192.168.71.11:2379 - Windows 2000 SP4, XP SP1
<Wed May 20 19:56:09 2009> 192.168.71.11:2380 - Windows 2000 SP4, XP SP1
<Wed May 20 19:56:20 2009> 192.168.30.14:46752 - UNKNOWN
[2048:37:0:44:M1460:..:??]
<Wed May 20 19:56:22 2009> 192.168.71.2:7731 - Windows 2000 SP4, XP SP1
<Wed May 20 19:56:22 2009> 192.168.71.2:7731 - Windows 2000 SP4, XP SP1
<Wed May 20 19:56:26 2009> 192.168.30.15:1196 - Linux 2.0.3x (2)
<Wed May 20 19:56:26 2009> 192.168.30.15:1195 - Linux 2.0.3x (2)
<Wed May 20 19:56:26 2009> 192.168.30.15:1197 - Linux 2.0.3x (2)
<Wed May 20 19:56:26 2009> 192.168.30.15:1198 - Linux 2.0.3x (2)
<Wed May 20 19:56:26 2009> 192.168.30.15:1202 - Linux 2.0.3x (2)
<Wed May 20 19:56:26 2009> 192.168.30.15:1204 - Linux 2.0.3x (2)
<Wed May 20 19:56:26 2009> 192.168.30.15:1205 - Linux 2.0.3x (2)
<Wed May 20 19:56:28 2009> 192.168.30.15:1208 - Linux 2.0.3x (2)
<Wed May 20 19:56:31 2009> 192.168.30.15:1209 - Linux 2.0.3x (2)
<Wed May 20 19:56:31 2009> 192.168.30.15:1210 - Linux 2.0.3x (2)
<Wed May 20 19:56:31 2009> 192.168.30.15:1212 - Linux 2.0.3x (2)
<Wed May 20 19:56:31 2009> 192.168.30.15:1214 - Linux 2.0.3x (2)
<Wed May 20 19:56:31 2009> 192.168.30.15:1215 - Linux 2.0.3x (2)
<Wed May 20 19:56:32 2009> 192.168.30.15:1216 - Linux 2.0.3x (2)
<Wed May 20 19:56:32 2009> 192.168.30.15:1218 - Linux 2.0.3x (2)
<Wed May 20 19:56:32 2009> 192.168.30.15:1219 - Linux 2.0.3x (2)
<Wed May 20 19:56:32 2009> 192.168.30.15:1220 - Linux 2.0.3x (2)
<Wed May 20 19:56:35 2009> 192.168.30.14:46749 - UNKNOWN
[3072:46:0:44:M1460:..:??]
<Wed May 20 19:56:45 2009> 192.168.30.2:1645 - Linux 2.0.3x (2)
<Wed May 20 19:56:45 2009> 192.168.30.2:1645 - Linux 2.0.3x (2)
<Wed May 20 19:56:50 2009> 192.168.30.14:46750 - UNKNOWN
[1024:56:0:44:M1460:..:??]
<Wed May 20 19:56:51 2009> 192.168.30.15:1222 - Linux 2.0.3x (2)
<Wed May 20 19:56:51 2009> 192.168.30.15:1222 - Linux 2.0.3x (2)
<Wed May 20 19:57:05 2009> 192.168.30.14:46749 - UNKNOWN
[3072:46:0:44:M1460:..:??]
<Wed May 20 19:57:07 2009> 192.168.30.15:1225 - Linux 2.0.3x (2)
<Wed May 20 19:57:14 2009> 192.168.30.11:49321 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:57:20 2009> 192.168.30.14:46750 - UNKNOWN
[3072:42:0:44:M1460:..:??]
