MASARYKOVA UNIVERZITA
FAKULTA INFORMATIKY

Security of small office home routers

BACHELOR THESIS

Mária Hatalová

Brno, spring 2015

Declaration

Hereby I declare, that this paper is my original authorial work, which I have worked out by my own. All sources, references and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Advisor: RNDr. Marián Novotný Ph.D.

Acknowledgement

I would like to thank my advisor Marián Novotný for his guidance, valuable advices and feedback on the thesis. I want to express my gratitude to Slovanet and SH systém for lending me devices for testing and I want to thank my colleague Jiří Schäfer for his tips and advices on tools for testing the devices. I am thankful to my uncle Pavol Hatala for allowing me to use his DSL connection to the Internet for the testing and to my family and close friends for their support.

Abstract

The thesis deals with security of Small Office Home (SOHO) routers. It discusses security issues brought up by design and implementation of a typical SOHO router and it describes vulnerabilities and weaknesses that are the most common ones regarding these devices. Attacks on SOHO routers from past few years are analysed to help understand impact of distinct weakness categories. The thesis reviews a set of tools for testing vulnerabilities of SOHO routers and using them together with a proposed methodology it evaluates a sample of devices supplied by Internet Service Providers in Slovakia and Czech Republic.

Keywords

Router, Network, Security, Vulnerability

Contents

1 Introduction 3

2 Security issues of SOHO routers 5

2.1 Misconfiguration of services 6

2.2 Assumption of security on the LAN 7

2.3 Insecure by default 7

2.4 Poor security design and implementation 9

3 Vulnerabilities and security weaknesses 10

3.1 CVE – Common Vulnerabilities and Exposures 10

3.2 CWE – Common Weakness Enumeration 11

3.3 Weaknesses associated with SOHO routers 12

3.3.1 CWE-20: Improper Input Validation 13

3.3.2 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') 14

3.3.3 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 14

3.3.4 CWE-264: Permissions, Privileges, and Access Controls 15

3.3.5 CWE-352: Cross-Site Request Forgery (CSRF) 16

3.4 Attacks on SOHO routers 16

3.4.1 The Moon malware 17

3.4.2 Polish banking attack 17

3.4.3 DNS settings of over 300,000 SOHO routers compromised 18

3.5 Summary of vulnerability categories 18

4 Tools 20

4.1 Nmap 20

4.2 Slowloris 20

4.3 Nikto 21

4.4 w3af 21

4.5 Nessus 22

4.6 Revok 22

4.7 Evaluation of the tools 23

5 Evaluation of SOHO routers supplied by ISPs 24

5.1 Methodology for evaluation 24
5.2 Devices 27
5.2.1 GREENPACKET CPE INDOOR DX350 27
5.2.2 ZyXEL VMG1312-B30B 29
5.2.3 ZyXEL Prestige 660HN-T3A 30
5.2.4 D-Link DSL-2641R 32
5.2.5 D-Link DIR 600 33
5.2.6 ADB VV3212 34
5.2.7 Technicolor TC 7200 35
5.2.8 CISCO EPC 3010 37
5.3 Evaluation results summary 38
5.3.1 Open ports 38
5.3.2 Detected vulnerabilities 39
5.3.3 Problems encountered during testing 40
6 Conclusion 41
7 References 42
A Summary of evaluation of the SOHO routers 45
B Slowloris script 46
C Scan reports 46

1 Introduction

Small Office Home (SOHO) routers are widespread network devices that are used by millions of users all over the world. A SOHO router is typically a single point of ingress to a local home or small office network and although it is called a router, it provides much more functionality then just routing. It serves as a DHCP server, Network Address Translator (NAT), firewall, wireless hotspot, etc. Besides these features it supports multiple services, e.g. HTTP(s), Telnet, FTP and UPnP. The rich service and feature sets come at a significant cost to security and they are source of multiple security issues. Besides the problems that originate in the typical design and implementation of SOHO routers, manufacturers' approach to security has also negative impact. They are trying to make the initial set up and usage of the devices as simple as possible and to reach that they often omit security mechanisms. Besides this, software updates for home routers that would patch found vulnerabilities are not being released often enough and moreover, most end users do not have sufficient technical skills to install them themselves. Security of SOHO routers is often underestimated by both manufacturers and end users and should be paid more attention.

