A. S. TERGEUSIZOVA, A. J. TOIGOJINOVA

(Almaty University of Power Engineering & Telecommunications, Almaty, Republic of Kazakhstan)

ROUTER SECURITY ISSUES

Annotation. A key task in securing a network is to secure the routers. Routers are the gateway into the network and are obvious targets. Basic administrative talks including good physical security, maintaining updated IOS and backing up configuration files are a start. Cisco IOS software provides a wealth of security features to harden routers and close doors opened by used ports and services, most of which can be completed using the one-step lockdown feature of Cisco SDM.

Keywords: network security, router security, gateway, cisco router, router security issues, router are targets.

Тірек сөздер: желі қауіпсіздігі, маршрутизатор қауіпсіздігі, шлюз, cisco маршрутизаторы, маршрути-затор қауіпсіздігіне қатысты сұрақтар, маршрутизатор нысана ретінде.

Ключевые слова: сетевая безопасность, безопасность маршрутизаторов, шлюз, маршрутизатор cisco, вопросы безопасности маршрутизатора, маршрутизатор в качестве мишени.

The Role of Routers in Network Security

You know that you can build a LAN by connecting devices with basic Layer 2 LAN switches. You can then use a router to route traffic between different networks based on Layer 3 IP addresses.

Router security is a critical element in any security deployment. Routers are definite targets for network attackers. If an attacker can compromise and access a router, it can be a potential aid to them. Knowing the roles that routers fulfill in the network helps you understand their vulnerabilities.

Routers fulfill the following roles:

– Advertise networks and filter who can use them.

– Provide access to network segments and subnetworks.

Routers are Targets

Because routers provide gateways to other networks, they are obvious targets, and are subject to a variety of attacks. Here are some examples of various security problems:

– Compromising the access control can expose network configuration details, thereby facilitating attacks against other network components.

– Compromising the route tables can reduce performance, deny network communication services, and expose sensitive data.

– Misconfiguring a router traffic filter can expose internal network components to scans and attacks, making it easier for attackers to avoid detection.

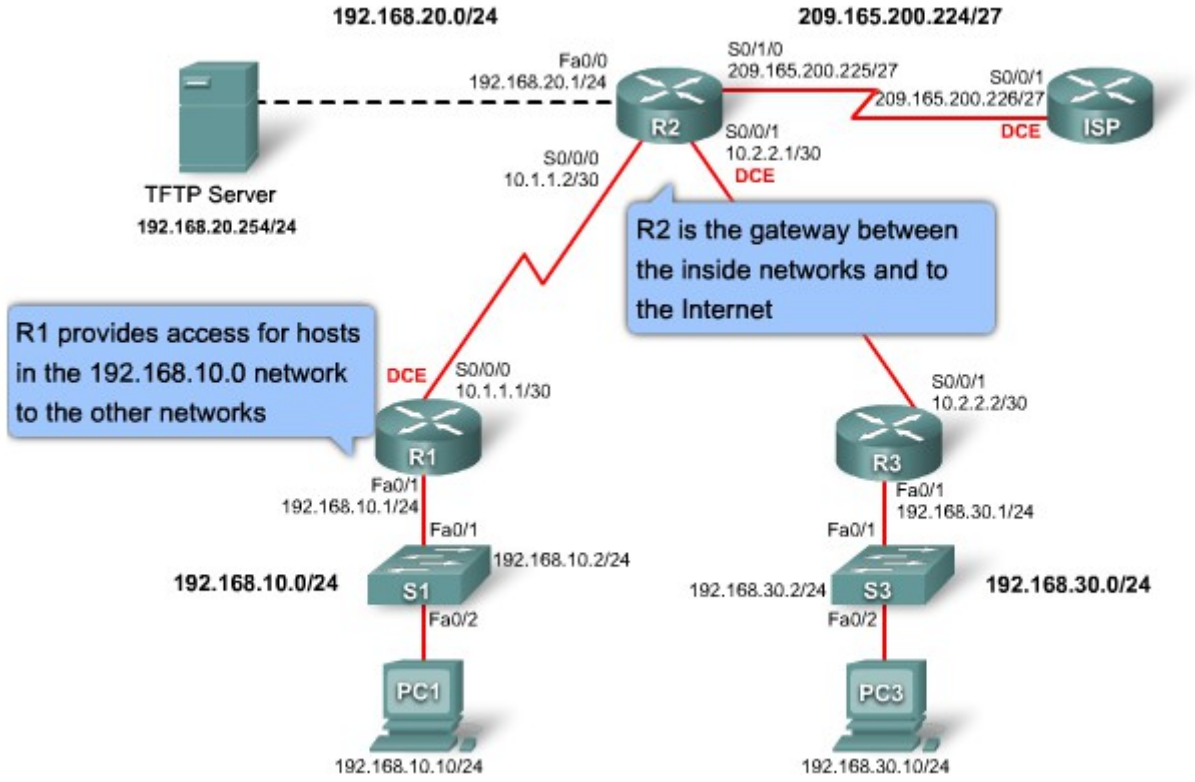

Figure 1 – The Role of Routers in Network Security

Attackers can compromise routers in different ways, so there is no single approach that network administrators can use to combat them. The ways that routers are compromised are