<Wed May 20 19:57:21 2009> 192.168.30.15:1226 - Linux 2.0.3x (2)
<Wed May 20 19:57:25 2009> 192.168.30.11:49322 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:57:25 2009> 192.168.30.11:49323 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:57:25 2009> 192.168.30.11:49324 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:57:26 2009> 192.168.30.11:49325 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:57:26 2009> 192.168.30.11:49326 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 19:57:26 2009> 192.168.30.11:49327 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]

```

<Wed May 20 19:57:26 2009> 192.168.30.11:49328 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:26 2009> 192.168.30.11:49329 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:26 2009> 192.168.30.11:49330 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:26 2009> 192.168.30.11:49331 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:26 2009> 192.168.30.11:49332 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:26 2009> 192.168.30.11:49333 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:28 2009> 192.168.30.11:49334 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:28 2009> 192.168.30.11:49335 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:28 2009> 192.168.30.11:49336 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:28 2009> 192.168.30.11:49337 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49338 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49339 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49340 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49341 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49342 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49343 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:32 2009> 192.168.30.11:49344 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:33 2009> 192.168.30.11:49345 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:33 2009> 192.168.30.11:49346 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:33 2009> 192.168.30.11:49347 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:33 2009> 192.168.30.11:49348 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:33 2009> 192.168.30.11:49349 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:33 2009> 192.168.30.11:49350 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:34 2009> 192.168.30.11:49351 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:34 2009> 192.168.30.11:49352 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:34 2009> 192.168.30.11:49353 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 19:57:35 2009> 192.168.30.14:46751 - UNKNOWN
[3072:50:0:44:M1460:.:?:?]
<Wed May 20 19:57:50 2009> 192.168.30.14:46752 - UNKNOWN
[2048:45:0:44:M1460:.:?:?]
<Wed May 20 19:57:53 2009> 192.168.30.2:1654 - Linux 2.0.3x (2)
<Wed May 20 19:57:53 2009> 192.168.30.2:1654 - Linux 2.0.3x (2)

```

<Wed May 20 19:57:57 2009> 192.168.30.11:49354 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:57:57 2009> 192.168.30.11:49354 - UNKNOWN
[8192:63:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:58:05 2009> 192.168.30.14:46842 - UNKNOWN
[2048:53:0:44:M1460:.:??:?]
<Wed May 20 19:58:15 2009> 192.168.30.14:46749 - UNKNOWN
[2048:41:0:44:M1460:.:??:?]
<Wed May 20 19:58:16 2009> 192.168.30.11:49355 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:58:28 2009> 192.168.30.11:49356 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:58:28 2009> 192.168.30.11:49357 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:58:28 2009> 192.168.30.11:49358 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:58:28 2009> 192.168.30.11:49359 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:58:30 2009> 192.168.30.14:46750 - UNKNOWN
[1024:40:0:44:M1460:.:??:?]
<Wed May 20 19:58:45 2009> 192.168.30.14:46751 - UNKNOWN
[3072:38:0:44:M1460:.:??:?]
<Wed May 20 19:58:52 2009> 192.168.30.11:49360 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 19:59:00 2009> 192.168.30.14:46752 - UNKNOWN
[2048:49:0:44:M1460:.:??:?]
<Wed May 20 19:59:15 2009> 192.168.30.14:46842 - UNKNOWN
[2048:49:0:44:M1460:.:??:?]
<Wed May 20 19:59:26 2009> 192.168.30.14:46749 - UNKNOWN
[3072:46:0:44:M1460:.:??:?]
<Wed May 20 19:59:41 2009> 192.168.30.14:46840 - UNKNOWN
[1024:40:0:44:M1460:.:??:?]
<Wed May 20 19:59:51 2009> 192.168.30.14:46749 - UNKNOWN
[2048:41:0:44:M1460:.:??:?]
<Wed May 20 20:00:06 2009> 192.168.30.14:46750 - UNKNOWN
[3072:54:0:44:M1460:.:??:?]
<Wed May 20 20:00:10 2009> 192.168.71.11:2381 - Windows 2000 SP4, XP SP1
<Wed May 20 20:00:21 2009> 192.168.30.14:46751 - UNKNOWN
[2048:57:0:44:M1460:.:??:?]
<Wed May 20 20:00:29 2009> 192.168.71.2:7744 - Windows 2000 SP4, XP SP1
<Wed May 20 20:00:29 2009> 192.168.71.2:7744 - Windows 2000 SP4, XP SP1
<Wed May 20 20:00:33 2009> 192.168.30.15:1228 - Linux 2.0.3x (2)
<Wed May 20 20:00:33 2009> 192.168.30.15:1229 - Linux 2.0.3x (2)
<Wed May 20 20:00:36 2009> 192.168.30.14:46752 - UNKNOWN
[3072:46:0:44:M1460:.:??:?]