The goal of the thesis is to analyse security risks of SOHO routers and to describe vulnerabilities that are caused by them. Using a proposed methodology and tools the thesis evaluates security of several routers that are supplied by Internet Service Providers (ISP) in Slovakia and Czech Republic.

In the second chapter the security problems of SOHO routers are analysed. According to a technical report published by Independent Security Evaluators (ISE) [1] these problems can be divided into four basic categories and the thesis discusses them all.

The third chapter covers categorization of vulnerabilities of SOHO routers. The categorization in this field is not steady and distinct papers and technical reports on security of home routers use different categories. For the purpose of the thesis categorization according to MITRE Corporation is used [2]. MITRE assigns a unique CWE (Common Weakness Enumeration) identifier to each vulnerability category. The thesis focuses on a few categories that are the most common ones in the field and can have the most serious consequences.

In the fourth chapter security of several SOHO routers is evaluated. All ports of different devices were scanned using the *Nmap* tool from both LAN and WAN side. Resistance to denial of service attack was tested using the

Slowloris tool that floods the device with incomplete HTTP requests and can cause overload of the web server. The web interfaces of the routers were checked for vulnerabilities using the tools *Nikto, w3af*, *Nessus* and *Revok*.

The thesis analyzes security issues originating in the typical design and implementation of SOHO routers. An audit methodology was proposed and it was used together with the chosen tools to evaluate security of several devices. The thesis focuses only on the most common vulnerability categories and in the future it would be contributing to discuss more categories and cover security of SOHO routers from a larger scope.

2 Security issues of SOHO routers

This chapter introduces SOHO routers and describes their role in SOHO networks. Security issues that leverage from design and implementation of a typical SOHO router are discussed and the motivation of attackers to target these devices is presented.

SOHO routers are widespread network devices that are commonly used in small offices and households. A typical SOHO network consists of a SOHO router and up to 10 hosts [3]. Hosts can be personal computers, laptops, printers, or even tablets and smartphones. Many SOHO routers support wireless connection so besides using a cable the devices can connect to the router via Wi-Fi. The point of ingress to a SOHO network is commonly a SOHO router. SOHO routers support a wide range of services and features. They serve as Dynamic Host Configuration Protocol (DHCP) servers, Network Address Translators (NAT), firewalls, and more. They support various protocols including Hypertext Transfer Protocol (HTTP) that is used for router administration via web interface, Telnet for administration via command line, File Transfer Protocol (FTP) and Samba (SMB) for file and print services, Universal Plug and Play (UPnP) for automatic device discovery, and many others. Design, implementation and configuration of the protocols supported by SOHO routers bring up several security issues that can cause the devices to be vulnerable and to become targets of attackers. If an attacker manages to misuse vulnerabilities of a router he can modify its configuration, change DNS settings, enable remote management, or modify firewall rules. This would give him full control over the device. He could intercept and modify the traffic sent over the local network, perform man-in-the-middle attacks and other malicious activities.

