OISSG

FIST Conference 2004, Amsterdam

Ethical Hacking

Balwant Rathore, CISSP
Founder Open Information System Security Group
www.oissg.org

 www.oissg.org

OISSG

Agenda !

- **Information Gathering**
  - Network Surveying Scanning
  - Other Information Sources
  - Security Infrastructure Discovery
  - War-dialing
- **Scanning and Network Mapping**
- **Vulnerability Identification**
- **Penetration (Fun with exploits)**

www.oissg.org

OISSG

Objective

- **From an Attacker's Perspective**
  - Penetrate Company X Applications
  - Bypass the authentication and Security Mechanisms
  - Take Advantages of weak Security and Misconfiguration
  - Identify and Exploit "Vulnerabilities"

www.oissg.org

This course is not designed to tell that how the attacks are performed, but to create the effective defense from the attacks, it is essential to understand.

This document deals with the Common Web Application Vulnerabilities, which are Categorized in ten domains.

Objective

- **From Security Professional's Perspective**
  - Identify all the Vulnerabilities
  - Strengthen Default Configurations
  - Prepare for the Unexpected
  - Understand the Methodologies Employed by the Attacker
  - Implement the appropriate against the Attacks

OISSG

Information Gathering

- Network Surveying Scanning
- Other Information Sources
- Security Infrastructure Discovery
- Wardialing

WHOIS Enumeration
- -Organizational Query
- -Domain Query
- -Server Query
- -Network Query
- -POC Query
- -BGP Query
- -Safeguards

DNS Interrogation
- -Zone transfer with nslookup
- -Safeguards

OISSG

Whois Enumeration

Provides information - registered with whois servers

- Domain Information
- Organization Information
- Server Information
- Network Information
- BGP Information
- POC Information

www.oissg.org

Domain Names and the information that who owns the particular IP can be obtained using ARIN and WHOIS

OISSG Domain Information/Query

Domain Query to get all the information related to the domain: name, registrant, address, phone no., email etc.

- **Whois** target.com@rs.internic.net
- **Whois** target.com@whois-server.com

 www.oissg.org

Domain Query allows users to gather the information about Registrant, Domain Names, Contact Information, Domain Name Servers etc. To query the WHOIS domain database the knowledge of whois server is must.

OISSG Organisation Information/Query

- "name target"@networksolutions.com
- "name target"@whois.arin.net

For Example: The WHOIS organizational query can be used to refine the search like
"name Indian u." @networksolutions.com
"name Indian university. "@networksolutions.com
"name Indian university
department."@networksolutions.com
"name Indian university professor.
"@networksolutions.com

 www.oissg.org

Organizational Query allows generating the possible domain names. Sam Spade allows WHOIS Organizational Query. Following is the example of pattern matching:

"name Indian u."

"name Indian university."

"name Indian university department."

"name Indian university professor."

OISSG Server Information/Query

To determine the list of domains for a server:

- **Whois** “host IP-addr”@whois-server.com
- **Whois** “server dns-handle”@whois-server.com

 www.oissg.org

Server Query allows obtaining a list of Domains for which a particular DNS Server is authoritative.

In order to get the domain names using the WHOIS Server query the valid DNS Server IP Address is required.

OISSG Network Information/Query

- Provides the information related to the network i.e. whether the real network is associated with the DNS or not etc.
- Nslookup can also be used for the Whois Query

To determine the network IP block range:

Whois ipaddress@whois.arin.net

 www.oissg.org

Network Query allows determining whether a real network is associated with the target domain. It is also useful to determine the block of IP Addresses owned by the organization.

Nslookup and other tools can also be used in conjunction.

OISSG POC Information/Query

Provides the information related to user and mails etc

- **Whois** “handle name”@whois.networksolutions.com
- **Whois** “mail@target.com”@whois.networksolutions.com

 www.oissg.org

POC Query allows determining the additional information from POC fields.

Additional information like user and mails etc can be obtained by the POC Query.

To gather the information about the user/mail use following command Whois “mail@target.com” @whois.networksolutions.com

OISSG

BGP Information/Query

• Allows to determining the ASN number and it may also provide the additional addresses/networks

• **Whois** "ASN target"@twhois.arin.net

www.oissg.org

WHOIS BGP Query (Border Gateway Protocol) allows determining the ASN number and it may also provide the additional addresses/networks.

OISSG Whois Enumeration - Safeguards

- Limit the whois contact information fields.
- Use non-associated company account for domain registration.
- Apply Password or PGP authentication to change the whois information

 www.oissg.org

Following are the safeguards against the Whois Enumeration:

• Do not provide each and every information in the whois database, just limit the information, so as nobody can misuse that.

• Do not use the company account for the registration of Domain

• Always use the authentication mechanism to change/modify the information related to the Whois database.

OISSG

Information Gathering

- Network Surveying Scanning
- Other Information Sources
- Security Infrastructure Discovery
- Wardialing

WHOIS Enumeration
- -Organizational Query
- -Domain Query
- -Server Query
- -Network Query
- -POC Query
- -BGP Query
- -Safeguards

DNS Interrogation
- -Zone transfer with nslookup
- -Safeguards

www.oissg.org

OISSG

DNS Interrogation

DNS database provides the information mapping between the IP address and hostnames. Following are the methods used for the purpose.

- Zone transfer with nslookup
- Safeguards

www.oissg.org

DNS database provides the information mapping between the IP address and hostnames. Zone transfer is used to synchronize primary and secondary name servers.

OISSG DNS Interrogation-Zone Transfer

Using Zone Transfer primary and secondary name servers can be obtained

• Following are the commands for Zone Transfer:

Nslookup
server <ipaddresses>
set type=any
ls –d <target.com>

 www.oissg.org

The zone is a sub tree of the DNS that is administered separately. A common zone is a second-level domain, "ac.il" for example. Thus a lot of second-level domains divide their zone into smaller zones.

Whenever a new system is installed in a zone, the DNS administrator for the zone allocates a name and an IP address for the new system and enters these into the name server's database. A name server is said to have authority forone zone or multiple zones. Often, server software executes on a dedicated processor, and this computing machine is called the name Server.

OISSG DNS Interrogation-Safeguards

- Zone transfer should be allowed to the authorized servers only.
- Use allow-transfer directive for the specific zone transfer.
- Deny all unauthorised inbound connections to TCP Port 53.
- External name servers should not allow leakage of internal information

 www.oissg.org

General Safeguards against the DNS Interrogation which are self explanatory.

OISSG

Information Gathering

- Network Surveying Scanning
- ⇨ Other Information Sources
- Security Infrastructure Discovery
- Wardialing

OISSG Other Information Sources

- Search board and newsgroup postings for server trails back to the target network.
- Examine target web page source code and scripts for application servers and internal links.
- Examine e-mail headers, bounced mails, and read receipts for the server trails.
- Search newsgroups for posted information from the target.
- Search job databases and newspapers for IT positions within the organization relating to hardware and software.
- Doc Grinding (Electronic and physical) like News, Trade and Business journals

 www.oissg.org

Search for the publicly available information to get the clear understanding about the organisation and the organisation structure.

Publicly available information like information available in Newspapers, job databases, email headers etc.