<Wed May 20 20:00:38 2009> 192.168.30.15:1232 - Linux 2.0.3x (2)
<Wed May 20 20:00:38 2009> 192.168.30.15:1233 - Linux 2.0.3x (2)
<Wed May 20 20:00:39 2009> 192.168.30.15:1234 - Linux 2.0.3x (2)
<Wed May 20 20:00:39 2009> 192.168.30.15:1238 - Linux 2.0.3x (2)
<Wed May 20 20:00:39 2009> 192.168.30.15:1240 - Linux 2.0.3x (2)
<Wed May 20 20:00:39 2009> 192.168.30.15:1241 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1244 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1245 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1247 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1249 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1250 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1251 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1253 - Linux 2.0.3x (2)

```

<Wed May 20 20:00:45 2009> 192.168.30.15:1254 - Linux 2.0.3x (2)
<Wed May 20 20:00:45 2009> 192.168.30.15:1255 - Linux 2.0.3x (2)
<Wed May 20 20:00:51 2009> 192.168.30.14:46750 - UNKNOWN
[3072:42:0:44:M1460:..:??]
<Wed May 20 20:01:04 2009> 192.168.30.2:1671 - Linux 2.0.3x (2)
<Wed May 20 20:01:04 2009> 192.168.30.2:1671 - Linux 2.0.3x (2)
<Wed May 20 20:01:06 2009> 192.168.30.14:46749 - UNKNOWN
[1024:40:0:44:M1460:..:??]
<Wed May 20 20:01:13 2009> 192.168.30.15:1257 - Linux 2.0.3x (2)
<Wed May 20 20:01:13 2009> 192.168.30.15:1257 - Linux 2.0.3x (2)
<Wed May 20 20:01:14 2009> 192.168.71.11:2384 - Windows 2000 SP4, XP SP1
<Wed May 20 20:01:14 2009> 192.168.71.11:2385 - Windows 2000 SP4, XP SP1
<Wed May 20 20:01:14 2009> 192.168.71.11:2387 - Windows 2000 SP4, XP SP1
<Wed May 20 20:01:14 2009> 192.168.71.11:2388 - Windows 2000 SP4, XP SP1
<Wed May 20 20:01:14 2009> 192.168.71.11:2389 - Windows 2000 SP4, XP SP1
<Wed May 20 20:01:14 2009> 192.168.71.11:2390 - Windows 2000 SP4, XP SP1
<Wed May 20 20:01:21 2009> 192.168.30.14:46750 - UNKNOWN
[1024:40:0:44:M1460:..:??]
<Wed May 20 20:01:29 2009> 192.168.30.15:1260 - Linux 2.0.3x (2)
<Wed May 20 20:01:36 2009> 192.168.30.14:46751 - UNKNOWN
[3072:42:0:44:M1460:..:??]
<Wed May 20 20:01:42 2009> 192.168.30.15:1261 - Linux 2.0.3x (2)
<Wed May 20 20:01:47 2009> 192.168.30.11:49361 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49362 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49363 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49364 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49365 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49366 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49367 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49368 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49369 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49370 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:47 2009> 192.168.30.11:49371 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:49 2009> 192.168.30.11:49372 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:49 2009> 192.168.30.11:49373 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:49 2009> 192.168.30.11:49374 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:49 2009> 192.168.30.11:49375 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:51 2009> 192.168.30.14:46752 - UNKNOWN
[2048:53:0:44:M1460:..:??]
<Wed May 20 20:01:57 2009> 192.168.30.11:49376 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:01:57 2009> 192.168.30.11:49377 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]

```

<Wed May 20 20:01:57 2009> 192.168.30.11:49378 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49379 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49380 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49381 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49382 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49383 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49384 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:57 2009> 192.168.30.11:49385 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:58 2009> 192.168.30.11:49386 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:58 2009> 192.168.30.11:49387 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:58 2009> 192.168.30.11:49388 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:58 2009> 192.168.30.11:49389 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:58 2009> 192.168.30.11:49390 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:01:58 2009> 192.168.30.11:49391 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:02:06 2009> 192.168.30.14:46749 - UNKNOWN
[2048:57:0:44:M1460:.:?:?]
