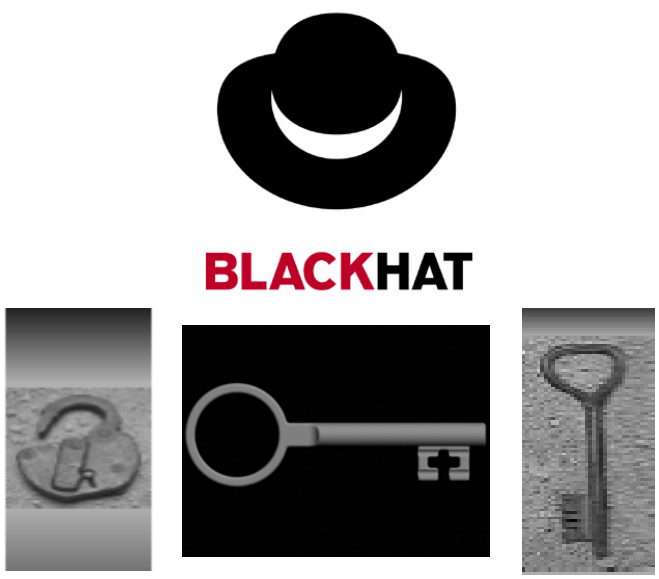
FIST-Conference Delhi

Hack and Investigate



10th to 16th May 2004, Delhi – India

TABLE OF CONTENTS

Registration:

Email: balwant [at] oissg [dot] org

Sponsor:

Looking for sponsors who can bear the cost of printing and/or Internet and/or food cost for participants.

Date and Time:

10th to 16th May 2004
Every day @ 09:00 to 18:00

We expect some guest speakers every day in evening so please be flexible with evening timings. You may have to stay little later.

Cost:

- FIST is absolutely open and free event.
- You have to take care of your boarding and lodging expenses. If required we can suggest you.
- We may need to pay for course material and certification printing/internet uses and for CD if we don't get any sponsor for this. It's not going to be > € 20 (Rupees 1000).

Location:

D–89, South Ganesh Nagar, Opp Mother Dairy, Patparganj, New Delhi - 92

Point of Contact:

Balwant Rathore, Phone: 91-11-2253-1445

Lab

The lab includes Routers, Switches, Firewalls, Intrusion Detection Systems, Windows and Unix Hosts. It will cover around 40 extensive exercises, which will provide detailed practical knowledge of attacking and securing systems. Various commercial and open source tools will be used on multiple operating systems and network devices.

Every day data will be collected in templates and reports will be generated.

We recommend you to come with your laptops, Ethernet card and cable (Straight and Cross Over); **it's not mandatory** (we have enough PCs) but will help you to get most out of course. Install two operating systems (Windows 2k server / professional or XP professional and Linux) in it. Configure it in following way:

- Dual-boot system with Windows partition and Linux on top of it.

or

- Install Windows and Linux on top of it using any Virtual machine (e.g. VMware workstation). Virtual machine allows multiple operating systems simultaneously on single laptop. You should do this only if you have minimum 256 MB RAM in your laptop, so you can assign 128 MB RAM to each operating system. You can download a free thirty-day trial version from

http://www.vmware.com/. To establish a base line of commonality we recommend you to use RedHat 9.0, 8.0.

Your laptops may be attacked in lab intentionally or un-intentionally by someone. OISSG will not be liable for this. We recommend you to not to store sensitive data in it.

A CD full with attack code/tools/products and reading material will be given to you to use it in lab and later. You will also get updates of these CDs in future.

Teamwork is a must in order to cover several topics in this short span of time.

Target Audience: Ethical Hacking

- Penetration Tester, Security Auditor and Security testers
- Security testing / penetration testing project managers
- Security engineers and consultants
- System/network administrators
- Web application administrator
- Technical and Functional managers
- IT Staff responsible for information security

Target Audience: Forensics

- Members of Computer Security Incident Response Team (CSIRT)
- Security professionals
- Forensic application developer

Agenda:

In this duration you will learn how to attack and investigation techniques. Below mentioned contents are used by both attackers and investigators. This process is structured, systematic and disciplined. Details are given below:

Day One: 10th May 2004

Instructor: Balwant Rathore, CISSP, balwant [at] oissg [dot] org

Ethical Hacking
Module 1: Getting Acquainted

- With Speaker and Participants
- About Course
- Course Objective
- Course Goal

Module 2: Introduction and Overview

- HACKERS, CRACKERS AND "SCRIPT-KIDDIES"
- BLACK BOX AND WHITE BOX TESTING
- INDUSTRIAL TRENDS
  - VULNERABILITY ASSESSMENT
  - PENETRATION TESTING
  - SECURITY TESTING
  - SECURITY AUDIT
- RISK ASSESSMENT METHODOLOGY
- OVERVIEW OF INFORMATION SYSTEM RISK
- RATING A VULNERABILITY
- RETURN ON SECURITY TESTING INVESTMENT
- LEGAL ISSUES
  - LEGAL ASPECT OF SCANNING
  - LEGAL ASPECTS OF PUBLISHING EXPLOIT CODE
  - PRIVACY ISSUES
  - INTERRUPTION OF COMMUNICATION
- PRIORITIZE SECURITY TESTING ACTIVITIES
- COMPARISON OF TESTING TECHNIQUES

