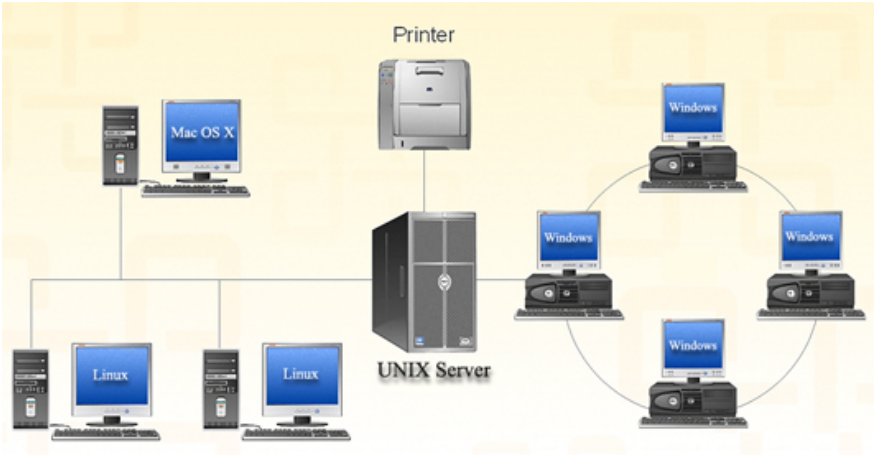
Secure multi-platform network system

Today, networks increasingly contain many different types of computers (including many types of hardware, software and operating systems) that are no longer new.

***Network Administration* - Today, networks increasingly contain many different types of computers (including many types of hardware, software and operating systems) that are no longer new.**

Net networks are becoming less and less common, many companies have used Windows domains for UNIX Web servers, accessed by Windows, Linux and Mac operating systems.

In addition, there are many types of smart phones (such as Windows Mobile, iPhone, Android, Symbian, etc.) that need to download mail or access other resources on the network. In those cases we will face many difficulties in securing the network. In this article we will plan to secure this multi-platform network.



Common multi-platform network model.

Security difficulties in multi-platform networks

For systems that use multiple operating systems to work stably is not a simple task. Therefore, what is often focused on cross-platform networking is not security, but how this network can operate. Multi-platform sharing becomes the main goal, the restrictions for sharing are often forgotten or removed.

Most administrators are trained to administer a specific type of system (Windows, UNIX, Mainframe, .). While security is a sensitive area, we need not only administrators to configure and manage many different types of systems on the network, but also those who are trained in security systems. This different operator. They need basic knowledge of security and are trained by providers. So we can fully exploit the integrated security mechanism of the operating system, and know when it is appropriate to use third-party tools.

The results obtained depend in part on security habits. If an administrator has to memorize many different operations and methods for each device type, there are always certain risks that lead to a weak network. That's why mixed network systems need to be managed by many dedicated employees for each different type of system, however, in fact very few companies pay attention to this point, and evidence is that they often use very little, even a single employee to do network administration.

Statistics of network components

In many IT environments, network systems are not planned specifically, but are usually spontaneous systems when in need, resulting in the purchase and deployment of new computers that do not follow a set of rules. any order The first rule to comply with network security is to know what we have, so the network hardware and software inventory process cannot be ignored. There are countless tools to help detect and provide information about network components. Most important is to use a tool that can support all operating systems in the network.

Often overlooked (non-secure) platforms include operating systems that run on laptops and phones that do not often connect to the network, as well as operating systems that operate on virtual machines. Computer A may be using Windows as the main operating system, but if that computer contains a Linux virtual machine, we will have to treat the virtual operating system as another computer on the network and apply security measures. Secret suite. Similarly, remember that many Mac and Linux users also use Windows on a virtualized environment to run Windows-only applications. In addition, we can also use computers with multiple operating systems, especially in test and development environments.

A statistic must include all the hardware and all software running on the network even though some devices do not often connect to the network.

Update and / or upgrade

No matter which system or platform is used, there is no guarantee that the system is inviolable.

Usually when referring to Windows, users often consider this as the 'weakest' system and other systems are 'safe'. But the truth is not so, it is only because the Windows operating system is used by many users so this is the most attractive 'bait' to hackers. Typically, in the case of Linux, last year a kernel vulnerability was discovered on most Linux versions that allowed hackers to completely control the system. Last year, Apple had to release a patch of 67 security vulnerabilities in Mac OS X and the Safari browser application, not to mention a vulnerable Java vulnerability.

Therefore, it is not only necessary to use Windows updates but also need to pay attention to updates of UNIX / Linux and Mac when they are released.