OISSG Other Information Sources

• Company Web-Site: The Company web-site may be very useful for obtaining the information about the company / organisation. Other than the main web pages can also be helpful in obtaining the information.

• Following are the interests:
  • News, Technologies & Current Events: Latest News related to the company/organisation, technologies and the current events could be helpful to gain more and more information.
  • Names and E-mails: Company/Organisation web-site could be one of the best ways to get the information about the Names of employees, vendors and/or the clients. Simultaneously the e-mails can also be obtained.

 www.oissg.org

Company WebSite itself is the useful way to gather the information about the organisation. The interested area are to get information like Name, Emails, Company News, Current Events, Technologies etc. To gather all these information the company WebSite itself is the best way.

OISSG Other Information Sources

• Source Sifting
Use Offline Browsers: After downloading the web pages, it might be worthwhile to mirror them using the browsers to get the related information. Wget (Command Line for UNIX) are the utilities for the same.
• Tools Used: HTTrack, Wget etc…
• Business Information Sites: Publicly available information sites that are providing the business information can be helpful in gathering the information structure of the organization, subsidiary information etc.

 www.oissg.org

Publicly available information sites that are providing the business information can be helpful in gathering the information structure of the organization, subsidiary information etc.

OISSG Other Information Sources

• Financial Research: These can also be used to gather the information about the organisation structure etc. Following are the examples (Sites) which helps to obtain the information about the organisation.
  • Security Exchange Commission web site
  • Yahoo Finance

• Google:
Best way to gather information. Advance Search helps to search within domain, specific type of file.
www.AllTheWeb.com

 www.oissg.org

Financial Research is the most important and most useful way to get the information about the organisation and the structure. There are various sites which helps in determining the information related to the finance.

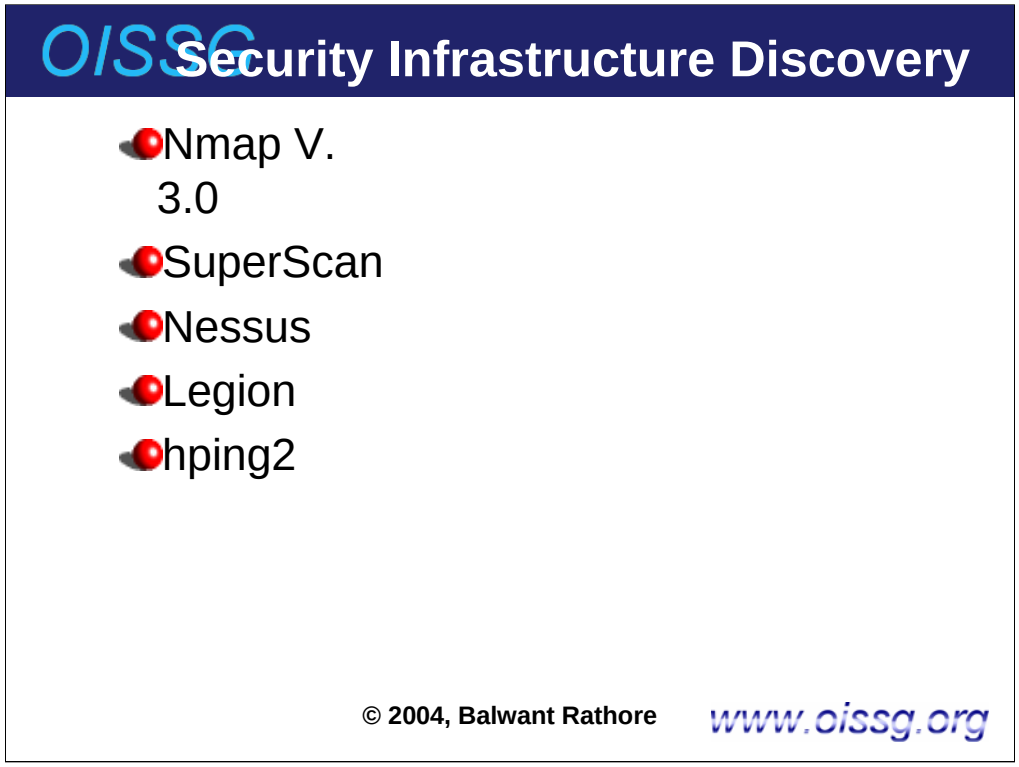
Searching the information using the Search Engines like Google Etc.

Using the advance search options information can be gathered.

OISSG

Information Gathering

- Purpose of the course
- Network Surveying Scanning
- Other Information Sources
- ⇨ Security Infrastructure Discovery
- Wardialing



Tools for the scanning purpose.

OISSG Security Infrastructure Discovery

Nmap V. 3.0

- Available for Linux, Windows, Open/Free/Net BSD, Solaris, IRIX, Mac OS X, HP-UX, Sun OS
- Written by Fyodor and available at:
  - http://www.insecure.org/nmap
- It does three things:
  - Determine hosts are alive or not
  - Determine which services are listening
  - Determine OS type

 www.oissg.org

Nmap is the full featured tool for the scanning of the network, services and guessing the Operating System.

Nmap is very popular tool since it supports nearly all the platforms (OS).

OISSG Security Infrastructure Discovery

- Allows for conducting numerous types of scans:
  - "Vanilla" TCP scans
    - Use 3-way handshake
    - Slow and easily detectable
  - SYN scan (aka "half-open" scan)
    - only do initial SYN and look for SYN|ACK (open)

      or RST (closed)
    - Never send ACK back
    - Fast and Harder to detect and never

Security Infrastructure Discovery

- ACK scans
  - Stealthy and bypass packet filters
- FIN (-sF), NULL (-sN) and XMAS (-sX)
  - All similar coz they all rely on RFC-compliance.
  - Don’t work against boxes like Win95/98/NT or IRIX.
  - They all can be combined.
  - They splits the packet into two tiny fragments which can sometimes get through firewalls and avoid detection.

Security Infrastructure Discovery

- UDP Scanning
- FTP Proxy “Bounce Attack” Scanning
- RPC Scanning

  -sR/-I RPC/Identd scan (use with other scan types)
- TCP Sequence prediction test

- My best way to scan (Decoy + Spoof)
  - Use as a block of decoy IPs as you can and In between a spoof IP
  - Sniff Spoof IP

OISSG

Security Infrastructure Discovery

Scanning with Nmap

- Options

  (not required, most can be combined)

  - * -O Use TCP/IP fingerprinting to guess remote operating system
  - -p <range> ports to scan.

    Example range: '1-1024,1080,6666,31337'

www.oissg.org

Using the various options as stated above Operating system can be guessed.

Also the Ports within given range can be scanned for the vulnerabilities.

Security Infrastructure Discovery

- Options…
  - F Only scans ports listed in nmap-services
  - v Verbose. Recommended.
  - P0 Don't ping hosts
  - * -Ddecoy_host1,decoy2[,...] Hide scan using many decoys

 www.oissg.org

Nmap also allows to scan the ports which are listed in the Nmap services, without pinging the hosts and allows the hiding scan using many decoys.