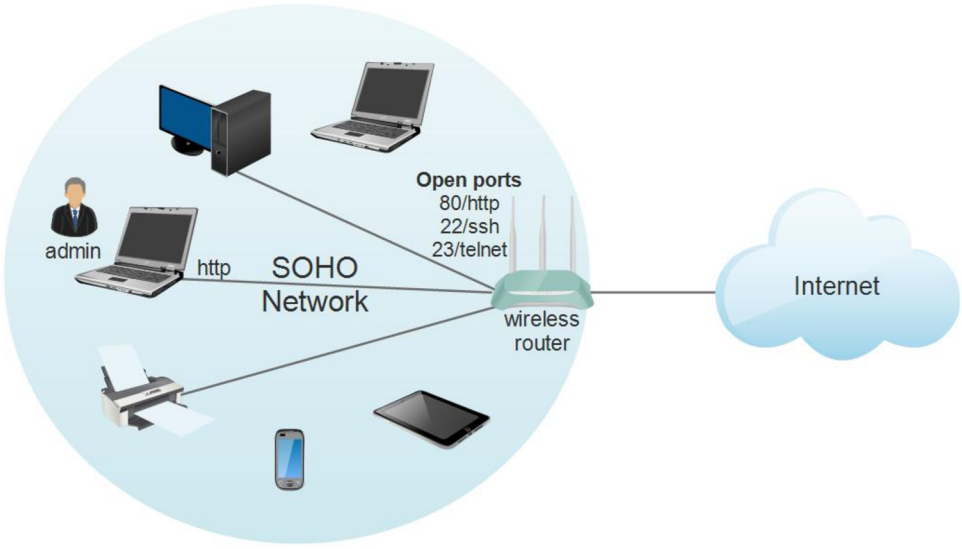

Figure 2.1: SOHO Network

According to the technical report published by Independent Security Evaluators (ISE) [1] the security issues that cause SOHO routers to be vulnerable can be divided into four basic categories: the misconfiguration of network services, the assumption of security on the LAN, insecure default configurations, and poor security design and implementation. This chapter discusses these four categories.

2.1 Misconfiguration of services

This category is characterized by network services that lack configuration options or utilize unnecessarily lenient permissions [1]. The services are often running with root privileges or with read/write access to unrelated system directories. If an attacker gains write access he could overwrite system files and get control over the router. Altering executable files can leverage in arbitrary command execution with root permissions. Read access can be used to disclose sensitive data that are often stored in clear text. An attacker could read a password or crack a password hash and perform authentication bypass to gain administrative access to the router. This could be avoided using salted password hashes or encryption.

The problem about the misconfiguration of a network service, e.g. improperly handled permissions, is that if it lacks configuration options there is nothing the administrator can do to change the service configuration, modify the permissions or disable the feature.

2.2 Assumption of security on the LAN

Many SOHO routers have poor security on the LAN. Protocols that are used lack secure channels. Web interfaces of most of the routers use Hypertext Transfer Protocol (HTTP) for authentication and therefore the user credentials are sent in plaintext and can be easily intercepted by an attacker in the local network. Many routers have Telnet enabled by default and as this protocol does not support encryption using it can leverage to sensitive data disclosure. Moreover, Telnet has little practical purpose and users commonly do not use it. To adjust security on the LAN the HTTP protocol should be replaced with HTTPS (Hypertext Transfer Protocol Secure) for the process of authentication and if text-based shell connection is needed SSH (Secure Shell) should be used instead of Telnet. Both HTTPS and SSH use encryption and therefore they represent a better alternative to HTTP and Telnet.

Another problem regarding security on the LAN is the assumption that attackers will not be able to gain access to the local network and could attack the routers only from an external network. Routers use Wi-Fi encryption standards that are known to be vulnerable. Of the routers tested, most use WPA2-PSK that is considered effective although it has security flaws. However, there are some that use WEP which is very easy to hack.

In addition to the vulnerable Wi-Fi encryption standards it is necessary to consider the fact that some local networks are intended for guest access, e.g. coffee shops or shopping centres.

2.3 Insecure by default

SOHO routers are commonly used by users that have minimal knowledge within information technology and do not realize security concerns. Therefore, vendors try to make the router set up and administration as easy as possible. This brings up several security issues as there are more potentially vulnerable services. Although some of the services are not enabled by default, for all the services that are available on the router there is a risk that they would be enabled by an adversary in case of attack. A good example of a service that is present in a large number of home routers and is publicly known to be vulnerable is UPnP (Universal Plug-and-Play). In 2013 Rapid7[1]

[1] Rapid7 is engineering better security to help companies reduce risk of breach, detect and respond to attacks, and build effective cybersecurity programs. More information on web page http://www.rapid7.com/company/index.jsp.

published a research [4] on security flaws in UPnP. It showed up that 81 million unique IP addresses responded to UPnP discovery requests. Although for many services that are commonly used there exist enhanced implementations that are more secure, manufacturers tend to use outdated versions.

Another problem regarding default set up of the routers is that some of the security protections, although when they are available on routers, are sometimes disabled by default. For example firewall. And as common users are typically not aware of security risks they would not use the protections unless they were enabled by default.

Another security issue is that service credentials are weak or publicly known. If the users changed the default credentials when setting up their home router this would not be a problem. But the truth is that many users do not change them. There are a few researches showing that default credentials are quite common. Ang Cui, et al., from Columbia University of New York did a research on embedded network devices [5]. They tried to exploit routers by accessing their administrative interfaces from WAN and found a number of devices that still had the factory default password set. Tripwire[2] Vulnerability and Exposure Research Team (VERT) did another research that focused on security of SOHO routers [6]. They asked 653 IT and security professionals and 1,009 employees working remotely about settings of their home wireless routers. Besides default service credentials the respondents were also asked about default IP addresses of the web interfaces of the routersand firmware updates. The following graph shows how they responded.