Module 3: Project Management, Responsibilities, Guidelines and Ethics

- AUTHORIZATION
- DEFINE THE SCOPE OF WORK
- DEFINE THE “OUT OF SCOPE” AREAS
- SET MILESTONES AND TIMELINES
- TEAM COMPOSITION
- COMMERCIALS
- REPORT GENERATION
- SEND SAMPLE REPORT AND PROPOSAL
- MAINTAIN CONFIDENTIALITY OF CUSTOMER DATA
  - BEFORE START OF PROJECT
  - DURING THE PROJECT
  - AFTER THE PROJECT
- GUIDELINES
  - ENSURE TESTER MACHINE SECURITY
  - PROVIDE PROOF OF TESTER MACHINE SECURITY
  - ALWAYS OPERATE IN THE LIMITATIONS OF YOUR AGREEMENT
  - RECORD EVERYTHING DURING THE COURSE OF TESTING
- RESPONSIBILITIES
- BEST PRACTICES
  - SUBMIT YOUR REPORT BEFORE PRESENTATION
  - GATHER TEST INFORMATION IN STRUCTURED ORDER
  - DEFINE TEST CASES AND GET IT APPROVED FROM CUSTOMER IF YOUR ENGAGEMENT NEED THEM
  - OBTAIN CUSTOMER APPROVAL ON REPORT FORMAT
- MAN-DAYS CALCULATION
- SET DELIVERABLES
- ACCEPTANCE CRITERIA
- DEFINE PROJECT SCHEDULE AND MILESTONES
- DEFINE ACCESS POINTS

Module 4: Methodology

Network- and telecommunication, system, application and Database Security Methodology

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Penetration
- Gaining Access & Privilege Escalation
- Enumerate Further
- Maintaining Access
- Delude thy Presence (Covering The Tracks)
- Reporting
- Clean up and Destroy Artifacts

Day Two: 11th May 2004

Instructor
1. Balwant Rathore, CISSP, balwant [at] oissg [dot] org
2. Nilanjan De, n2n [at] front [dot] ru
3. Abhisek Datta, Abhisek [at] front [dot] ru

Module 6: Windows Hacking

1. Identify Live Hosts
2. Identify Ports and Services
3. Enumeration Attack
   - Identify Users
   - Identify Shares
   - Identify Policies
   - Enumerate Registry
   - Netbios enumeration
     - Netbois Name enumeration
     - Netbios Session enumeration
   - MIB Enumeration
     - SNMPwalk
     - SNMPget
4. Examine Common Protocols
5. Examine Windows WinNT/2k/2003
   - Remote Attacks
     - Password Attacks
       - SMBGrind
     - Bufferoverflow Attacks
       - Parameter Checks in System Calls
     - Heapoverflow Attacks
     - Integeroverflow Attacks
     - Formatstring Attacks
     - Web Server Attack
     - Mail Server Attacks
     - NetBIOS Attacks
       - RedButton
       - Server Message Block Attacks
       - MD4 Collision Attacks
       - Scheduling Attacks

- Registry Attack
- Reverse Shell Attacks
- Port Redirection
- Sechole Attack (IIS)
- Denial of Service Attack
  - WinNuke
  - Teardrop, Teardrop2 (bonk and boink)
  - Land and LaTierra

- Local Attacks
  - Registry Attacks
  - Privilege escalation
    - GetAdmin
    - pipeup admin
    - LPC attack
    - everyone2user.exe
  - Password Attacks
    - Password Dumping
    - DLL Injection
  - By passing the Authentication
    - Using other Operating System
    - Using bootable Tools
  - File System Attack
    - File Allocation Table (FAT
    - High Performance File System (HPFS
    - NT File System (NTFS)
    - Namned Pipe File System (NPFS)
    - Mailslot File System (MSFS)
  - Denial of Service Attack
    - NTCrash
    - CPUHog
    - System Initialization
    - Rollback
    - Virus Attacks

Module 7: UNIX Hacking

- Identify Live Hosts
- Identify Ports and Services
- Enumeration Attack
  - Identify Users
  - Identify Shares
  - Identify Policies
- Examine Common Protocols
- Examine Unix
  - Remote Attacks
    - Password Attacks
    - RPC Attacks
    - Bufferoverflow Attacks
    - Heapoverflow Attacks
    - Integeroverflow Attacks
    - Formatstring Attacks
    - Web Server Attacks
    - Mail Server Attacks
    - X-insecurities
    - NFS Share Attacks
  - Local Attacks
    - File and Directory Permission Attacks
    - Symlink attacks
    - System call attacks
    - Key logger attacks
    - Booting from other operating system
    - Root-kit attacks