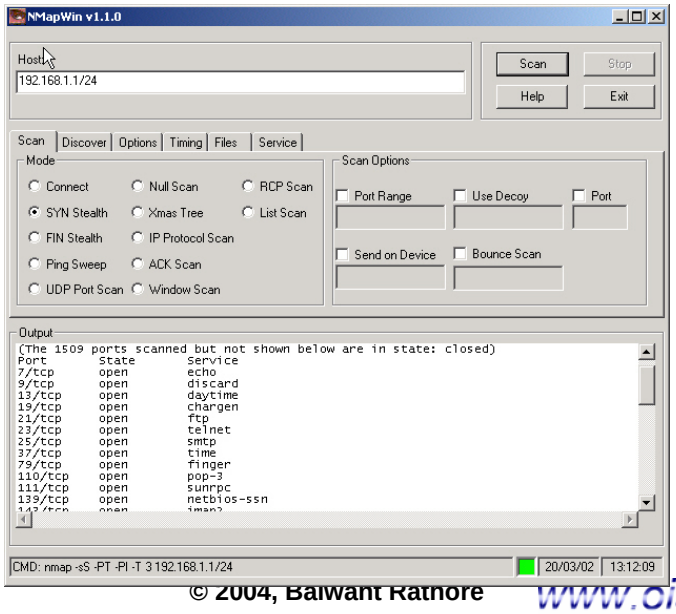
OISSG Security Infrastructure Discovery

- Options…
  - -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  - oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  - iL <inputfile> Get targets from file;
  - -S <your_IP>/-e <devicename> Specify source address or network interface

 www.oissg.org

Options used with NMap

OISSG Security Infrastructure Discovery



Nmap for windows platform

Ideal Host Scanning

- Choose Ideal Host
  - by analyzing ID field, if the ID field value changes frequently, host is experiencing some sort of Traffic.
  - Low Traffic
  - Any device with TCP/IP stack including workstation, printer, router etc

Security Infrastructure Discovery

- Options…
  - -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  - oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  - iL <inputfile> Get targets from file;
  - -S <your_IP>/-e <devicename> Specify source address or network interface

OISSG Public Information Gathering

- Purpose of the course
- Network Surveying Scanning
- Other Information Sources
- Security Infrastructure Discovery
- ⇨ Wardialing
  - Perform Scan with THC-Scan
  - Perform Scan with Toneloc
  - Safeguards - WarDialing

OISSG

WarDialing - Toneloc

- Scans for the followings:
  - It can also detects Carrier and Tone modes
  - Run the command from command shell

    toneloc 1234-XXXX /M: /R:

    Where 1234-XXXX represents the number ranges to be dialed.

    /M - is to use number from mask file.

    /R - is to specify a particular range to dial
  - When detects a tone for modem, PBX etc. plays sound
  - Very fast dialing capabilities - up to 180 lines per hour

 www.oissg.org

Toneloc is one of the best WarDialers available, which allow users to change the configuration. It is basically a command line dialer and alerts the user by playing sounds when it detects the tone or carrier signals. It can dial numbers randomly as well as sequentially.

OISSG

WarDialing - THC Scan

- Scans for the followings:
  - It can detects Carrier and Tone modes
  - It Can dial sequential as well as the Random Numbers
  - Best Option to detect and hack the PBX's
  - Supports the scripting language for hacking
  - can scan 100-125 lines per hour

 www.oissg.org

THC-Scan is available at: http://thc.inferno.tusculum.edu

Features of THC-Scan:

- Supports multiple instances of THC-Scan
- Random waits can be inserted between the calls/dials
- Rudimentary jamming detection-System stops working if it reaches a particular maximum number of busy calls.

OISSG

WarDialing-Safeguards

- Activating the scanning detection functionality of the PBX can be helpful in detecting attack.
- Conduct war dialing exercise against the own network

 www.oissg.org

WarDialing can be very harmful for an organisation, as it could be used detect the tone and carrier signals, also can be used to hack the PBX.

To avoid the WarDialing harms, install the appropriate safeguards:

• Always activate the system, which detects the WarDialialing attacks.

The detection is usually possible if someone is dialing the numbers sequentially.

• Perform the Scanning exercise against the own network, to find out the vulnerability, if exists and install the proper safeguards.

?

OISSG

Scanning and Network Mapping

www.oissg.org

OISSG

Mapping the Victim

- Which machines are alive?
- What applications are running?
- Which version of OS is running?

www.oissg.org

What the attacker needs to know to be successful in his goals ?

-commonly used tools to check the above is Nmap & Nessus. Nessus has more options.

OISSG Which Machines Are Alive?

- ICMP ping sweep
  - Sends ICMP_echo_request packets
  - Scans a whole network address range
  - Tools include fping, pinger, ping sweep
  - Will not work if victim network blocks ICMP_echo_request packet

 www.oissg.org

ICMP Ping Sweep:-

It usually sends the similar packets to various hosts in the network with random TTL values. Using random TTL values different routes can be determined. It is usually assumed that packets with small TTL/hope the packets unable to reach the destination and sent back to the originating hosts with message that “Sorry, TTL was not good enough to reach destination”.

OISSG

A Subtler Sweep…

- TCP ping sweep
  - Send TCP ACK packets
  - If machine is alive, it will respond with a RST
  - Else, no response is received
  - Scan a whole network address range

 www.oissg.org

TCP Ping Sweep:-

Once you obtain the IP block of the target organization, you use pinger to see what hosts are active.

TCP ping sweeper first sends ACK packet and wait for the respons. If if it get the response(RST) than the host is live, otherwise the host is not live.

What Applications Are Running?

- Server applications listen on known ports
  - A list of open ports on the server reveals server applications

A list of all the open ports can be obtained by the help of tools like nmap, fscan, superscan etc. Using this, the services and the application can be found.

OISSG

The Basic Port Scan

- Try to open a connection to each port:
  - If the connection succeeds, the port is open
  - Else, the port is closed
- Noisy scan
  - Too many short-lived connections appear in the logs

 www.oissg.org

It is the systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into target computer.

OISSG

The Half-open scan…

- TCP
  - Open port – SYN/ACK received
  - Closed port – RST received
- UDP
  - Open port – No response
  - Closed port – ICMP port unreachable