similar to the types of attacks you learned about earlier in this chapter, including trust exploitation attacks, IP spoofing, session hijacking, and MITM attacks.

Securing Your Network

Securing routers at the network perimeter is an important first step in securing the network.

Think about router security in terms in these categories:

– Physical security

– Update the router IOS whenever advisable

– Backup the router configuration and IOS

– Harden the router to eliminate the potential abuse of unused ports and services

To provide physical security, locate the router in a locked room that is accessible only to authorized personnel. It should also be free of any electrostatic or magnetic interference, and have controls for temperature and humidity. To reduce the possibility of DoS due to a power failure, install an uninter-ruptible power supply (UPS) and keep spare components available.

Physical devices used to connect to the router should be stored in a locked facility, or they should remain in the possession of a trustworthy individual so that they are not compromised. A device that is left in the open could have Trojans or some other sort of executable file stored on it.

Provision the router with the maximum amount of memory possible. Availability of memory can help protect against some DoS attacks, while supporting the widest range of security services.

The security features in an operating system evolve over time. However, the latest version of an operating system may not be the most stable version available. To get the best security performance from your operating system, use the latest stable release that meets the feature requirements of your network.

Always have a backup copy of a configuration and IOS on hand in case a router fails. Keep a secure copy of the router operating system image and router configuration file on a TFTP server for backup purposes.

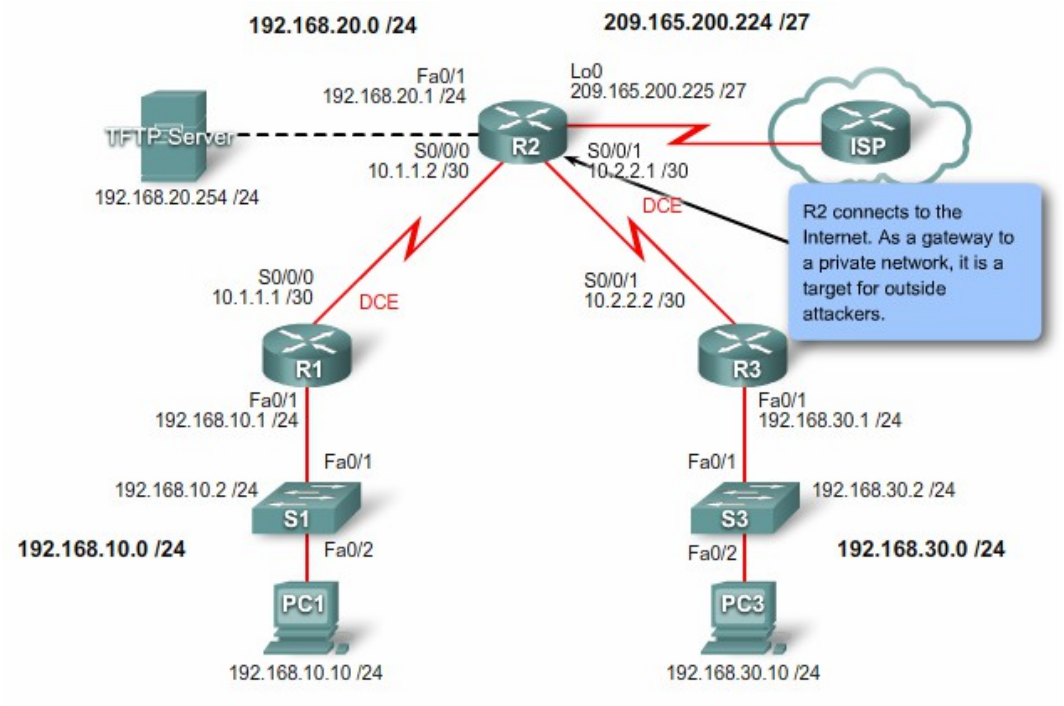

Figure 2 – Routers are Targets

Harden the router to make it as secure as possible. A router has many services enabled by default. Many of these services are unnecessary and may be used by an attacker for information gathering or exploitation. You should harden your router configuration by disabling unnecessary services.

