Penetration Testing

"Let us find your vulnerabilities before anyone else does."

A Penetration Test or Vulnerability Assessment is used to discover what an unauthorised individual(s) may be able to achieve when targeting your computer systems. Motives to attack you are numerous and include extortion, theft, or denying you the use of your system. The common denominator is a vulnerability which can be exploited. Let us find your vulnerabilities before anybody else does. It is imperative that your network is periodically tested by an authorised team to identify how an attacker would achieve their goals and allow us to recommend ways to mitigate the threats presented.

Computer Network Defence (CND)

CND is a leading Information Security Consultancy, offering a broad range of services from detecting eavesdropping devices to securing entire enterprises. Founded in 2004, CND have rapidly gained utmost respect within Government and Defence. This is largely due to the experience and knowledge gained over decades of experience working within the Information Security world. CND's consultants have the highest level of Security Clearance and all are Subject Matter Experts within the information security field. CND is ideally situated to perform a Penetration Test tailored to meet your needs and to offer expert advice and assistance in mitigating any threats that are identified.

Terminology : Penetration Test vs Vulnerability Assessment

The term Penetration Test (Pen Test) is often misused and as a result many clients request a Pen Test when they actually require a Vulnerability Assessment.

A Vulnerability Assessment is the identification of security vulnerabilities, or potential avenues of attack which could be exploited.

A Penetration Test will extend this and attempt to actually exploit the detected vulnerabilities. Many of the apparent vulnerabilities are not exploitable. The tools and techniques used to find the vulnerabilities may have given false readings, or other factors, such as configuration, security applications or hardening prevent or mitigate the possible exploitation of a vulnerability.

- A Penetration Test will encompass a Vulnerability Assessment, however, a Vulnerability Assessment will not include a Penetration Test
- A Vulnerability Assessment is cheaper than a Penetration Test
- A Penetration Test is more accurate than a Vulnerability Assessment
- A Penetration Test carries more risk than a Vulnerability Assessment
- A Vulnerability Assessment can be mostly automated

In order to align with our competitors, Computer Network Defence Ltd, will use the term "Penetration Test" to cover both Pen Tests and Vulnerability Assessments. The Pen Test scope, created with you the client, will identify if vulnerability exploitation will occur, or you can choose which vulnerabilities you wish to be tested for exploitation, this will give the client the best of both worlds.

Scope:

We will work with the client to establish the scope of the Pen Test, this outlines the parameters of the test and defines exactly what needs to be tested and to what level the tests should be conducted, what constraints should in place and how the test will be conducted. The Pen Test scope will also notify the tester about what must not be tested.

Continued..

Contact : CND Ltd, 1 Queen Square, Bath, BA1 2HA

Email: Enquiries@CNDLtd.com

Telephone: 01225 811 806

Website: www.CNDLtd.com

Reconnaissance:

This involves passive and active discovery of your visible network assets, this will also allow us to confirm the scope of the Pen Test

Level 1 - External penetration testing (anonymous hacker)

Establish whether unauthorised network access can be gained via the external network interfaces by a hacker who has limited and/or no previous knowledge of your network.

Level 2 - External penetration testing (supplier/customer level access)

Establish whether unauthorised network access can be gained, via external network components by a hacker who has the same level of access as your customers and suppliers, to the target production environment and other key systems.

Level 3 - External penetration testing (user level access)

Establish whether unauthorised logical access or privilege escalation can be gained, via external network components by an external registered website user.

Level 4 - Internal penetration testing (unauthorised user)

Ascertain whether unauthorised access can be gained via internal penetration and audit testing of your systems by exploiting weaknesses in your networks services and resources.
Determine whether it is possible to manipulate key controls implemented for the protection of your system(s).
Assess whether existing procedures for responding to such a breach of security are adequate and effective.
Assess the security of certain sensitive servers and workstations.

Level 5 – Firewall and security systems review

Analyse the effectiveness of the policies employed by your firewalls and the infrastructure in place for administration.
Review the operating system configuration for a secure implementation. (system hardening and patch management)
Review your procedures and processes for monitoring and reporting of incidents on the firewall.
Review network and host security components for example, IDS.

Level 6 – Defence in depth and the weakest link

Assess the system for any gaps in the security mitigation controls
Identify and prioritise the “weakest links” which may be possible attack vectors
Identify missing security technology which could provide defence in depth within the network.

Periodic Testing and/or Automated Scanning

The Pen Test is a snapshot of known vulnerabilities identified on the day of the test. In addition to periodic manual scans, CND offer a regular automated scan of the network in the weeks and months following a Pen Test. The automated scan could never replace the quality of a Manual Pen Test. However, it will identify new vulnerabilities, backdoors and miss-configured systems, giving the client peace of mind that they are not exposed to new emerging threats.

The standard package is a weekly out of hours scan, the report is emailed to the client. Once per month an irregular scan is performed, this is analysed by CND and the client is briefed on any salient points.

The Risk

There is a small risk of outages when undergoing a Pen Test and whilst we do all we can to minimise these risks, they remain present. It is highly recommended that systems are fully backed up prior to the Pen Test commencing. It should also be considered, that if an authorised Pen Test causes an outage, then an attacker could do the same when you least expect it, an authorised Pen Tester would also be able to shed some light on what might have caused the outage. The riskier elements, or indeed the entire Pen Test can be performed out of hours, in the evening or weekends if required.

Reporting

A Pen Test always culminates in an understandable report detailing findings and what can be done to mitigate any identified vulnerabilities.

What next?

For more information on Computer Network Defence, our Penetration Testing and Vulnerability Assement packages or an initial consultation please call us on 01225 811 806 or email enquiries@CNDLtd.com and we will put together a tailored proposal in line with your network/business needs and requirements.

Contact : CND Ltd, 1 Queen Square, Bath, BA1 2HA

Email: Enquiries@CNDLtd.com

Telephone: 01225 811 806

Website: www.CNDLtd.com