[2] Tripwire is a company delivers advanced threat, security and compliance solutions used by over 9,000 organizations. Tripwire enables enterprises, service providers and government agencies around the world to detect, prevent and respond to cyber security threats. More information on web page http://www.tripwire.com/company/.

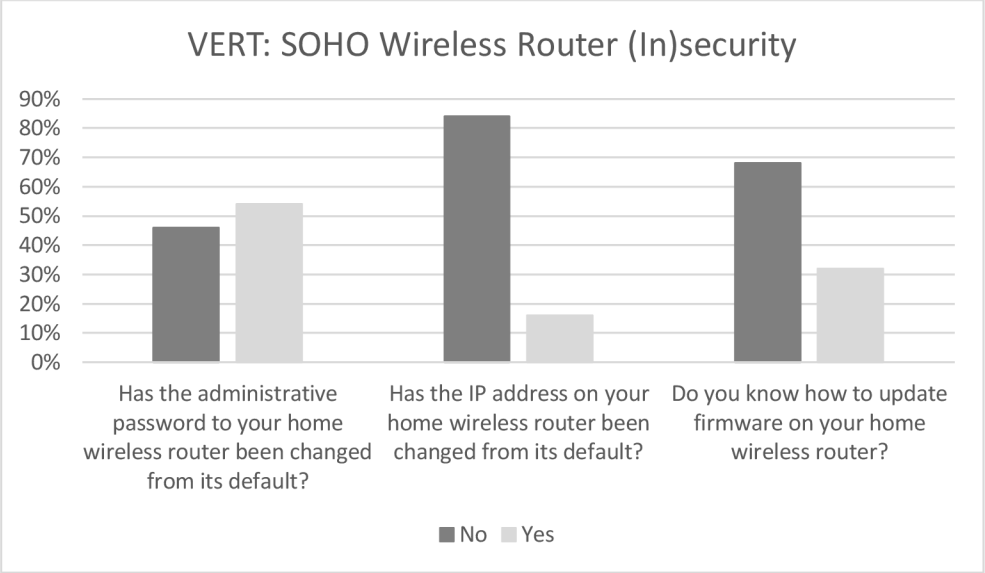

Figure 2.2: VERT: SOHO Wireless Router (In)security

2.4 Poor security design and implementation

Home routers face design and implementation issues. Very serious and common problem is lack of input validation. Although input validation in general can be a problem in any system that receives data from an external source, within home routers it is mostly associated with their web interfaces. Insufficient input validation within a web application can leverage in web based attacks, such as Cross-Site Request Forgery, Cross-Site Scripting, Directory Traversal, and Command Injection. The first three will be discussed more deeply in the next chapter.

Besides the web based attacks, buffer overflow vulnerabilities can be also caused by improper input validation. These vulnerabilities can be present within multiple network services supported by home routers. The more services a device supports, the higher probability of being vulnerable it has. Exploiting a buffer overflow within a service with root level privileges can provide an attacker with full administrative control over the router. Although if the vulnerable service does not run as root, the attacker can misuse other vulnerabilities to escalate the privileges.

3 Vulnerabilities and security weaknesses

Security issues of SOHO routers discussed in the previous chapter leverage to vulnerabilities that can be misused by attackers. Vulnerability is defined as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [7]. It is the intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw [8]. Vulnerability exploitation can result in compromise of confidentiality, integrity or availability of resources.

To make identifiers of the vulnerabilities, descriptions and categorization unified among communities within security field standards and norms are needed. This chapter will introduce Common Vulnerabilities and Exposures (CVE) [10] and Common Weakness Enumeration (CWE) [2] standards. CVE database maintains disclosed vulnerabilities and assigns each vulnerability a CVE identifier. To handle categorization vulnerabilities are divided to CWE categories.

After the standards introduction several CWE categories that conform to security of SOHO routers will be discussed and attacks on SOHO routers from past few years will be analyzed to help understand impact of the chosen vulnerability categories.

