Spoofing essay sample

Business, Company

consequences and how to defend against it

Our world changes on a rapid speed and new dangers come with it. As humanity starts to use a computer on a regular basis for almost every aspect of life like pleasure, communication shopping and exploring new dangers appeared. Nowadays we have plenty of things our ancestors have no clue, like internet, cellphones, computer viruses and spoofing.

Spoofing is the name for an attack when one party pretends to be someone else. The most common spoofing attacks are MAC-spoofing, ARP-spoofing, IP-spoofing, DNS-spoofing and e-mail spoofing. Let’s take a look at each one of them.

MAC- spoofing is the link attack. On the network card MAC- address changes, which causes the router to send the port , hacked by attacker, packets that were not available for him before. ARP-spoofing is an attack that abuses weak spots of the ARP protocol. It allows to place in the victim’s ARP- cache false record about matching IP – address if another victim to attackers MAC-address.

IP-spoofing attack is the most common spoofing. This is an attack where the source port number is modified in order to mislead the NAT and firewalls, as well as to hide its presence on the network. Firewalls are not serviced properly can use outdated rules under which can be open certain ports on the nodes with known IP-addresses. This attack uses this fact. This may lead to crash of the server make it unresponsive to any requests. Luckily, modern software security systems can identify denial-of-service attacks and ban their transmissions. (“ Spoofing” n. d.)

DNS-spoofing is based on the infection of victim’s cache DNS- server with

false information about matching of DNS- name of the trusted host and attackers IP- address .

This attack is also known as DNS poisoning, and it leads to more serious consequences. In this case, the domain name server is exposed. It is going to cause alter entries of domain names to reflect the attackers' IP address. This leads to the fact that Web and email traffic is sent to the site of the attacker. This attack is carried out by creating multiple packages modified IP- address, port, and service type fields in order to achieve a goal. Consequences of this attack can be very disastrous. For example, website can be defaced, or e-mail information may be stolen. (Phatak. P. 2011)

E-MAIL spoofing is an attack when attacker fabricates an e-mail header, so it appears that the message was send by someone other than the real source. Spam spreaders often take advantage of spoofing in order to get recipients to open or even reply to, their solicitations. (" email spoofing" n. d.)

Although the attack based on spoofing packets is difficult to restrain, there are a number of preventive measures .

Deploying modern firewall and its enhanced ability to fight spoofed packets can be the first line of defense.

Free Linux based systems come with built in option called source address verification. This kernel feature once turned on allows you to drop packets that look like came from the internal network, but in fact did not.

" Hosts. conf" file modification and adding " nospoof on" is another level of protection, which one can try to apply.

In terms of determining the presence of the attack for small networks based on Linux, there is a great utility called " arpwatch", which is very useful. It

monitors IP and MAC-addresses, records all changes and can be used with scripts.

Looking for the MAC address cloning may anti ARP spoof attack. However? there is also the legal cloning of MAC address . There was MAC cloning if we have two or more IP address is returned. (“ Anti ARP spoofing” n. d.)

Attacks based on spoofing packets are attacks that are difficult to neutralize. They can lead to serious data loss while there are ways to identify and prevent these attacks. So in spoofing protection the most significant steps are configuring firewalls, routers and switches. Installation of IPS devices without a doubt helps to control IT network. . (Phatak. P. 2011)We need to protect ourselves and our date as who own the information owns the world.

References

CCGetMAC. (n. d.). Anti ARP spoofing to protect your network. Retrieved from: http://www. youngzsoft. net/cc-get-mac-address/anti. htm

Phatak, P. (2011). Cyber Attacks Explained: Packet Spoofing. Linux for you. Retrieved from: http://www. linuxforu. com/2011/12/cyber-attacks-explained-packet-spoofing/

Spoofing. (n. d.). TechTerm. com. Retrieved from http://www. techterms. com/definition/spoofing