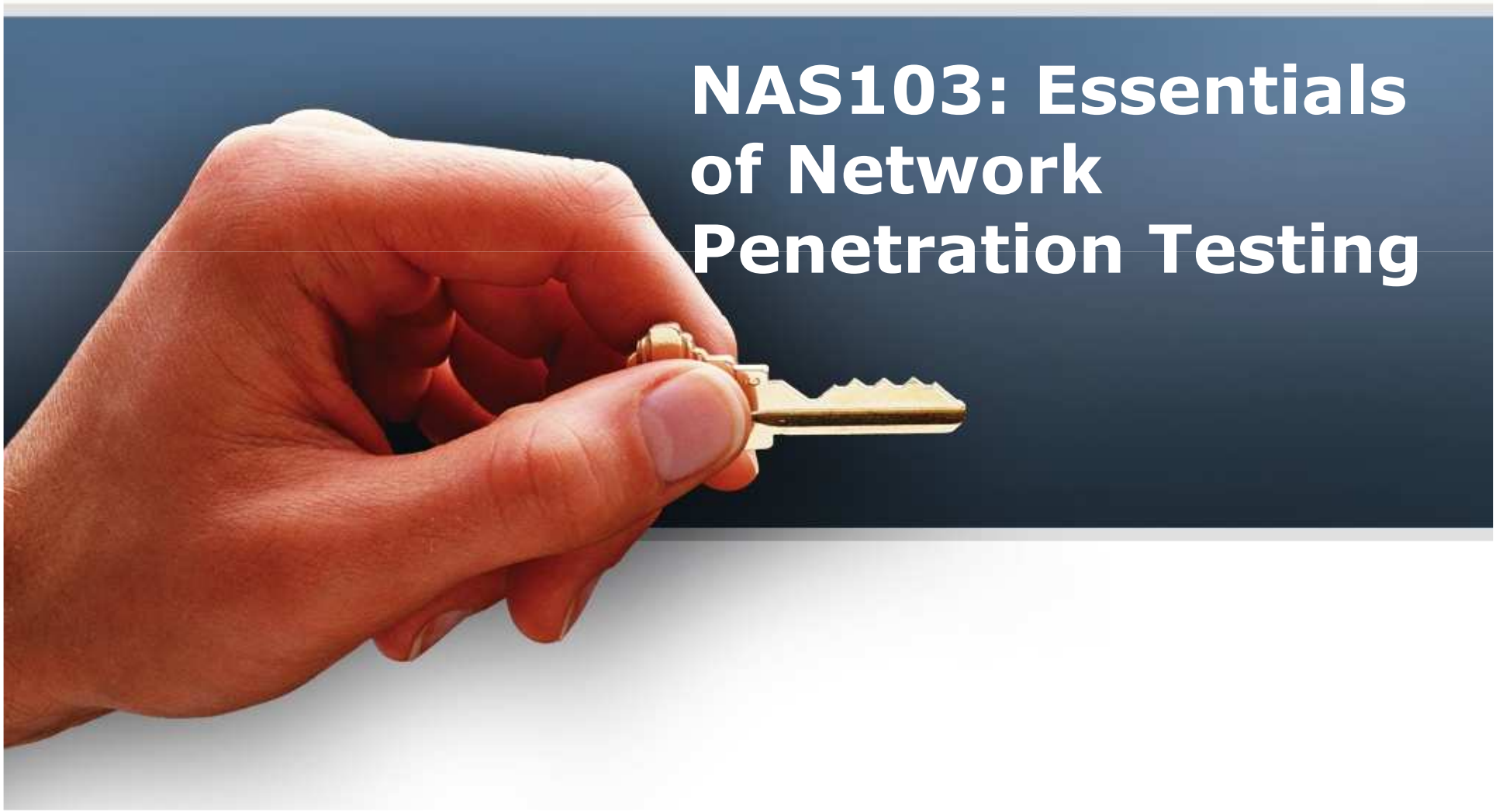
NAS103: Essentials of Network Penetration Testing



