



TYPES OF PENTESTS

WHITE BOX

Definition – Pentesting done with the full knowledge of an organization's infrastructure to be tested including network diagrams, IP Addressing, and even source code. This pentest is done with cooperation from IT administration and staff.

Type of Results – Gives quick results on services or platforms of concern.

Pros – There is low disruption or no disruption in service, and this pentesting focuses only on critical systems.

Cons – This type of pentesting does not test the current IT staff's or department's response to real hacker penetration, nor its incidence response policy, if any.

BLACK BOX

Definition – Pentesting done without any prior knowledge of an organization's security infrastructure.

Type of Results – Gives an outside attacker's point of view of the organization's security. It tests the level of security that is in place, where an outside hacker to penetrate into critical systems.

Pros – It is a better simulation of a real attack event. This testing allows organization to find out how its IT department, staff, and

DEEDOC MANAGED SECURITY SERVICES (DMSS)

Penetration Testing



Do you really know that your sensitive data is secure? Even the best applications and web developers accidentally may be not aware of the latest secure coding practices. There is no application that is 100% bullet-proof against vulnerability exploitation. Is your banking application safe from SQL-injection? Can your enterprise-wide application be crashed by a hacker with no prior knowledge of the application? Is the customer database, which contains personal identifiable information, secured from tampering and manipulation? There are many questions in the minds of banking directors, non-profit organization, and private businesses on these issues. One way to find out for your firm is to go through penetration testing (pentest, for short). DeeDoc Consulting offers penetration testing services to simulate what a hacker would do, and to test whether your firm is ready for hacking, intrusion, and even denial of service attacks.

Penetration testing, or pentesting, is the procedure of examining a computer system, a network, or a web application to verify if it is vulnerable to unauthorized access or other malicious activity. From the single web application layer to the holistic enterprise network, penetration tests are designed to analyze many components of a computer system. The process of penetration testing uses the same process and methodology used by real hackers that helps determine the actual weaknesses an attacker would exploit in order to compromise the system and access protected data. The main objective of penetration testing is to give an organization a clear view of how its systems are vulnerable to potential attacks. DeeDoc Consulting offers several types of penetration testing that include internal, white box, black box, and red box pentesting.

Internal penetration testing is the type of test that mimics an attack originating from inside a company's network. Generally speaking, an internal hack or intrusion originates from inside security perimeter, perhaps from a disgruntled employee, a former employee with access rights, an unauthorized visitor, or an external hacker who manages to

get into the internal network through wireless access or through successful external penetration test. The majority of hacking and data compromise occurs from within the organization, which is why DeeDoc Consulting provides internal penetration testing.

An external penetration test is the direct opposite of internal penetration test. An external penetration test is a test that mimics the first phase of an external hacker's methodology to hacking. Before a network can be hacked into, a vulnerability scan is done to find any open holes and windows. Then the hacker attempts to "penetrate" into the organization's internal network until successful. Once in, the hacker fulfills his/her objective whether it is to delete, corrupt, steal, and modify sensitive data. The external penetration test examines the external IT systems such as firewalls, web servers, online banking servers, web applications, email servers, and other externally available services for any weakness that could be used by a hacker to disrupt the confidentiality, integrity, and availability of the network.



Service Features and Benefits

security policy would react to a real cyber attack, and how fast.

Pros – This pentest takes more time, unlike the white box pentest, and may lead to real time disruption of business processes, and services.

WHITE BOX

Definition – Pentesting done with the full knowledge of an organization's infrastructure to be tested including network diagrams, IP Addressing, and even source code. This pentest is done with cooperation from IT administration and staff.

Type of Results – Gives quick results on services or platforms of concern.

Pros – There is low disruption or no disruption in service, and this pentesting focuses only on critical systems.

Cons – This type of pentesting does not test the current IT staff's or department's response to real hacker penetration, nor its incidence response policy, if any.

For more information on any of our products or services please visit us on the Web at:
<http://www.deedoc.com>



DeeDoc Consulting's Internal Penetration Test follows best practices methodology and includes the following:

- ✓ scoping and rules of engagement
- ✓ network mapping (internal network scanning, systems fingerprinting, services probing)
- ✓ identification and analysis of attack vectors
- ✓ exploit testing and penetration attacking (vulnerability attack, exploitation of configuration flaws, authentication attacks)
- ✓ immediate notification of critical risks

A company's internal network (server, workstations, etc) is exposed to threats such as external intruders breaching firewalls or malicious insiders attempting to access or damage sensitive information and IT resources. Within a 12-month period, a company on average could lose more than 100 million personal and sensitive records due to security breaches.

Figure 1: The Pentest Process



Business Benefits of Pentesting

- ✓ Avoid network downtime caused by security breach
- ✓ Helps organizations understand their level of security
- ✓ Provide an efficient way to evaluate the effectiveness of security controls and countermeasures

IT Benefits of Pentesting

- ✓ Demonstrate the feasibility of an attack and its impact without incurring risk
- ✓ Help evaluate and reinforce an IT staff's readiness for a real-time hacking attack

OTHER AVAILABLE SERVICES

- Policy Drafting
- ISO Compliance
- PCI-DSS Compliance
- Intrusion Prevention (IPS)
- Enterprise Security Training
- Network Mitigation

Siège mondial

1307 E. Millbrook Rd.
Ste C-106
Raleigh, NC 27609
Tel: 1.919.876.4000
Fax: 1.270.568.8907

Afrique

106A Eti-Osa Way
Dolphin Estate
Lagos, Nigeria
Tel: 234.1.873.0931

Amérique du Nord

3315 Guess Rd.
Ste 6
Durham, NC 27705
Tel: 1.919.479.5588

support@deedoc.com
<http://www.deedoc.com>