PECB

When Recognition Matters

NETWORK SECURITY AND SPOOFING ATTACKS

Nowadays it is very common to hear from people that internet network is the largest engineering system, and something that we cannot imagine life without. That is the reason why modern life activities became completely centered around or driven by the internet applications, and so many people are taking advantage of opportunities presented by internet. This created a huge demand for software designers and network engineers with skills in creating new internet-enabled applications or porting existing/legacy applications to the internet platform. We are constantly seeking for the best applications, so we can perform with different, fast, reliable, attractive and most important secure tasks.

So to achieve security there are some methods which protect and analyze network traffic. Very important role in this issue have software programs, which are designed to control, analyze and filter packets that carry our very important data. However, while these programs are used for positive purposes, they are also used for actions which may cause network hazards and attacks.

One of the biggest attacks is Spoofing. Very familiar word, but what is in fact spoofing? And who uses it?

Spoofing

In the computer world, spoofing refers to stolen identity, when a person pretense as another individual, organization or business with the purpose of gaining access to sensitive personal information including user names and passwords, bank account information, and credit card numbers. Spoofing is both part of the setup for phishing as well as a technique to gain direct access to an individual or organization's computer or computer network. There are some known spoofing types such as: IP spoofing, URL spoofing, Email spoofing, DNS spoofing, and MAC spoofing.

IP spoofing

IP spoofing is the act of manipulated headers of the IP datagram in a transmitted message, this to cover hackers true identity so that the message could appear as though it is from a trusted source. The IP protocol specifies no method for validating the authenticity of the packet's source. This implies that the attacker could forge the source address to become whoever they desire.

How is this possible? If we look an IP datagram we can see that an IP header contains information about the packet, inside these datagram are saved sources and destination IP addresses. Using several tools an attacker can easily modify these addresses – specifically the "source address" field.

URL spoofing

This spoofing attack occurs when one false website poses like a real one. This is caused because the URL of the site in fact is not the real one, therefore, the information is sent to a hidden web address. This attack is used to direct users to leave their username and password, so the attacker can use them later.

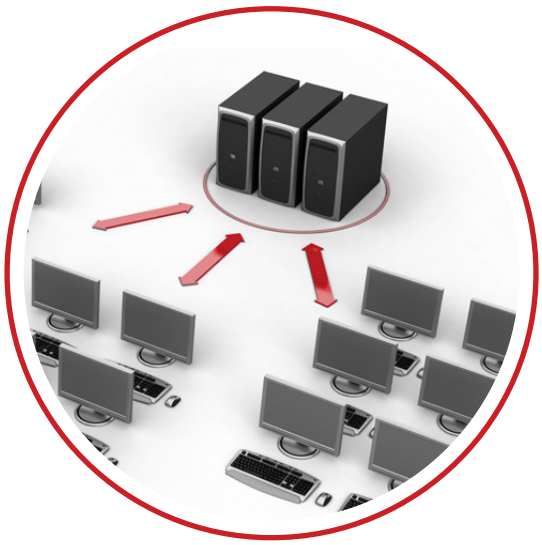
Usually, the attacker collects the username and password then displays a password error message and directs the user to the legitimate site. Using this technique the hacker could create a series of fake websites and steal user's private information without noticing.The solution to this attack is by the fact that security patches are released from the web browsers which add features of revealing the "true" URL of a site in the web browser.

Email spoofing

It is very common to receive different emails in our email account originating from people that in fact are not truly sent by the real e-mail sender who appears on header of email. This action is called Email spoofing.

Attacks that usually are caused from IP spoofing are known to confuse or discredit persons, Social Engineering, phishing etc. Some ways to be protected by email spoofing are: checking the content and form of the received emails, pay attention to the sender of the received email, ask yourself if this email was expected or need to be confirmed, update and login any kind of information, check the header of the email, etc.

DNS spoofing



One of the most important features of internet network systems is the ability to map human readable web addresses into numerical IP addresses. Thanks to this, we do not have to remember IP address like numbers. Who would be capable of remembering all IP addresses of web pages that we visit. Such mapping is done by a server called Domain Name Server DNS. All over the world there are some public and private DNS servers, which are configured by different operators/companies for taking care of mapping for different parts of networks.

Spoofing comes into scenario if an intruder causes DNS to return an incorrect IP address, diverting traffic to intruder's computer. Then the intruder will use the received information for different purpose.

MAC spoofing

All devices connected to a network have a MAC (media access control) address. A MAC address is always required in order to connect with a network services to enhance security connection. Despite the fact that MAC address is hard-coded on a network interface controller (NIC) and cannot be changed, there are some tools which can make MAC address to look different. This of course is done in order to cause the receiver to send the response to the spoofing party.

What is the solution?

To achieve spoofing there are lots of spoofing software that assist scammers to pretense of being someone or something that they are not. But understanding how spoofing software works can help people understand how to avoid being scammed. Different software play an important role here, they help us monitor network and detect spoofing.

Everyone with basic skills of networking can use software like Wireshark, Network Monitor, Colaspoft, etc., which collect the entire data passing to and from the monitored machines that we work on. With these kinds of software we can look at conversations and find out the source and destination of the IP addresses and understand the particular packets and the data inside. Moreover, as long as you understand the role of specific network protocols, packets meaning can be decoded and seen what is written there. But be careful! Always use them just for a good purpose.

Today network security is one of the biggest topics in network platform. In fact every day we face up with new inventions, publications, and different applications that claim different ways to achieve secure transmission of data in networks. It is not very uncommon to hear and read that the trend of security enhancement has been improved in the same scale as has improved different methods of network threading. In fact most of the job done in network security platform is kind of an answer to "bad guys" that use their knowledge to have unauthorized access, and attack network for different reasons.

Furthermore, these advanced attacks on network security over the past years led to many compromises and breaches on the data security. However, solutions are always available it only requires actions from company officers and administrations. Moreover, these network security solutions should be part of continuing involvement on the highest level of organizational management in its design, plan and implementation. And network security compliances should become part of daily responsibilities, and certified personnel is more than needed, not just for IT sector but in wider range of employees who are involved and influenced by network security in general and spoofing attacks in particular.

Professional Evaluation and Certification Board (PECB) is a personnel certification body on a wide range of professional standards. It offers ISO 27001, ISO 27005, ISO 29100 and ISO 20000 training and certification services for professionals wanting to support organizations on the implementation of these management systems. ISO Standards and Professional Trainings offered by PECB:

- Certified Lead Implementer (5 days)
- Certified Lead Auditor (5 days)
- Certified Foundation (2 days)
- ISO Introduction (1 day)

Lead Auditor, Lead Implementer and Master are certification schemes accredited by ANSI ISO/IEC 17024.

Rreze Halili is the Security, Continuity, and Recovery (SCR) Product Manager at PECB. She is in charge of developing and maintaining training courses related to SCR. If you have any questions, please do not hesitate to contact: scr@pecb.com.

For further information, please visit http://pecb.com/site/renderPage?param=139