The Context of Ethical Hacking in Network Security and Business protection

What is Ethical Hacking?

Ethical hacking involves computer and network professionals who use their expertise to safeguard the networks of an organization on behalf of its owners. In order to test a security system, they seek vulnerabilities that a malicious hacker could exploit. Ethical hacking is also known as penetration testing, intrusion testing, and red teaming. An ethical hacker is sometimes called a white hat while the other one is called black hat. Ethical hackers collect and assess information on issues like loopholes which are truly a security threat, the depth to which a hacker can get into via one of these holes and the patching requirements in order of priority.

The ethical hacker aims to help the organization take anticipatory measures against malicious attacks by attacking the system himself; all the while staying within legal limits. The most important point is that an Ethical Hacker has authorization to probe the target. The reason is that as technology advances and organizations depend on technology increasingly, information assets have evolved into critical components of survival and need to be protected at any cost.

In Contrast - Malicious Hacking

For a further probe into ethical hacking, let us understand what hacking is. Hacking is basically unauthorized use of computer and network resources. Hackers make use of malicious codes which in effect are software programs, particularly keyloggers, Trojans, malware and other spyware, in gaining entry into an organization's network for stealing vital information. For instance, famed hacker Kevin Mitnick used a Trojan horse written by the West German Chaos Gang to gain access to hundreds of systems. Financial gain is the motive behind most hacking activities unlike in the past where hackers were motivated by fame and show off value of their programming skills.

The damage caused by hacking is extensive, particularly in a corporate environment where the economic repercussions can be enormous such as Identity theft, Loss of confidential user data, Loss of productivity, Use of corporate network resources: bandwidth abuse, mail flooding and tarnishing the consumer's trust in the brand. Mostly the information elicited is used in carrying out unauthorized transactions using credit or debit card numbers, selling user's personal information such as phone numbers, address, account numbers etc., to others and ruining the customer's trust in the services provided by the bank and maligning the brand name and for a price.

Need for Ethical Hacking

As network security assumes significance for businesses and investment in security infrastructure grows by the day, the need to validate the knowledge and skills of network security professionals has also grown proportionately. If hacking involves creativity and lateral thinking, then vulnerability testing and security audits will not ensure a foolproof network security of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and estimate the security posture for vulnerabilities and exposure.

The Trend of Certified Hacker Programmes CHP

In the present times, where network security assumes utmost importance for businesses around the globe, teaching "hacking" as a legitimate means of training students in how to protect a future employer's data assets has been introduced into courses with increasing frequency. So much so that leading companies and institutions like, Cisco Corporation, Novell, Canon, Hewlett Packard, US Air Force Reserve, US Embassy, Microsoft Corporation, UK Ministry of Defense, US Department of Defense, University of Memphis are offering courses in Ethical Hacking and training professionals to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker.

Scope and Limitations of Ethical Hacking

Ethical hacking is a crucial component of risk assessment, audit, counterfraud, best practice and good governance. Ethical hacking is used to identify risks and highlight remedial actions and also reduces ICT costs by resolving those vulnerabilities. However, unless the businesses first know what it is at that they are looking for and why they are hiring an outside vendor to hack systems in the first place, chances are there wouldn't be much gain out of the experience. Ethical hacker thus can only help the organization to better understand their security system, but it's up to the organization to place the right guards on the network.

Unified Threat Management Security: Combating Attacks by a Malicious Hacker

Hackers are increasingly using blended software programs that combine the characteristics of viruses, worms, Trojan Horses, and malicious code that can very easily dodge point solutions, firewalls, and other traditional technology defenses. Blocked at one entry point, an application may simply enter unnoticed through other points.
Ethical hackers help organizations understand the present hidden problems in their servers and corporate network. But it is important that while ethical hackers carry out the task of penetration testing, organizations imperatively need to put results into a business context.

Ethical hackers help organizations understand the present hidden problems in their servers and corporate network. But it is important that while ethical hackers carry out the task of penetration testing, organizations imperatively need to put results into a business context.

This can only be done using the Unified Threat Management approach which provides broad network protection by combining multiple security features—firewall, anti-virus, anti-spam, intrusion prevention system, and content control and filtering—on a single hardware platform. UTMs employ an inbuilt system that regularly updates the solution staying a step ahead of threats to the network. With the rise in zero-day attacks, there is a need for real-time security solution.

Businesses can no longer rely only on signature-based technology. There is a need for powerful gateway level security, which stops threats at their very entry point. Also, to fight against a hacker's use of blended threats, which enter though multiple modes, there is a need of Unified Security solution, which has all the needed security features to curb threats.

UTMs like Cyberoam provide comprehensive protection with its tightly integrated multiple security features working together on a single appliance. The tight integration and interoperability among various features on the UTM equips it uniquely to fight blended threats that a hacker employs at attacking networks, completely protecting the databases and other resources of the organization.