OISSG

Stealthier Scans

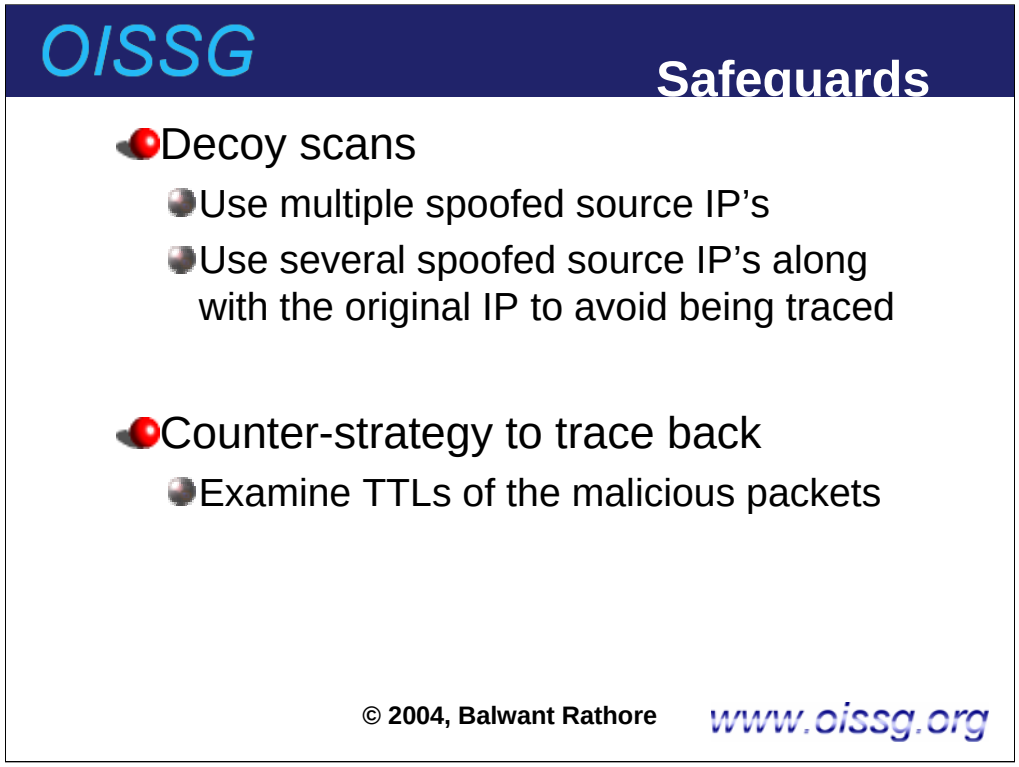
- **FIN scan**
  - Sends TCP packet with FIN flag set
- **XMAS scan**
  - Sends TCP packet with FIN, URG, PSH set
- **Null scan**
  - Sends TCP packet with no option set

[Ineffective against windows]

FIN scan :- Sends TCP packet with FIN flag set

XMAS scan :- Sends TCP packet with FIN, URG, PSH set

Null scan :- Sends TCP packet with no option set



Safeguards against the network scanning.

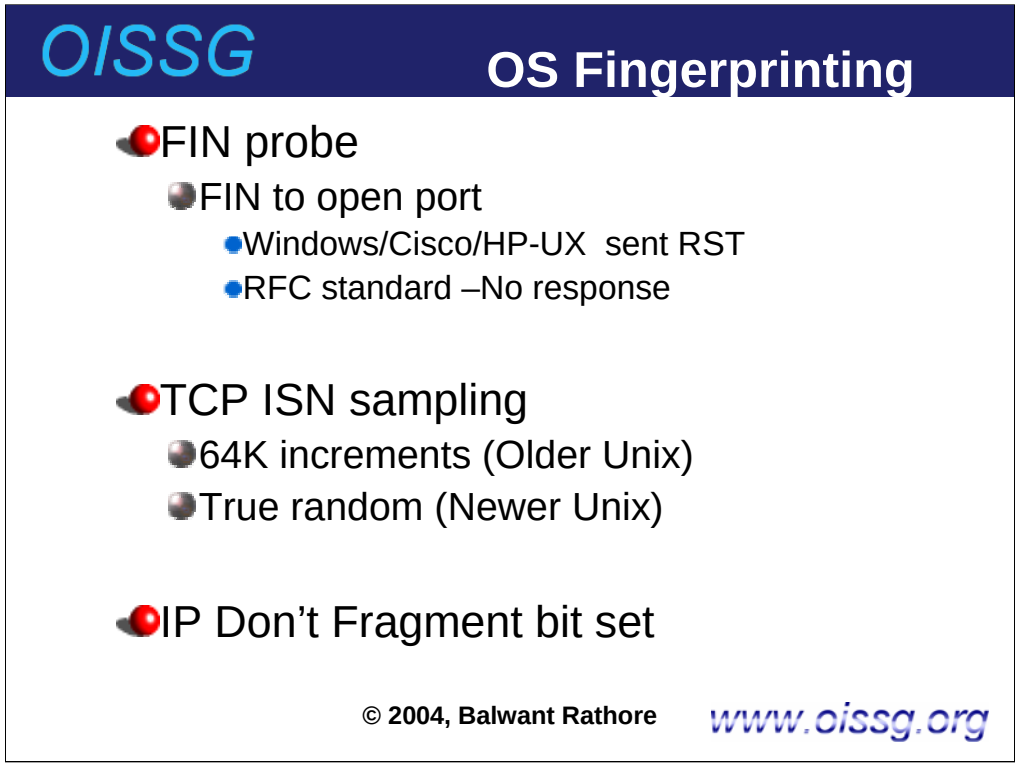
OISSG

Safeguards

- Reduce the speed of the scan
  - Paranoid scan
  - Polite scan
- Fragment TCP packets

www.oissg.org

Safeguards against the network scanning.



The Operating System of the host can be guessed in the following way:

- Telnet Banner Grabbing: - It is pretty self-explanatory, connect to telnetd on the remote host, and see what the telnet login banner prints, to guess the operating system.

- FTP Banner Grabbing: - It is also having the same basic concept as telnet banner grabbing, just with ftpd instead of telnetd.

OISSG

OS Fingerprinting

- TCP initial windows size
- Fragmentation handling
  - OS handle overlapping fragments differently

www.oissg.org

• HTTP head method, try and determine an OS by checking what web server (httpd) the target is running. i.e. Microsoft-IIS should be WindowsNT/2k.

OS Fingerprinting using NMAP

- TCP options
  - Not all OS's have implemented them
  - Response to TCP packets vary with OS
  - Nmap analyses response to 7 packets

Nmap is one of the best options available for the OS fingerprinting. It is very much user friendly and very quick to respond. Nmap is separately discussed in the course.

OISSG

ICMP OS Fingerprinting

- Using Regular ICMP Query Messages
- Using Crafted ICMP Query Messages
- Using ICMP Error Messages

www.oissg.org

Another option for the OS finger printing is the ICMP querying:

ICMP query are of three types:

• Regular ICMP Query Message

• Crafted ICMP Query Message

• ICMP Error Message

The "Who answer what?" approach

- The question "Which operating system answer for what kind of ICMP Query messages?"

helps us identify certain groups of operating systems.

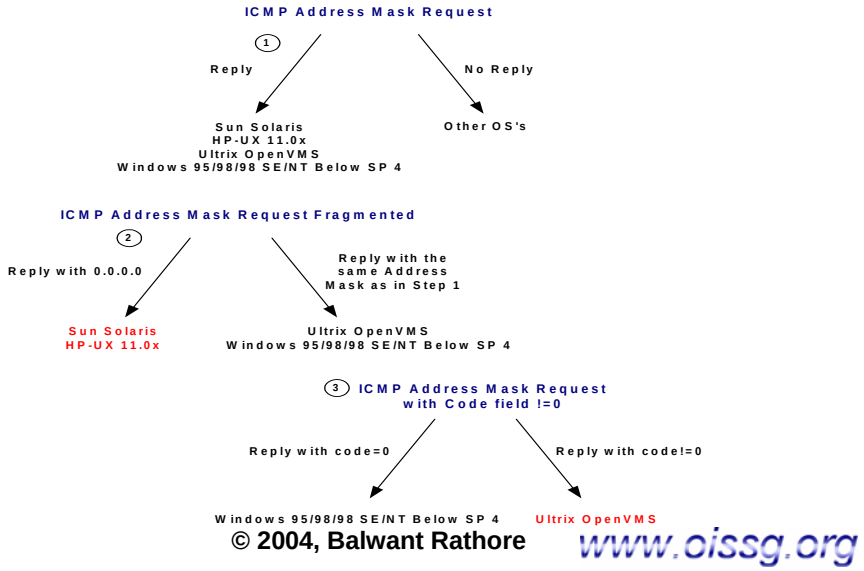
OISSG

IP Time-to-Live Field

Operating System	IP TTL value in the ECHO Requests	IP TTL value in the ECHO Replies
Windows	32	128
Microsoft Windows 2000	128	128
Microsoft Windows 95	33	32
*BSD	255	255
Solaris	255	255
Linux Kernel 2.2.x and 2.4.x	64	255
LINUX Kernel 2.0.x	64	64

www.oissg.org

Fragmented ICMP Address Mask Requests



OISSG ICMP Error Message Quenching

- An attacker can use this to send UDP packets to a random, high UDP port and count the number of ICMP Destination unreachable messages received within a given amount of time.
  - Solaris – 2msg/s
  - Linux – 80/4s
  - MS - all