3.1 CVE – Common Vulnerabilities and Exposures

Till the end of the previous century most security tools used their own databases with their own names for security vulnerabilities. There was no effective interoperability among the separate databases and tools. To fix this problem Common Vulnerabilities and Exposures (CVE®) was launched in 1999 [9]. CVE is a dictionary of common identifiers for publicly known information security vulnerabilities along with standardized descriptions. These CVE identifiers facilitate data share across distinct security databases and tools. They also provide a guideline for evaluating the coverage of security tools.

CVE is managed by MITRE Corporation and the CVE List is publicly available on MITRE's CVE Web site. Besides this the list is integrated to U.S. National Vulnerability Database (NVD) that is maintained by the National Institute of Standards and Technology (NIST).

CVE is an international information security community effort. MITRE created CVE Editorial Board which includes numerous information security-related organizations including commercial security tool vendors, members of academia, research institutions, government agencies, and other prominent security experts. The Board identifies the vulnerabilities or exposures to be included in the CVE List. Along with the efforts of the Board and CVE Sponsor, many organizations all over the world have adopted the use of CVE.

3.2 CWE – Common Weakness Enumeration

With the advent of CVE List a need to categorize the vulnerabilities came up. MITRE's CVE Team developed a classification of vulnerabilities, attacks and other concepts to help define common software weaknesses. However, the system was not sufficient and the efforts to create a common baseline standard for weakness categorization continued. The next step was a document entitled Preliminary List Of Vulnerability Examples for Researchers (PLOVER) published by Steve Christey from the MITRE Corporation in 2006 [11]. It proposes 290 types of software weaknesses and provides a large number of vulnerability examples for each of them. Subsequently acceptable definitions a descriptions of these common weaknesses are established by community under National Institute of Technology (NIST) Software Assurance Metrics and Tool Evaluation (SAMATE) project and Common Weakness Enumeration (CWE) List is created [2].

The CWE List is maintained by the MITRE Corporation and is available at its website. Along with being a common language for describing software security weaknesses the list serves as a standard measuring stick for software security tools targeting these weaknesses. Nowadays it consists of 1003 CWE's that are organized into a hierarchical structure. There are five levels of abstraction (definitions according to CWE Glossary available on MITRE's CWE website [12]):

- **Category** is a CWE entry that contains a set of other entries that share a common characteristic.
- **Weakness Class** is a weakness that is described in a very abstract fashion, typically independent of any specific language or technology. More general than a Base weakness.
- **Weakness Base** is a weakness that is described in an abstract fashion, but with sufficient details to infer specific methods for detection and

prevention. More general than a Variant weakness, but more specific than a Class weakness.

- **Weakness Variant** is a weakness that is described at a very low level of detail, typically limited to a specific language or technology. More specific than a Base weakness.
- **Compound Element** is an entry that closely associates two or more CWE entries.

3.3 Weaknesses associated with SOHO routers

Now that sufficient theoretical background about vulnerabilities and security weaknesses was provided we can get down to weakness categories that are related to SOHO routers. There are many such categories and studying all of them would be too complex for the scope of the thesis. Besides this, categories that are used in different technical reports are not steady and they vary. The thesis will focus on a few categories that are the most common ones on home routers and that have the highest number of publicly known vulnerabilities with CVE identifiers assigned. This criterion considers primarily how often are the vulnerabilities disclosed and how difficult it is to detect them. To take into account also impact of individual vulnerabilities, the most well-known attacks on SOHO routers from past few years will be discussed and consequences of exploitation of the vulnerabilities will be presented.

Inspecting a sample of SOHO routers supplied by Internet Service Providers in Slovakia and Czech Republic showed that most publicly known vulnerabilities belong to these categories[3]: CWE-20 Improper Input Validation; CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'); CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); CWE-264 Permissions, Privileges, and Access Controls; CWE-352 Cross-Site Request Forgery (CSRF).