<Wed May 20 20:02:21 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 20:02:29 2009> 192.168.30.11:49392 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:02:29 2009> 192.168.30.2:1683 - Linux 2.0.3x (2)
<Wed May 20 20:02:29 2009> 192.168.30.2:1683 - Linux 2.0.3x (2)
<Wed May 20 20:02:36 2009> 192.168.30.11:49393 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:02:36 2009> 192.168.30.11:49393 - UNKNOWN
[8192:63:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:02:36 2009> 192.168.30.14:46749 - UNKNOWN
[3072:50:0:44:M1460:.:?:?]
<Wed May 20 20:02:51 2009> 192.168.30.14:46750 - SunOS 4.1.x
<Wed May 20 20:02:58 2009> 192.168.30.11:49394 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:03:01 2009> 192.168.30.11:49395 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:03:01 2009> 192.168.30.11:49396 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:03:01 2009> 192.168.30.11:49397 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:03:06 2009> 192.168.30.14:46751 - SunOS 4.1.x
<Wed May 20 20:03:11 2009> 192.168.30.11:49398 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:?:?]
<Wed May 20 20:03:21 2009> 192.168.30.14:46752 - SunOS 4.1.x
<Wed May 20 20:03:36 2009> 192.168.30.14:46749 - UNKNOWN
[3072:46:0:44:M1460:.:?:?]
<Wed May 20 20:03:51 2009> 192.168.30.14:46750 - SunOS 4.1.x

```

```

<Wed May 20 20:04:06 2009> 192.168.30.14:46751 - UNKNOWN
[1024:56:0:44:M1460:..:??]
<Wed May 20 20:04:21 2009> 192.168.30.14:46752 - SunOS 4.1.x
<Wed May 20 20:04:36 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 20:04:51 2009> 192.168.30.14:46750 - UNKNOWN
[1024:52:0:44:M1460:..:??]
<Wed May 20 20:05:06 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 20:05:21 2009> 192.168.30.14:46750 - UNKNOWN
[2048:53:0:44:M1460:..:??]
<Wed May 20 20:05:24 2009> 192.168.71.2:7765 - Windows 2000 SP4, XP SP1
<Wed May 20 20:05:24 2009> 192.168.71.2:7765 - Windows 2000 SP4, XP SP1
<Wed May 20 20:05:30 2009> 192.168.30.15:1265 - Linux 2.0.3x (2)
<Wed May 20 20:05:30 2009> 192.168.30.15:1266 - Linux 2.0.3x (2)
<Wed May 20 20:05:30 2009> 192.168.30.15:1267 - Linux 2.0.3x (2)
<Wed May 20 20:05:30 2009> 192.168.30.15:1268 - Linux 2.0.3x (2)
<Wed May 20 20:05:30 2009> 192.168.30.15:1272 - Linux 2.0.3x (2)
<Wed May 20 20:05:30 2009> 192.168.30.15:1274 - Linux 2.0.3x (2)
<Wed May 20 20:05:31 2009> 192.168.30.15:1275 - Linux 2.0.3x (2)
<Wed May 20 20:05:36 2009> 192.168.30.14:46843 - UNKNOWN
[1024:52:0:44:M1460:..:??]
<Wed May 20 20:05:36 2009> 192.168.30.15:1278 - Linux 2.0.3x (2)
<Wed May 20 20:05:36 2009> 192.168.30.15:1279 - Linux 2.0.3x (2)
<Wed May 20 20:05:36 2009> 192.168.30.15:1281 - Linux 2.0.3x (2)
<Wed May 20 20:05:36 2009> 192.168.30.15:1283 - Linux 2.0.3x (2)
<Wed May 20 20:05:36 2009> 192.168.30.15:1284 - Linux 2.0.3x (2)
<Wed May 20 20:05:37 2009> 192.168.30.15:1285 - Linux 2.0.3x (2)
<Wed May 20 20:05:37 2009> 192.168.30.15:1287 - Linux 2.0.3x (2)
<Wed May 20 20:05:37 2009> 192.168.30.15:1288 - Linux 2.0.3x (2)
<Wed May 20 20:05:37 2009> 192.168.30.15:1289 - Linux 2.0.3x (2)
<Wed May 20 20:05:46 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 20:06:00 2009> 192.168.30.2:1702 - Linux 2.0.3x (2)
<Wed May 20 20:06:00 2009> 192.168.30.2:1702 - Linux 2.0.3x (2)
<Wed May 20 20:06:01 2009> 192.168.30.14:46751 - SunOS 4.1.x
<Wed May 20 20:06:09 2009> 192.168.30.15:1291 - Linux 2.0.3x (2)
<Wed May 20 20:06:09 2009> 192.168.30.15:1291 - Linux 2.0.3x (2)
<Wed May 20 20:06:16 2009> 192.168.30.14:46752 - UNKNOWN
[3072:46:0:44:M1460:..:??]