OISSG ICMP Error Message Quoting

- Except for LINUX and Sun Solaris all other operating systems TCP/IP stacks will quote 8 bytes of the datagram that triggered the error message
- Sun Solaris sends more than 8 bytes of quoted information from the datagram that have triggered the CIMP error message
- Linux takes this to the extreme

 www.oissg.org

OISSG ICMP Error Message Echoing Integrity

- When sending back an ICMP error message, some stack implementations may alter the original IP header
  - AIX and BSDI send back an IP 'total length' field that is 20 bytes too high
  - Some BSDI, FreeBSD, OpenBSD, ULTRIX, and VAXen change the IP ID that you sent them

www.oissg.org

When sending back an ICMP error message, some stack implementations may alter the original IP header

Stealth port-scanning using Hping

- Idle host scan technique
  - Exploits predictability of IP identification numbers
  - Steps
  - Identify trusted host
  - Attacker sets up continuous IP session with trusted host
  - Attacker sends packets to ports on target with spoofed source ip (trusted host)
  - IP identification numbers in attacker-trusted host session changes if target port is open(no change if port is closed)

 www.oissg.org

HPing is a tool which enables to send packet with non traditional IP stack parameters and gather information from the results of the incoming packets (which were generated in responds to the sent packet), this information isn't displayed by regular application since much of it is for debugging and internal network functionality.

?

OISSG

Vulnerability Identification with Nessus

www.oissg.org

OISSG

Vulnerability Scanners

- Software which audits remotely a given network and determine whether it can break/Misuse by attacker
- Automates Security Checks across a large number of systems over the network.
- Only checks for the vulnerability that they know.
- Large number of tools available today.
- Our favorite freeware tool is Nessus.

OISSG Nessus - Vulnerability Scanner

- Conduct war dialing exercise against the own network
- Free, Open-source general Vulnerability scanner
- Used by both white hat community & black hat community.
- Nessus project was started by Renaud Deraison.
- Free Download available at http://www.Nessus.org
- Nessus does not take anything for granted.
- Works on Client server technology.
- Fast, reliable and has a modular architecture.
- Client available for windows as well as Linux. Server is available for Solaris, Free BSD & Linux.

 www.oissg.org

Nessus is very useful tool, and has some advantages over the commercial tools.

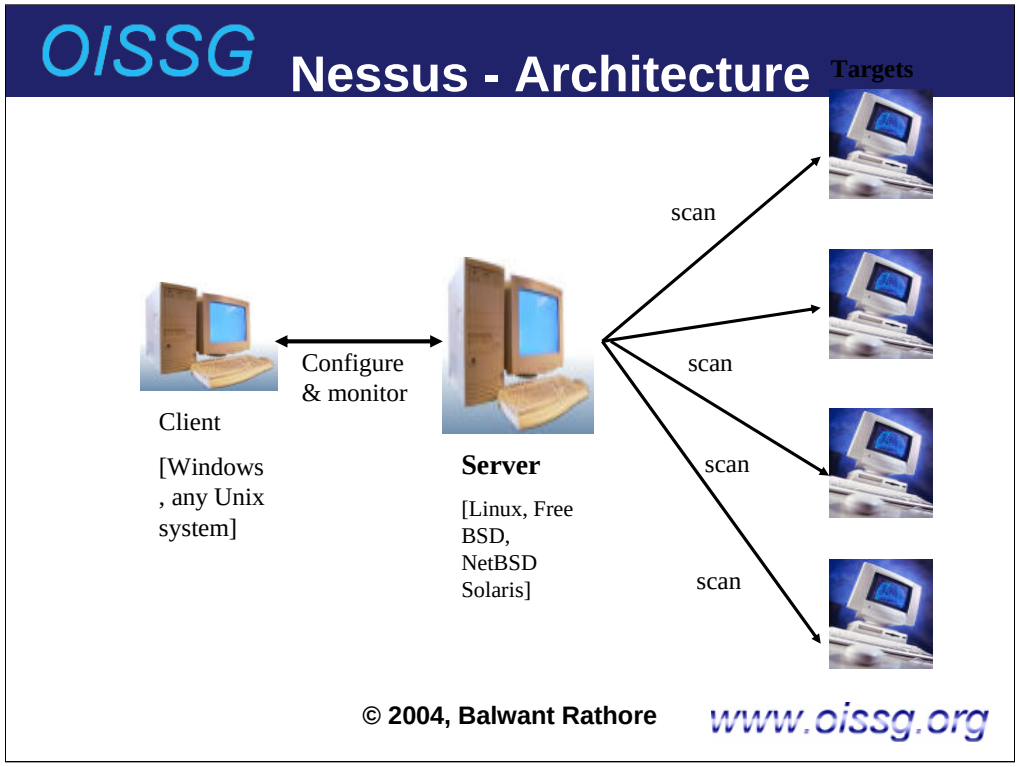
• Unlike many other security scanners, Nessus does not take any thing for granted. That is, it will *not* consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security.

• You can review the source code to make sure that nothing fishy is going on.

• You can write your own test code.

• You can write security test either in C or NASL.

• It's absolutely free.



• Nessus has a Client- Server Architecture. The main feature of Nessus is client & server can be on different networks.

• Server has numerous plugins with various test.

• The server has large number of plugins & you can write your own plugins.

• Information sent between the client & server can be encrypted.

OISSG

Nessus - Platform

- **Nessus Server available for**
  - Free BSD, Linux, Solaris.
- **Nessus Client available for**
  - Free BSD, Linux, Solaris, windows
  - Java.
- Client & server can run on same machine or on different machines, in most of the cases they are put on the same machine. Nessus recommends to use both client & server on the same machine.
- Provides separate plugin for each type of attack.

 www.oissg.org

The Java client really allows for portability. You can run the client from a Java virtual machine on numerous types of system, including a Macintosh.

Windows NT Nessus has only fewer capabilities compare to Unix Nessus.