Another important factor to consider is that in most cases, the new operating system versions are always more secure than previous versions, even though they are completely patched. For example, Windows 7 and Windows Vista integrate some security mechanisms such as UAC, IE security mode, BitLocker drive encryption tool, etc. that Windows XP does not have. The latest version of Mac OS X integrates malware detection tool. The latest version of OpenSUSE supports TPM technology (Trusted Platform Module). In many cases, upgrading to a new version of any operating system also enhances security.

The same is true for mobile operating systems. For example, the new iPhone series incorporates stronger security features, such as strong password support using alphabetic characters, numbers and symbolic characters, and the ability to delete remote data that sessions Original iPhone version is not integrated.

Note: *The iPhone series still has some security issues in the enterprise environment, because it can only deploy existing Exchange and iTunes security policies that are preinstalled.*

These multi-platform network security fundamentals

Here are some guidelines to take into account when applying security measures to multi-platform networks:

1. Secure devices at the edge with a reliable firewall system, and an intrusion detection / prevention system.

2. Use anti-virus and anti-malware software (on every system) and update regularly.

3. Implement security monitoring / verification tool to detect arising vulnerabilities.

4. Turn off unnecessary services to reinforce the system.

5. Close unused ports.

6. Limit physical access to the system.

7. Only assign administrative access to users who really need it. On UNIX systems, limit root access rights to endpoint security.

8. Deploy file-level licenses. On UNIX systems, partition the file system and use read-only partitions to store infrequently updated data, and use ACL (Access Control List) for the administration process. Complex license logic.

9. On UNIX systems, limit the access processes on the system file with the ulimit and chroot commands.

10. Deploy using strong password policies.

11. In strong security environments, two-factor authentication should be applied.

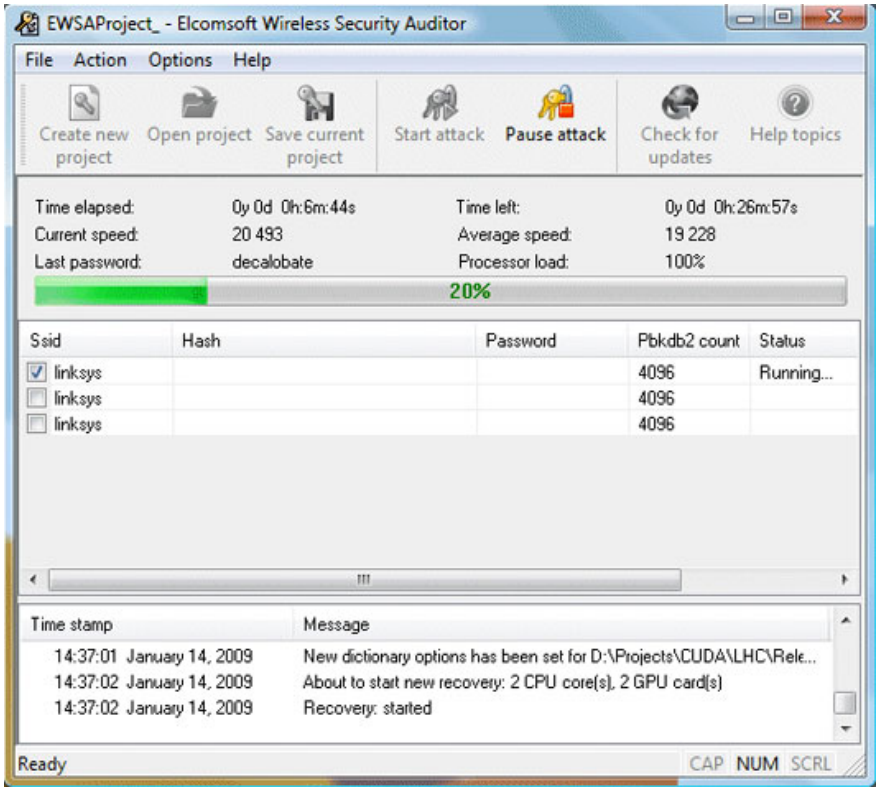
12. On UNIX systems, use SSH (Secure Shell) for remote access by command.

13. Use encryption tools to protect the drive, protect data over the network, protect the operating system from unauthorized access.

14. Deploy a Public Key structure to issue digital licenses.

Use security assessment tools

A third-party security assessment tool is useful in evaluating and guiding while deploying security measures in a complex network, especially it is much more useful in cross-platform networks. A company that uses security assessment tools for network systems will help employees easily check many different types of systems to find the weaknesses and remedies that system administrators can't control all. .



Wifi EWSAProject security verification tool.

These tools can carry out penetration tests to detect vulnerability and suggest an optimal solution to overcome.

Conclude

Multi-platform networking has always had a lot of security issues, however, these networks are becoming more and more popular, so knowing this network's security principles will help the administrator's work. Membership is done smoothly. Keep in mind that the basic security principles need to apply to all platforms, but need to have a separate application method on each different operating system.

You finished reading the article "**Secure multi-platform network system**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.