<Wed May 20 20:06:25 2009> 192.168.30.15:1294 - Linux 2.0.3x (2)
<Wed May 20 20:06:31 2009> 192.168.30.14:46750 - UNKNOWN
[3072:42:0:44:M1460:..:??]
<Wed May 20 20:06:37 2009> 192.168.30.15:1295 - Linux 2.0.3x (2)
<Wed May 20 20:06:42 2009> 192.168.30.11:49399 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:42 2009> 192.168.30.11:49400 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:42 2009> 192.168.30.11:49401 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:43 2009> 192.168.30.11:49402 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:43 2009> 192.168.30.11:49403 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:43 2009> 192.168.30.11:49404 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:43 2009> 192.168.30.11:49405 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]
<Wed May 20 20:06:43 2009> 192.168.30.11:49406 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:..:??]

```

<Wed May 20 20:06:43 2009> 192.168.30.11:49407 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:43 2009> 192.168.30.11:49408 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:43 2009> 192.168.30.11:49409 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:43 2009> 192.168.30.11:49410 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:45 2009> 192.168.30.11:49411 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:45 2009> 192.168.30.11:49412 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:45 2009> 192.168.30.11:49413 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:45 2009> 192.168.30.11:49414 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:46 2009> 192.168.30.14:46843 - UNKNOWN
[3072:42:0:44:M1460:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49415 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49416 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49417 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49418 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49419 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49420 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:48 2009> 192.168.30.11:49421 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:49 2009> 192.168.30.11:49422 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:49 2009> 192.168.30.11:49423 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:49 2009> 192.168.30.11:49424 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:50 2009> 192.168.30.11:49425 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:50 2009> 192.168.30.11:49426 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:50 2009> 192.168.30.11:49427 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:50 2009> 192.168.30.11:49428 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:50 2009> 192.168.30.11:49429 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:50 2009> 192.168.30.11:49430 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:06:56 2009> 192.168.30.14:46749 - SunOS 4.1.x
<Wed May 20 20:07:11 2009> 192.168.30.2:1715 - Linux 2.0.3x (2)
<Wed May 20 20:07:11 2009> 192.168.30.2:1715 - Linux 2.0.3x (2)
<Wed May 20 20:07:11 2009> 192.168.30.14:46751 - UNKNOWN
[2048:45:0:44:M1460:.:??:?]
<Wed May 20 20:07:20 2009> 192.168.30.11:49431 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]

<Wed May 20 20:07:20 2009> 192.168.30.11:49431 - UNKNOWN
[8192:63:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:26 2009> 192.168.30.14:46752 - SunOS 4.1.x
<Wed May 20 20:07:30 2009> 192.168.30.11:49432 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:41 2009> 192.168.30.14:46750 - UNKNOWN
[3072:42:0:44:M1460:.:??:?]
<Wed May 20 20:07:47 2009> 192.168.30.11:49433 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:47 2009> 192.168.30.11:49434 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:47 2009> 192.168.30.11:49435 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:47 2009> 192.168.30.11:49436 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:56 2009> 192.168.30.11:49437 - UNKNOWN
[8192:64:1:48:N,W2,N,N,S:.:??:?]