Course Introduction

- Duration: 1 Day
  - 3 Sessions

- Objectives
  - Introduce you to definitions involved in Penetration Testing
  - Prepare you for a Network based Penetration Test
  - Take you through a Network Penetration Test Tools and Methodology
  - Enable you Understand and Write a Penetration Testing Report
  - No Tool, Tool, Tool Demonstration. Conceptual knowledge for strong base

- Prerequisites
  - Working knowledge of TCP/IP
  - Working knowledge of Windows Commands
  - Working knowledge of Bash Commands

Course Benefits

- This course will be helpful for
  - Penetration Testing Practitioners within the Organizations or Consultants
  - Network Penetration Testing Project Leads
  - Network Engineers and Administrators
  - Prospective Network Penetration Testing Clients

- At the end, you will be able to
  - Setup a Basic Network Penetration Testing Lab
  - Brainstorm and Dialog with Professional Penetration Testers
  - Write Basic Network Penetration Testing Reports
  - Understand Paid Network Penetration Reports

- You will not be able to
  - Setup a Professional Network Penetration Testing Lab
  - Perform Professional Network Penetration Testing
  - Write rigorous Penetration Testing Report

Mindset

- *"We break computers, making them do stuff that their designers, implementers, and system administrators didn't plan on them doing."* by a Noted Penetration Tester

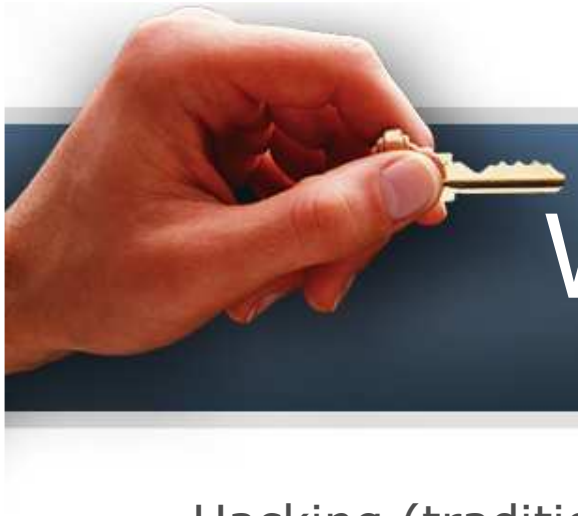
- Successful penetration testers and ethical hackers
  - Think out of the box, to do things differently
  - Be pragmatic but careful
  - Take notes regularly to make work reproducible

What is Security?

- Confidentiality
  - Confidentiality, also referred to as privacy, is the process of making sure that data remains private and confidential
- Integrity
  - Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification
- Availability
  - From a security perspective, availability means that systems remain available for legitimate users

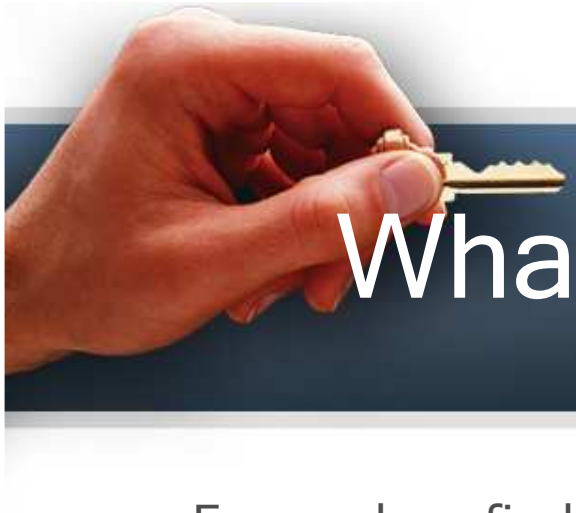
Base Definitions

- Threat: An agent that may cause harm to the target organizations
- Vulnerability: Flaw or loophole in our resources that can be used by an attacker to cause damage or destruction
- Risk: Identification of vulnerabilities and threats shape into risks. That is, we have a risk when our system carries a vulnerability which can be attacked by a threat
- Exploit: Exploit is an object which is initiated by the threat agent to cause damage to the organization using a vulnerability
- Attack: Series of actions that exploits vulnerabilities in the target which may violate Confidentiality, Integrity and Availability of the organization



What is Ethical Hacking?