3.3.1 CWE-20: Improper Input Validation

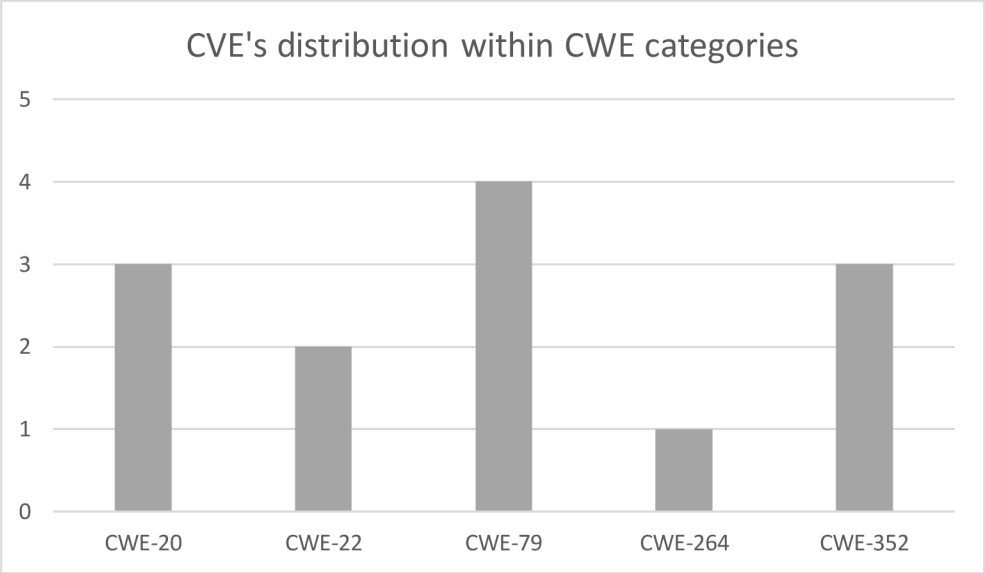

Figure 3.1: CVE's distribution within CWE categories

Improper Input Validation weakness class covers vulnerabilities that can originate in a system that receives data from an external source and does not validate the input properly. Untrusted input can enter the system in several ways, e. g. as a part of parameters or arguments, cookies, query results, URL components, files and anything read from the network. Not validating the input may allow an attacker to read and modify data, alter control flow or execute commands. In addition to this, malicious input may cause consumption of resources, such as memory and CPU, and this may result in denial of service.

When validating input it is necessary to check its type and length, the full range of acceptable values and missing or extra inputs. A software should

[3] For each router inspected CVE's assigned to it were found on http://www.cvedetails.com/ along with the information to which CWE category it belongs. The figure above shows the distribution of the found CVEs within five most frequent CWE categories.

reject any input that does not conform to expected format or transform it to something acceptable.

The CWE-20 weakness class is within the CWE's hierarchy parent of CWE-22 (Improper Limitation of a Pathname to a Restricted Directory) and CWE-79 (Improper Neutralization of Input During Web Page Generation) which will be discussed more deeply later in the chapter. Besides this, the Improper Input Validation class covers buffer overflow, remote code execution, denial of service vulnerabilities and others.

3.3.2 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-22 weakness class known as Path Traversal refers to vulnerabilities that are caused by improper neutralization of special elements within pathnames. When a software receives an external input to construct a pathname and does not verify it properly it may allow an attacker to read, create, or modify critical data. This may result in unauthorized code execution when the files are used to execute code, authentication bypass when an attacker gets access to sensitive data such as passwords and may cause a system crash when critical files are corrupted.

To prevent exploitation of these weakness one should properly validate pathnames that are input by external sources. Special attention should be paid to elements that are potentially dangerous within pathnames, such as ".." or "/". For example sequence "../" is commonly interpreted as parent directory of current location and when being part of an improperly neutralized pathname it may resolve to a file or directory outside of restricted location. Besides this, principle of least privilege should be applied. It means that all code should run with the lowest privilege that is essential to accomplish its task.

3.3.3 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

When untrusted data enters a web application and is not validated sufficiently it may leverage to a cross-site scripting (XSS) vulnerability. The web application generates a web page that contains the data entered. If the data contains executable content that is not neutralized properly it will be executed when a victim visits the web page.

There exist three main types of XSS vulnerabilities. First of them is reflected XSS also called as non-persistent. It occurs when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser [13]. Second type is stored XSS also called as persistent. When the application stores malicious data, e.g. in a database and later on the data is included in a generated web page the stored XSS occurs. Third type is DOM-Based XSS and its main difference from the first two types is that in this case the injection of XSS is performed by client, not server. It may occur when the client submits a form into the web application, the potentially dangerous data is not validated properly and is injected into the web page.