<Wed May 20 20:07:57 2009> 192.168.30.14:46749 - SunOS 4.1.x

Bibliography

1. Berrueta, D. B. (2003, March 11). *A practical approach for defeating Nmap OS-Fingerprinting*. Retrieved March 12, 2009, from Help Net Security: <http://www.net-security.org/article.php?id=406>
2. Birch, S. (2009, February 24). Basic OS Obfuscation. (S. Murphy, Interviewer)
3. Crenshaw, A. (2008). *OSfuscate: Change your Windows OS TCP/IP Fingerprint to confuse P0f, NetworkMiner, Ettercap, Nmap and other OS detection tools*. Retrieved Mar 12, 2009, from Irongeek.com: <http://www.irongeek.com/i.php?page=security/osfuscate-change-your-windows-os-tcp-ip-fingerprint-to-confuse-p0f-networkminer-ettercap-nmap-and-other-os-detection-tools>
4. Hernan, S., Lambert, S., Ostwald, T., & Shostack, A. (2006, November). *Uncover Security Design Flaws Using The STRIDE Approach*. Retrieved May 09, 2009, from MSDN Magazine: <http://msdn.microsoft.com/en-us/magazine/cc163519.aspx>
5. Hoover, J. N. (2009, April 22). *Pentagon Creating Cyber Warfare Command*. Retrieved May 02, 2009, from InformationWeek: <http://www.informationweek.com/news/government/technology/showArticle.jhtml?articleID=217000202&pgno=1&queryText=&isPrev=>
6. Joint Task Force Global Network Operations. (2009, February 17). *JTF-GNO Unclass Threat Brief*. Retrieved April 23, 2009, from Joint Task Force Global Network Operations: https://www.jtfgno.mil/JTF-GNO_Unclass_Threat_Brief.ppt
7. Lacey, T. (2009, April 04). (S. Murphy, Interviewer)
8. Levine, A. (2009, April 7). *Official: Millions spent defending Pentagon computers from attack*. Retrieved April 25, 2009, from CNN Politics.com: <http://www.cnn.com/2009/POLITICS/04/07/military.computers/>
9. Lyon, G. (2009, January 1). *Chapter 1. Getting Started with Nmap*. Retrieved March 15, 2009, from Insecure.org: <http://nmap.org/book/intro.html#id497837>
10. Lyon, G. (2009, January 1). *Chapter 8: Remote OS Detection*. Retrieved April 3, 2009, from Insecure.org: <http://nmap.org/book/osdetect.html#id389729>
11. Lyon, G. (2006). *Top 2 OS Detection Tools*. Retrieved Jun 19, 2009, from Insecure.Org: <http://sectools.org/os-detectors.html>
12. Lyons, G. (2009, January 1). *Chapter 14. Understanding and Customizing Nmap Data Files*. Retrieved May 08, 2009, from Insecure.org: <http://nmap.org/book/nmap-os-db.html>
13. Lyons, G. (1998, October 18). *Remote OS detection via TCP/IP Stack FingerPrinting*. Retrieved May 10, 2009, from Insecure.org: <http://nmap.org/nmap-fingerprinting-article.txt>
14. Lyons, G. (n.d.). *TCP/IP Fingerprinting Methods Supported by Nmap*. Retrieved March 19, 2009, from INSECURE.ORG: <http://nmap.org/book/osdetect-methods.html>
15. Microsoft. (2009). *Registry Entry Name*. Retrieved May 17, 2009, from Microsoft TechNet: <http://technet.microsoft.com/en-us/library/>

16. Miles, D. (2009, April 22). *Secretary Gates presses to boost network security*. Retrieved April 23, 2009, from Air Force Link:
<http://www.af.mil/news/story.asp?storyID=123145616>
17. Repik, K. M. (2008). *Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques*. Air Force Institute of Technology.
18. Scambray, J., McClure, S., & Kurtz, G. (2001). *Hacking Exposed: Network Security Secrets and Solutions*. Berkeley: McGraw-Hill.
19. Skoudis, E., & Liston, T. (2006). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Upper Saddle River: Prentice Hall.