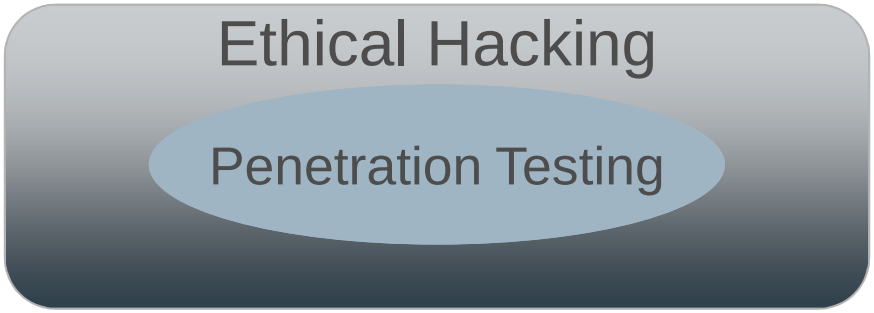
- Hacking (traditional)
  - Manipulating technology to make it do something that it is not designed to do
- Hacking (threatening)
  - Breaking into computers and network systems without permissions
- Hacking – Computer Security (wikipedia)
  - Hacking means finding out weaknesses in a computer or computer network and exploiting them, though the term can also refer to someone with an advanced understanding of computers and computer networks
- Ethical Hacking (wikianswers)
  - Ethical hacking is where a person hacks to find weaknesses in a system and then usually patches them

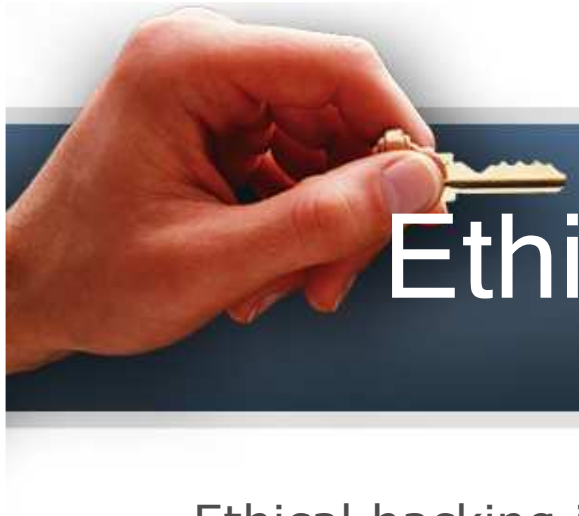


What is Penetration Testing?

- Focused on finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems, or steal information
  - Using tools and techniques very similar to those employed by criminals
  - To prevent a thief, you may need to think like a thief
  - The goal is actual penetration – compromising target systems and getting access to information

- Penetration testing is a subset of ethical hacking



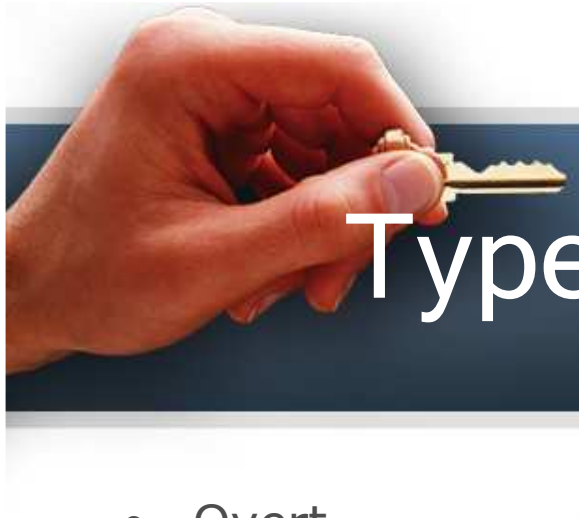


Ethical Hacking v/s PenTest

- Ethical hacking is a general process of using hacker techniques for good purpose, which includes vulnerability discovery in a target organization's network, software product vulnerability research, and other tasks