OISSG

Nessus - Installation

- **Download the Nessus** (nessus 2.0, the current stable version of nessus)
  - http://www.nessus.org/download.html
- **Install Nessus**
  - sh nessus-installer.sh
- **Create a Nessusd account.**
  - The Nessusd server has its own users database, each user having a set of restrictions
  - The utility *Nessus-adduser* takes care of the creation of a new account
  - Restriction on a user is put by defining user rules.

 www.oissg.org

The nessus security scanner relies on the following items

- GTK. ftp://ftp.gimp.org/pub/gtk/v1.2.
- Open SSL http://www.openssl.org.

There are two ways to install Nessus :

- The easy and dangerous way (*ala ximian gnome :)*) If you are installing Nessus from a computer directly connected to the internet that has lynx installed, type this command (NOT as root!) :

lynx -source http://install.nessus.org | sh

- The easy and less dangerous way

sh nessus-installer.sh

OISSG Nessus - Installation (cont...)

Example:

Login : balwant

Authentication (pass/Cert) [pass] : pass

Password : secret

- **Configure your Nessus daemon**
  - In the file /usr/local/etc/nessus/nessusd.conf, you can set several options for nessusd.
- **Start Nessusd**.
  - nessusd -D (give this command as a root)
- **Configure Nessus client**.
  - /nessus/bin/./nessus. (GUI based)

 www.oissg.org

User rules:-

Nessusd has a rules system which allows you to restrict the hosts

that balwant has the right to test. For instance, you may want him to be able to scan his own host only. Enter the rules for this user, and hit ctrl-D once you are done : (the user can have an empty rules set)

deny 10.163.156.1

allow 10.163.156.0/24

default deny

Login : balwant

Password : secret

DN :

Rules :

deny 10.163.156.1

allow 10.163.156.0/24

default deny

Is that ok (y/n) ? [y] y

user added.

Nessus - GUI

The GUI runs at the client & allows for the configuration of the server.

Via the GUI, you can configure:

- The port of the client server communication.
- Encryption algorithm (Unix only)
- Target system(s) in a flat file.
- Which plugins to run.
- Port ranges & types of port scanning.
- Email address for report.

OISSG

Nessus - Plugins

- There is a defined API for writing Nessus plug-ins
  - Most of the plug-ins are written in NASL (around 99%).
  - Plugins can be written in C language as well.
  - One plugin is designed to perform some specific attack & to report the result to the Nessus server in specified format.
  - Each plugin uses some of the functions from the Nessus library & store information in the shared knowledge base which is used by other plugins to make the test faster.
- Over 1000 plugins are available.
- An older Windows - NT server exist, but with only few plugins.

 www.oissg.org

A very nice capability of Nessus is the ability to write your own plugins, a capability not supported in the major commercial scanners.

New plugins can be written in to C or NASL whichever you prefer.

OISSG

Important Plugins - list

- Backdoors
- CGI abuses
- CISCO
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- NetWare
- NIS
- Port scanners
- Remote file access
- RPC
- Settings
- SMTP problems
- SNMP
- Untested
- Useless Services
- Windows

 www.oissg.org

Nessus Plugins can be used to test/check the vulnerabilities. The Nessus plugin list is shown here.

OISSG

Nessus - Knowledge Base

All the plugins have the ability to share their knowledge.

Example:

- A 1st plugin determines that port 137 UDP and 139 TCP are open.
- A 2nd plugin retrieves the remote host Netbios name.
- A 3rd plugin attempts to log in using a NULL session.
- A 4th plugin retrieves the remote host SID.
- A 5th plugin uses the remote host SID to get the list of users.

• Results are being re-used, thus allowing Nessus to do more powerful and more comprehensive audits

www.oissg.org

OISSG

Nessus - Features

- Plug-in architecture.
- NASL.
- Up-to-date security vulnerability database.
- Client-server architecture.
- Can test an unlimited amount of hosts at the same time.
- Smart service recognition.
- Multiples services.
- Tests cooperation.
- Complete reports.
- Exportable reports.

 www.oissg.org

Plug-in architecture. Each security test is written as an external plugin. So, you can easily add your own tests without having to read the code of the Nessusd engine.

NASL. The Nessus Security Scanner includes NASL, (Nessus Attack Scripting Language) a language designed to write security test easily and quickly.

Smart service recognition. Nessus does not believe that the target hosts will respect the IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (31337 say), or a web server running on port 8080

Multiples services. Imagine that you run two web servers (or more) on your host, one on port 80 and another on port 8080. When it will come to testing their security, Nessus will test both of them

Tests cooperation. The security tests performed by Nessus cooperate so that nothing useless is made. If your FTP server does not offer anonymous logins, then anonymous-related security checks will not be performed

OISSG

Nessus - Features

- Smart plugins.
- Non-destructive.
- Independent developers.

www.oissg.org

Full SSL support : Nessus has the ability to test SSLized services such as https, smtps, imaps, and more. You can even supply Nessus with a certificate so that it can integrates into a PKI-fied environement

Independent developers. The Nessus developers are independent from the rest of the world, so we will not hide a security vulnerability in the program XYZ because we have a contract with them.

Non-destructive (optional) : If you don't want to take the risk to bring down services on your network, you can enable the "safe checks" option of Nessus, which will make Nessus rely on banners rather than exploiting real flaws to determine if a vulnerability is present

OISSG

Nessus - Report

Report Format Supported by Nessus: -

.NBE: Read by Unix Client.

.NSR: Deprecated in favor of NBE.

HTML: Without pipes & graphs.

HTML: With Pipes & graphs.

ASCII: Simple text format.

PDF: In PDF Format.

OISSG

NASL - Overview

- Language designed to write network related operations in no time
- Optimized for being used with Nessus, but not mandatory
- Roughly looks like C
- Contains high level functions (ftp_log_in(), http_get(), etc...)
- Each script is self sufficient (no need to go fishing around for modules)
- Optimized for the reuse of the information collected during a scan.
- Faster than Perl.

 www.oissg.org

- NASL uses a real Bison parser. It is stricter and can handle complex expressions.
- NASL2 has more built-in functions NASL2 has more built-in operators.
- NASL2 is much quicker then Perl.
- NASL2 user-defined functions can handle array.

OISSG

Countermeasures

- Shut off all the unnecessary services.
- Close all unused ports.
- Keep your system up-to-date with all system patches.
- Put an Intrusion detection system.

www.oissg.org

OISSG

?

www.oissg.org

OISSG

Penetration Testing

"fun with exploits"

…

www.oissg.org

OISSG

- **WebDav**
- **.printer ISAPI**
- **WU-FTPd**
- **SQL Server Resolution Service**

www.oissg.org

OISSG

WebDav

www.oissg.org

OISSG What is WebDav?

- WebDav means "Web-based Distributed Authoring and Versioning"
- WebDav is the vulnerability present in IIS5.0 web Server
- It cause Web Server Crash
- It gives complete control to attacker

 www.oissg.org

Attackers can send malformed WebDAV requests to a machine running IIS version 5.0 using port 80. Once attacker established connection to web server, they can easily exploit the vulnerability

WebDav vulnerability allows attackers to mount a denial of service (DoS) attack against Windows 2000 machines or execute their own malicious code in the security context of IIS service, giving them unfettered access to the vulnerable system

OISSG WebDav Vulnerability

- Present in IIS 5.0 on Microsoft Windows 2000 is affected
- Present in IIS 5 .0 on Microsoft Windows NT
- Microsoft Sharepoint running on Windows 2000 uses WebDav
- It is a Buffer Overflow Vulnerability
- which allows users to edit and manage files on remote web servers
- present in Windows shared library (ntdll.dll)
- allows attacker to execute arbitrary code on server

 www.oissg.org

This vulnerability is just present in IIS 5.0 running on MS-Windows 2000 machine or the MS-Sharepoint running on MS-Windows 2000.