Day Three: 12th May 2004

Instructors:
1. Balwant Rathore, CISSP, balwant [at] oissg [dot] org

Module 8: Web Application Hacking

- Find out Running Services on Web Server
- Enumeration
  - Identify Web Server vendor and version
  - By header analysis
  - By default files
  - By banner Grabbing
  - Identify Web Server directory structure
  - Find username/password by view source
  - Check HTTP-EQUIV for auto redirection
  - Copy web site and perform offline analysis
    - Find keyword like "pass" into .html files
    - Find email addresses
    - Find External links
  - Check Web Server detection
  - Test View Source bugs
  - Test product specific bugs
  - Test Common Gateway Interface
  - Test Directory Traversal
  - Test Unvalidated Parameters
  - URL Manipulation
  - Hidden Form Fields Manipulation
  - Cookie Manipulation
- Vulnerability Identification
  - Check vulnerabilities associated with web server version
  - Run Automated Web Vulnerability Scanner
  - Input Validation Attack
  - Test Input Validation
  - Test Buffer overflow
  - PHF Insertion
  - Test SQL Injection

- Server Side Include

Module 9: Router, Routing Protocol and Firewall Attacks

- Router Attacks
  - Router issues
    - Path integrity
    - Source routing
  - Routing Protocol issues
    - Autonomous System Scanning
    - Routing Information Protocol (RIP) testing
    - RIP v1 testing
    - RIP v2 testing
    - Open Shortest Path First (OSPF) testing
    - Border Gateway Protocol (BGP) testing
    - IRDP testing
    - IGRP testing
    - EIGRP (discovery)
- Firewall Attacks

1. Identify firewall
   - Perform Tracerouting
     - ICMP (#traceroute -I target.com)
     - UDP (#traceroute target.com)
     - TCP (#tcptraceroute target.com)
   - Analyze the results and identify possible firewall network range.
   - Identify firewall presence
   - Scan for default firewall ports
   - Perform Banner Grabbing on Default Firewall Ports
   - Check target response on SYN/ACK, RST/ACK and ICMP type 3 code 13 message.
   - Identify Firewall Architecture
2. Map Firewall Rule-set
3. Attack Scenarios

Module 10: Bypassing Intrusion Detection System

Day Four: 13th May 2004

Module 11: Wireless Hacking
Module 12: Report Writing

Day Five: 14th May 2004

Forensics:

Module 13: Nuts and Bolts of Computer Forensics and Incident Response
Module 14: Recovering and Preserving Evidence
Module 15: Back Tracing
Module 16: Miscellaneous Cyber Crime Detection Techniques

Day Six: 15th May 2004

Exam

Examination would be based on two criteria's, which are as follows:
Phase I: Writing one paper
Phase II: Passing an exam

Participants who successfully pass this exam will be certified as "Certified Security Analyst"

Participants who can't pass this exam will be given certificate for attending this course.

Day Seven: 16th May 2004

Contest: Capture the Flag

Due to infrastructure constraints we were not able to organize this in Mumbai from 15th to 18th April as scheduled. Now we are doing it offline in the end of this conference.

There would be four challenges. Four hrs would be given to every team, the goal of which is to capture a flag image on the target system. The team capturing the flag first is required to send a message with the flag file to monitoring team.

For each challenge the first two teams to report back with the flag would be the winners for the challenge.

As soon as first two teams report, the challenge would be closed. The winners would be announced after analysis at the same day.

In a given time one has to get in using any allowed technique and whoever captures the flag will win.

Date and Time
16th May 2004, 17:00

Challenges
1. Windows Hacking
2. Unix Hacking
3. Web Application Hacking

Explicit denied techniques.
1. Any form of DoS and DDoS is not allowed (machine can't be taken down.)
2. Data deletion is not allowed.
3. Virus, Worm and Trojans are not allowed.
4. System can not be used for staging attacks on other systems other than the given target.

Permitted Techniques
* Everything is permitted accept the above mentioned techniques

Rules and Regulations
1. Server IP address will be given over yahoo messenger at the time of reporting for the challenges.
2. Any exploit (Including Zero Day) used needs to be disclosed.
3. Judgment of the OISSG managing committee for the challenge would be final and binding.
4. Teams violating the rules and regulation would be disqualified without any further discussion.
5. OISSG committee members and Organizers can not participate in the contest
6. Participating teams have to operate from remote location.
7. A team shall comprise of maximum 3 participants.
8. Prize distribution will be local and the shipping cost will be born by teams (If we will get sponsorship, we will send it)
9. The date and time notations are Indian Standard Time.
10. No exploit shall be used against monitoring and supports systems.