20. Smart, M., Malan, G. R., & Jahanian, F. (2000, Aug 14). *Defeating TCP/IP Stack Fingerprinting*. Retrieved April 23, 2009, from USENIX:
http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/smart/smart_html/
21. Swiderski, F., & Snyder, W. (2004). *Threat Modeling*. Redmond: Microsoft Press.
22. Wang, K. (2003, July 30). *Frustrating OS Fingerprinting with Morph*. Retrieved February 26, 2009, from Synacklabs:
<http://www.synacklabs.net/projects/morph/Wang-Morph-DEFCON12.pdf>
23. Washington Post. (2009, Feb 10). *Obama Asks for Review of Online Security*. Retrieved Feb 10, 2009, from Early Bird:
<http://ebird.osd.mil/ebfiles/e20090210656066.html>
24. Wolfram Mathematica. (2009). Retrieved May 20, 2009, from Wolfram Alpha Computational Knowledge Engine:
<http://www61.wolframalpha.com/input/?i=obfuscation>
25. Yuill, J., Denning, D., & Feer, F. (2006). Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques. *Journal of Information Warfare* , 26-40.
26. Zalewski, M. (2006). *p0f 2: Dr. Jekyll had something to Hyde*. Retrieved May 04, 2009, from The "SfR Fresh" Software Archive: <http://www.sfr-fresh.com/unix/privat/p0f-2.0.8.tgz:a/p0f/doc/README>
27. Zalewski, M. (2006, September 6). *the new p0f: 2.0.8*. Retrieved April 10, 2009, from p0f2: <http://lcamtuf.coredump.cx/p0f.shtml>

Vita

Major Sherry Murphy entered the Air Force through the Air Force Reserve Officer Training Corps program at Fayetteville State University in Fayetteville, North Carolina and was commissioned May 1995. Her academic degrees include a B.S. in Mathematics and an M.S. in Computer Information Systems.

Maj Murphy has served in operational and staff positions in a communications squadron and at agency, joint, and center levels. Her duties have included database administration and security; satellite terminal maintenance; telephony, computer and network systems support; communications mission area expert in the ops center; and software development. She was selected to attend AFIT in 2008 and is currently completing the Cyber Warfare Intermediate Developmental Education program. Upon graduation she will be assigned to Air Force Space Command.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 06-09-2009		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From – To) May 2008 – June 2009	
4. TITLE AND SUBTITLE DECEIVING ADVERSARY NETWORK SCANNING EFFORTS USING HOST-BASED DECEPTION				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Sherry B. Murphy, Maj, USAF				5d. PROJECT NUMBER 08-296	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/ICW/ENG/09-04	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) 8 th Air Force / Air Force Cyber (P) Attn: Brian T. Spink 245 Davis Avenue Barksdale AFB LA 71110-2279				10. SPONSOR/MONITOR'S ACRONYM(S) 8AF/AFCYBER	
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
13. SUPPLEMENTARY NOTES					
14. ABSTRACT In this research we demonstrate the usefulness of manipulating system traffic to deceive an attacker's operating system (OS) fingerprinting as part of their network scanning efforts. Specifically, we address whether host-based OS obfuscation has merit and application as an integral part of Air Force network defense and whether the technique warrants further research and application development. We accomplish this objective through a literature review and a proof of concept evaluation of a selected OS obfuscation tool against selected OS fingerprinting tools under current Air Force network configuration. Our focus areas in the literature review include: how to characterize the scanning phase of an adversary attack, a survey of current OS fingerprinting and obfuscation tools, and description of current AF network concepts. To evaluate effectiveness of a candidate OS tool, we setup an experimental network environment that simulates adversarial network scanning. The results of our study are: a) that current OS obfuscation tools designed for Windows OS are capable of providing some OS obfuscation on AF networks; b) that the current tools need to be evaluated for impacts on network maintenance tools and processes, to include future initiatives like IPv6; and c) that the current tools need to improve OS fingerprints and add options to force inconclusive results from fingerprinting tools.					
15. SUBJECT TERMS Operating System Masking, Polymorphic Host-based Defense, Digital Decoys, Deception, Network Reconnaissance, Network Scanning					
16. SECURITY CLASSIFICATION OF:		17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 87	19a. NAME OF RESPONSIBLE PERSON LtCol Jeffrey McDonald, PhD (ENG)	
REPORT U	ABSTRACT U			c. THIS PAGE U	19b. TELEPHONE NUMBER (Include area code) (937) 255-3636, ext 4639; e-mail: jmcdonal@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18