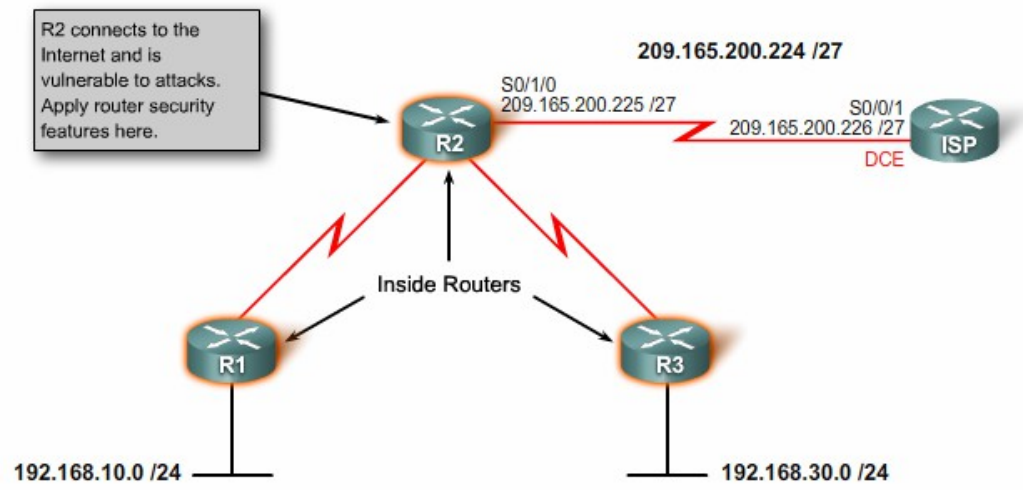

Figure 3 – Securing Your Network

Before you configure security features on a router, you need a plan for all the Cisco IOS security configuration steps [1].

Applying Cisco IOS Security Features to Router

Steps to safeguard a router:

Step 1. Manage router security

Step 2. Secure remote administrative access to routers

Step 3. Logging router activity

Step 4. Secure vulnerable router services and interfaces

Step 5. Secure routing protocols

Step 6. Control and filter network traffic

REFERENCES

1 Official Site Networking Academy Program Cisco (learning portal) http://cisco.netacad.net;

2 http://okitgo.ru/network/razvitie-setej.html

3 Vito Amato. Fundamentals of Networking Cisco. Vol. 1, 2: Corr. Per. from English. Moscow: Publishing house "Williams", 2004.

4 Networking Academy Program Cisco CCNA 1 and 2. Auxiliary guide. 3rd ed. With rev.: Per. from English. M. Williams, 2055. 1168 s.

5 Kulginov M. Networks. The practice of construction. For professionals. 2nd edition. St. Petersburg: Publishing House of the "Peter", 2003.

Резюме

А. С. Тергеусізова, А. Тойғожинова

(Алматы энергетика және байланыс университеті, Алматы, Қазақстан Республикасы)

МАРШРУТИЗАТОРДЫҢ ҚАУІПСІЗДІГІНЕ ҚАТЫСТЫ СҰРАҚТАР

Желі қауіпсіздігін қамтамасыз ету барысындағы негізгі мәселенің бірі болып маршрутизатор қауіпсіз-дігін қамтамасыз ету табылады. Маршрутизатор – желілерді өзара

байланыстыратын негізгі құрылғы. Жақсы-лап ойластырылған қауіпсіздікті жүзеге асыру барысындағы әкімшілік процесіне IOS-ты жаңартуды қолдау және бастапқы конфигурациялық файлдың көшірмесін алып сақтау жатады.

Тірек сөздер: желі қауіпсіздігі, маршрутизатор қауіпсіздігі, шлюз, cisco маршрутизаторы, маршрути-затор қауіпсіздігіне қатысты сұрақтар, маршрутизатор нысана ретінде.

Резюме

А. С. Тергеусизова, А.Тойгожинова

(Алматинский университет энергетики и связи, Алматы, Республика Казахстан)

ВОПРОСЫ БЕЗОПАСНОСТИ МАРШРУТИЗАТОРА

Одна из ключевых задач в обеспечении безопасности сети является обеспечение безопасности марш-рутизаторов. Маршрутизаторы являются первичными устройствами, которые соединяют сети между собой. Основные административные процессы, в том числе хорошо продуманной физической безопасности, это поддержка обновления IOS и резервное копирование файла начальной конфигурации.

Ключевые слова: сетевая безопасность, безопасность маршрутизаторов, шлюз, маршрутизатор cisco, вопросы безопасности маршрутизатора, маршрутизатор в качестве мишени.

Поступила 26.09.2013 г.