WebDav Vulnerability allows Attackers to execute arbitrary code and/or allows them to modify files on remote web server.

OISSG WebDav Detection

- Nessus is able to find this vulnerability, but risk to crash the server
- Test Manually using telnet
- Test Manually using NetCat

 www.oissg.org

Nessus can be used to find the WebDav vulnerability, but there is a risk to crash the IIS web server during the vulnerability scanning. Nessus has also provided the safe test, using that the risk of crashing the web server minimised.

Telnet and NetCat can also be used for manual detection of vulnerability.

Telnet: Telnet to the specified host with the http port (usually port 80)
i.e. "telnet 203.124.156.112 80”

NetCat: nc -vv 203.124.156.112 80

type the following: OPTIONS*HTTP/1.0

(Press Enter Twice to get the result)

OISSG WebDav Exploitation

- Tools can be used to exploit this vulnerability
  - **xwbf-woodv3.exe**
  - **WebDav.exe**

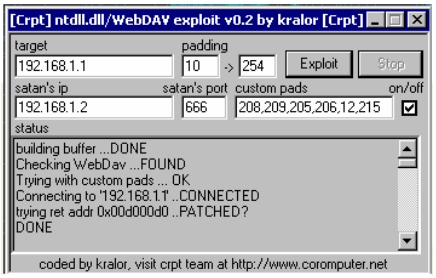
 www.oissg.org

xwbf-woodv3.exe: It uses intelligent bruteforcing of the stack offset using a list of offsets with a statstically higher probability of success. The GUI allows to attack IIS servers running on ports other than the standard port 80.

WebDav.exe: It is also same as the above one to exploit the WebDav vulnerability present in IIS 5.0 on Windows 2000 machine

OISSG WebDav Exploitation

- **xwbf-woodv3.exe**



 www.oissg.org

Graphical (GUI) view of the exploit.

Target :- Implies the target machine IP Address

Padding :- Specifies the padding range.

Press the Exploit button to exploit the target.

OISSG WebDav Precautions

- Microsoft has issued a patch for this vulnerability
- Use Microsoft's IIS lockdown
- If you don't need WebDav, disable WebDav by performing a Registry edit, and reboot the system

 www.oissg.org

Install the Patch to restrict the misuse of WebDav, just lock it down or disable it (using the registry)

To disable from registry:

Set registry key to 1:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\DisableWebDAV

OISSG

.printer ISAPI Vulnerability

www.oissg.org

OISSG What is .printer ISAPI

- ISAPI means "**I**nternet **S**erver **A**pplication **P**rogramming **I**nterface"
- Enables Web-based control of networked printers
- Present in Windows shared library (msw3prt.dll)

 www.oissg.org

The Windows 2000 Internet printing ISAPI extension contains msw3prt.dll that handles user requests. The .printer ISAPI filter which is present in window 2000 enables Web-based control of networked printers. Web-based printer support is enabled by default in IIS, therefore, a great many users will be affected.

The vulnerability occurs when a buffer of approximately 420 bytes is sent within the HTTP Host: header for a .printer ISAPI request. As Win 2000 automatically restarts the Web server after a crash, an attacker can gain easy access. The affected ISAPI extension is one that implements the Internet Printing Protocol (IPP).

OISSG .printer ISAPI vulnerability

- Present in Windows 2000 Professional + SP1
- Present in Windows 2000 Server + SP1
- Present in Windows 2000 Advanced Server + SP1
- Present in Windows 2000 Datacenter Server + SP1

The vulnerability is only exposed if IIS 5.0 is running

 www.oissg.org

Above Operating Systems are affected by the .printer ISAPI unchecked Buffer vulnerability. But could be exploited only if the IIS 5.0 web server is running.

.printer ISAPI vulnerability

- It's a Buffer Overflow Vulnerability
- which allows attacker to gain shell access on remote computer
- A remote attacker can gain full control of the host even behind a firewall
- Vulnerability cause Web Server Crash and Restart
- Vulnerability gives command shell access to a remote attacker
- Vulnerability occurs due to Unchecked Buffer in ISAPI Extension

 www.oissg.org

This vulnerability is present in IIS 5.0 running on MS-Windows 2000 machine. Usually it is enabled by default installation if Windows 2000.

This Vulnerability allows Attackers to gain the command shell access with system privileges and execute arbitrary code.

This vulnerability is due to the default web printer extensions msw3prt.dll unchecked buffer.

OISSG .printer ISAPI Detection

- Perl script “iiswebexplt.pl” could be used to check for the Vulnerability
- Perl script “iiswebexplt.pl” is only for detection not an exploit
- Jill.c is an exploit, which is used to exploit the vulnerability and to gain the shell access
- Jill.c is not for checking the vulnerability

 www.oissg.org

To detect the .printer ISAPI web-printing buffer overflow vulnerability, use the perl script iiswebexplt.pl. This script used to check the vulnerability not for exploitation.

To exploit the vulnerability, use jill.c and get the command shell access (and complete control of the web server) with the system privileges causing web server restart, so that attacker could not be identified.

.printer ISAPI Precautions

- Microsoft has issued patch for this vulnerability
- Remove .printer extension (if not using web printers) from the web server configuration

 www.oissg.org

Install the Patch to restrict the misuse of .printer ISAPI extension/filter, just disable it (using the web-server configuration)

To disable using web-server configuration:

- Open Internet Services Manager
- Select Web Site -> Properties
- Home Directory -> Configuration
- Remove .printer extension present there.

OISSG .printer ISAPI Exploitation

- Jill.c exploit can be used to exploit the Vulnerability
- For Exploitation, first use netcat to set listen port
- than use exploit to get the command shell access

 www.oissg.org

How to Exploit:-

Step 1: Set the listener port using netcat nc –l –p 23 -vv

Step 2: Run the exploit to get the command shell access

The web server accepts the print request and writes the data to the buffer. The program code is larger than the buffer so it overwrites the part of the program that controls the next instruction to be processed. The next instruction to be processed is the request for cmd.exe to load and connect to the attacker's machine on the port requested in netcat.