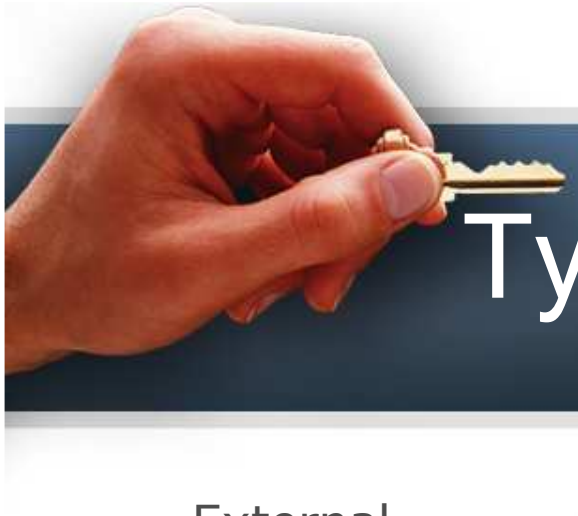
- Penetration testing is more narrowly focused phrase, dealing with process of finding flaws in a target environment with the goal of penetrating systems, taking control of them

- Penetration testing is focused on penetrating the target organization's defenses, compromising systems and getting access to information



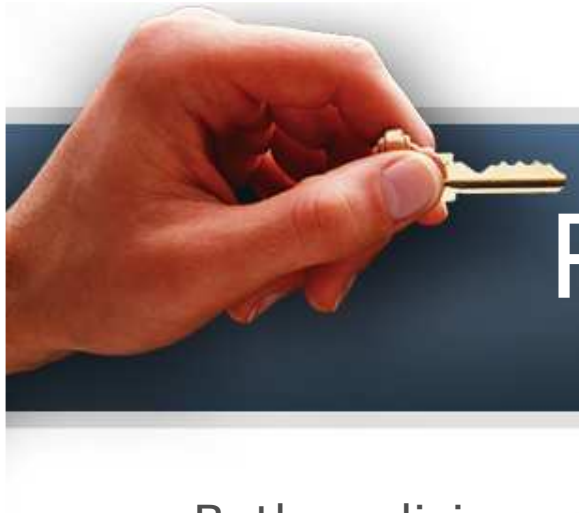
Types of Penetration Testing

- Overt
  - Also known as **White Hat Testing**, involves performing external and/or internal testing with the knowledge and consent of the organization's IT staff, enabling comprehensive evaluation of the network or system security posture.
  - As IT staff is fully aware of and involved in the testing, it may be able to provide guidance to limit the testing's impact along with some training opportunity, with staff observing the activities and methods used by assessors to evaluate and potentially circumvent implemented security measures
- Covert
  - Also known as **Black Hat Testing**, takes an adversarial approach by performing testing without the knowledge of the organization's IT staff but with the full knowledge and permission of upper management
  - Purpose of this testing is to examine the damage or impact an adversary can cause—it does not focus on identifying vulnerabilities.