OISSG

WU-FTPd “Globbing Heap Corruption” Vulnerability

www.oissg.org

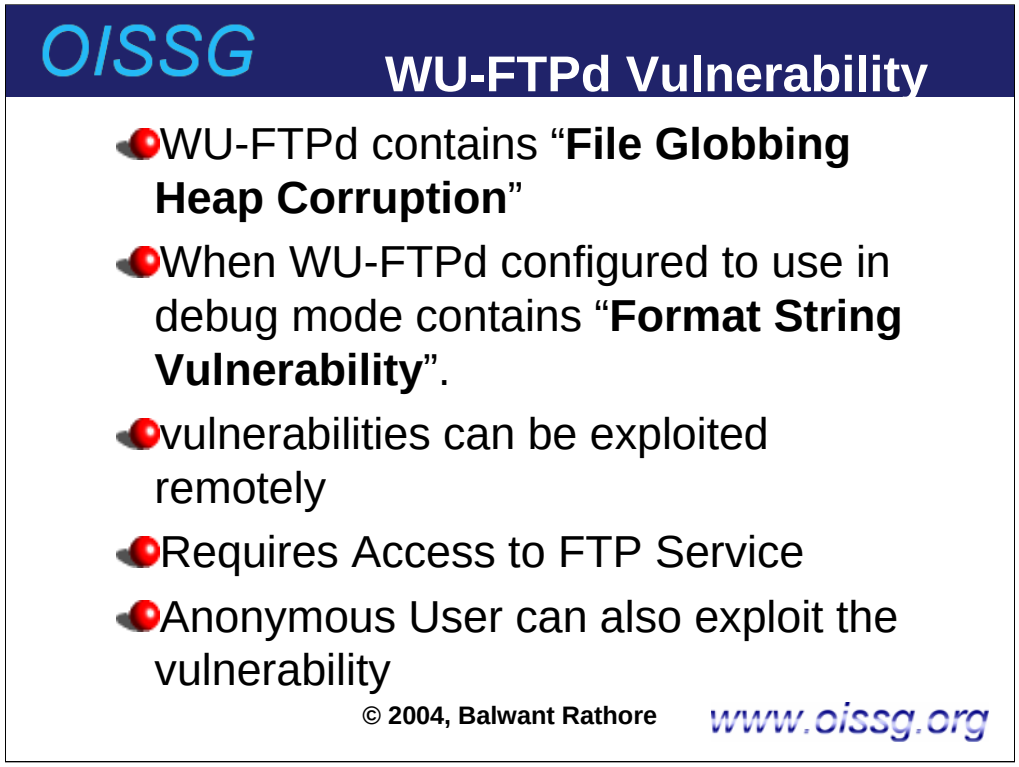
OISSG What is WU-FTPd ?

- WU-FTPd provides FTP services.
- WU-FTPd means Washington University FTP daemon
- The wuftpd package as shipped with SuSE Linux
- For Other Unix & Linux versions, need to install separately.
- Two vulnerabilities that expose the system to potential remote root access

 www.oissg.org

Washington University FTP daemon (WU-FTPD) is a widely deployed software package used to provide File Transfer Protocol (FTP) services on UNIX and Linux systems. The wuftpd package as shipped with SuSE Linux

There are two vulnerabilities in WU-FTPD that expose a system to potential remote root access to the FTP service.



WU-FTPD features globbing capabilities that allow a user to specify multiple file names and locations using typical shell notation. WU-FTPD implements its own globbing code instead of using libraries in the underlying operating system.

Both of these vulnerabilities can be exploited remotely by any user with access to the FTP service, including anonymous access. Both vulnerabilities allow an intruder to execute arbitrary code with the privileges of WU-FTPD, typically root. An exploit attempt that does not succeed in executing code may crash WU-FTPD or end the connection used by the intruder.

When the globbing code is called, it allocates memory on the heap to store a list of file names that match the expanded glob expression. The globbing code is designed to recognize invalid syntax and return an error condition to the calling function. However, when it encounters a specific string, the globbing code fails to properly return the error condition. Therefore, the calling function proceeds as if the glob syntax were correct and later frees unallocated memory that can contain user-supplied data.

OISSG

WU-FTPd Vulnerability

- Attacker can have the Super User/ROOT Privilege
- Attacker can execute the arbitrary code
- It can crash the WU-FTP
- Requires Access to FTP Service
- Anonymous User can also exploit the vulnerability

 www.oissg.org

If intruders can place addresses and shellcode in the right locations on the heap using FTP commands, they may be able to cause WU-FTPD to execute arbitrary code by later issuing a command that is mishandled by the globbing code.

This vulnerability is potentially exploitable by any user who is able to log in to a vulnerable server, including users with anonymous access.

If the exploit is successful, an attacker may be able to execute arbitrary code with the privileges of WU-FTPD, typically root.

If the exploit is unsuccessful, the thread servicing the request will fail, but the WU-FTPD process will continue to run.

OISSG

WU-FTPd Vulnerability

- WU-FTPd can be used on various UNIX and Linux systems
- need to be installed separately on the Unix and Linux systems
- Shipped with SuSE Linux by default

As the WU-FTPd can be compiled and run on a wide variety of UNIX and Linux systems and if WU-FTPD is installed separately, the source code patches from the WU-FTPD Development Group need to be applied.

OISSG

WU-FTPd Precautions

- Apply the patch issued by the system vendors
- Restrict access to WU-FTPd
- Disable the service, if not required explicitly
- Limit by blocking or restricting access to the control channel (by default, port 21/tcp)
- Disable the Anonymous FTP access

Note that blocking access from untrusted networks such as the Internet does not protect your systems against attacks from within your network.

www.oissg.org

As a general practice, disable services and access that are not explicitly required. The service is to be disabled until the patch is not applied.

If the service cannot be disabled, the exposure to these vulnerabilities can be limit by blocking or restricting access to the control channel (by default, port 21/tcp) used by WU-FTPD.

Although disabling anonymous FTP access does not prevent attacks from occurring, it does prevent unauthenticated users from attempting to exploit the globbing vulnerability.

OISSG

SQL Server Resolution Service Vulnerability

www.oissg.org

OISSG

What is SSRS?

- SSRS means “SQL Server Resolution Service”
- Microsoft SQL Server exploit that uses a known buffer overflow vulnerability
- Resolution Stack Overflow (CAN-2002-0649)
- Will only work if they did not patch with Service Pack 3

 www.oissg.org

Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability: -

There are two buffer overflow vulnerabilities present in SQL Server Resolution Service (SSRS) which allow unauthenticated remote attackers to overwrite portions of system memory (the heap in one case, the stack in the other).

Using these vulnerabilities attacker can execute arbitrary code by sending a specially crafted request to UDP port 1434. As the attackers can weaken the SQL Server security policy by elevating their privileges to run in the Local System security context, this vulnerability increases the severity of the other vulnerabilities and may enable attackers to compromise

OISSG

MS Resolution Service

- Allows incoming connections to choose among multiple SQL Server databases on a single machine.
  - Default instance listens on 1433/tcp
  - Connections rerouted to appropriate port
- Found in all MS products using MS Desktop Engine (MSDE) 2000

 www.oissg.org

MSRS: Microsoft SQL Server Resolution Service:

This Service is used to choose the SQL Server among the multiple incoming connections to the various SQL servers.

OISSG SSRS vulnerability

- Present in Windows 2000 + SP3
- Present in Microsoft SQL Server + SP0
- Present in Microsoft SQL Server + SP2

The vulnerability can be exposed only if Real Server 8 is running

 www.oissg.org

Above Operating Systems are affected by the vulnerability.

OISSG

SSRS Precautions

- Microsoft has issued patch for this vulnerability
- Administrators are advised to block all external access to database servers
- Access to TCP and UDP ports 1434 should be denied completely
- Microsoft recommends that affected users apply SQL Server 2000 Service Pack 3

www.oissg.org

Install the Patch to protect against the vulnerability, just disable TCP UDP ports 1434, also block external access to database servers.

Apply the SQL Server 2000 Service Pack 3 immediately .

?

Thanks for your time !