Types of Network PenTest

- External
  - This testing is conducted from outside the organization's security perimeter. This offers the ability to view the environment's security posture as it appears outside the security perimeter—usually as seen from the Internet—with the goal of revealing vulnerabilities that could be exploited by an external attacker
- Internal
  - In this type of testing, assessors work from the internal network and assume the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This kind of testing can reveal vulnerabilities that could be exploited from inside, and demonstrates the potential damage an internal attacker could cause
- If both internal and external testing is to be performed, the external testing usually takes place first. This is particularly beneficial if the same assessors will be performing both types of testing



Phases of an Attack

- Both malicious and ethical hackers rely on various phases in their attacks:
  - Reconnaissance
  - Scanning
  - Exploitation
- Malicious attackers often go further, into phases such as:
  - Maintaining Access with backdoors and rootkits
  - Covering tracks with covert channels and log editing

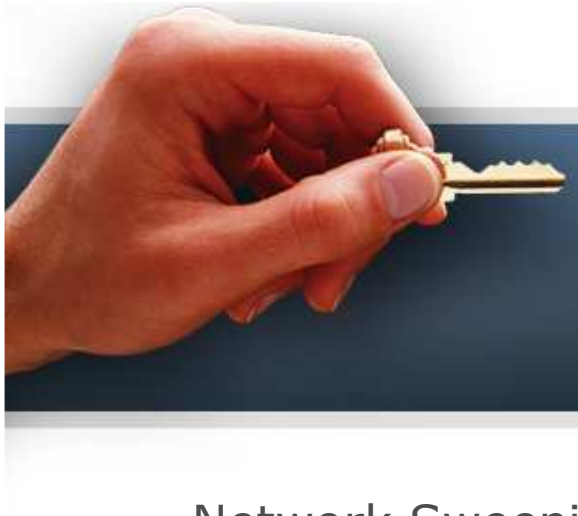
Reconnaissance

- Also known as Passive Information Gathering, this phase includes gathering information about the target from public sources
  - Web presence not just website
  - Search engines
  - Web archives
  - Personal websites of employees
  - Job postings
  - Newsgroups
  - Domain Registrar

- By the end of this phase, the penetration tester will have a wealth of information regarding the target without ever visiting the target's network. All passive information is gathered from third-party sources that have collected information about our target, or have legal requirements to retain this data.

Scanning

- Also known as Active Information Gathering, this phase includes gathering information by interacting with the target network
  - Network addresses of live hosts, firewalls, routers, etc
  - Network topology
  - Operating systems on live hosts
  - Open ports
  - Running services
  - Potential vulnerable services
- Minimize the chance of damaging the target machine(s), as there is always a possibility that our interactions could cause a target system or service to buzz the alarm of intrusion



Type of Scanning

- Network Sweeping
  - Identifying live hosts at IP addresses by sending probe packets
- Port Scanning
  - Determining listening TCP and UDP ports on systems
- OS Fingerprinting
  - Determining target operating system type based on network behavior
- Service Scanning
  - Identifying running services and protocols from open ports along with versions
- Vulnerability Scanning
  - Listing down potential vulnerabilities in the target environment

Exploitation

- Taking advantage of a vulnerable service in gaining access to a machine in target environment to run command in it

- Exploitation may involve:
  - Moving files to a target machine
  - Taking files from a target machine
  - Sniffing network data in the target network
  - Install software in target machine
  - Using one vulnerable machine to compromise whole network

- Acts as Proof of Exploitation (PoE), to be mentioned in the penetration testing report

Exploitation Risks

- Exploiting target machines does bring some significant risks which must be carefully discussed with the target organization

- Exploitation risks involve:
  - Service Crash
  - System Crash
  - Severe impact on system stability
  - Data exposure

Types of Exploitation

- Server Side Exploits
  - Attacking a service which is listening on the network by generating and sending exploitation packets
  - User interaction on the target machine is not required
- Client Side Exploits
  - Attacking a client application that fetches content from a server machine
  - Requires user interaction to actively pull content from the machine
- Local Privilege Escalation
  - Attacking the local machine with limited privileges to jump to higher privileges on the machine such as root, admin
  - May or may not require user interaction

PenTest Reports

- Executive Summary
- Test Methodology
- Findings
  - High Risks
  - Medium Risks
- Conclusions
- Remediations