XSS exploitation may have various consequences. One of them is application data disclosure. Attackers often target cookies to gain session information, confidential information may be compromised along with end user files and execution of unauthorized code is also possible.

To avoid XSS exploitation it is essential to be aware of all areas where untrusted input may enter the web application. Several areas were already listed within CWE-20 which in the CWE hierarchy is parent of cross-site scripting category. Special attention should be paid to cookies as attacks to disclose information stored in them are one of the most common ones. The session cookie should be set to be HttpOnly to prevent it from being accessible by malicious client-side script. Besides validating input, proper output encoding, escaping and quoting is very important. Improperly handled encoding within the web application components may leverage to injection attacks and may even allow an attacker to bypass security mechanisms.

3.3.4 CWE-264: Permissions, Privileges, and Access Controls

Weaknesses in this category are related to the management of permissions, privileges, and other security features that are used to perform access control [14]. With access controls not implemented properly an attacker can have access to the router's file system. This may allow him to execute malicious code either by modifying an executable file within the router's file system, uploading an executable file, or injecting the code into a non-executable file. Attackers often target services that have elevated privileges so that their malicious code would be executed with these high privileges.

To mitigate these weakness principle of least privilege should be enforced and one should ensure that files which are not supposed to execute are

not over-privileged. Privileges among distinct components should be constrained so that if an attacker hacks one of them he would not gain control over all the system. If possible, services that are not needed and are exposed unnecessarily should be disabled to reduce the risk of being hacked. Only services that are needed and support authentication mechanisms should be left enabled [15].

3.3.5 CWE-352: Cross-Site Request Forgery (CSRF)

When the web application does not verify properly whether a request was sent by the user intentionally a cross-site request forgery vulnerability may occur. If an attacker makes the user to unintentionally send a request to the web server and the server treats the request as authentic it may allow the attacker to perform operations assuming the user's identity. He might read and modify application data, bypass security mechanisms or cause system crash. When attacking SOHO routers, attackers can for example modify DNS settings of the routers, firewall rules, enable remote management or reset the device to default settings so that it has default credentials.

To mitigate CSRF vulnerability it is advised to generate a unique nonce for each form and verify it upon receipt. It is also necessary to identify dangerous operations and send a confirmation request when such operation is requested by the user. Besides this, GET method should not be used for any request that triggers a state change. However, all these mitigations can be bypassed using XSS and therefore it is essential to ensure the web application is free of XSS issues.

3.4 Attacks on SOHO routers

When evaluating seriousness of a particular weakness it is not sufficient to consider only the number of assigned CVEs it has. It is more adequate to consider probability of its misuse to compromise the router and harm that its exploitation would cause. When comparing weaknesses that can be exploited from internal network to those that can be misused from outside of it the external ones are more likely to be abused. Analyzing information about mass attacks on SOHO routers can also say a lot about which weaknesses represent real security threats and have serious impact.

This part of the chapter will discuss attacks from the past few years sourcing from technical reports and articles published by experts and teams

within the field of security in information technologies, such as CERT Polska[4], or Team Cymru[5] [20] [21] [22].

3.4.1 The Moon malware

In February 2014 an ISP in Wyoming, USA noticed that some of its customers' routers were compromised. The routers were Linksys E-Series models and were exceedingly scanning other IP address ranges on ports 80 and 8080 and saturating available bandwidth. Network security researcher Johannes Ullrich from SANS Technology Institute analysed operation of the malware that compromised the routers and found out that authentication bypass vulnerability was exploited [16]. The vulnerable routers allow attackers to execute a binary file without a need to authenticate. The attacker sends random admin credentials but the router does not verify them. When executed, the binary starts to scan for other devices to infect. The malware replicates itself and therefore is considered a worm. There are indicators of a command and control channel existence but Ullrich said it could not be confirmed yet.

The malware works only if the particular router has remote management enabled. However, the most home routers have it disabled by default. If a router administrator needs to access the device remotely it is advised that he allows the access only from a specific IP address.

3.4.2 Polish banking attack

In February 2014 CERT Polska informed that cybercriminals hacked into home routers to perform a financial theft on a several Polish banks [17]. The attackers gained access to the web interfaces of the routers and modified their DNS settings. This leveraged to man-in-the-middle attack. Users' requests for IP addresses of the victim banks' websites were redirected to a malicious DNS server which responded with a malicious server's address. This caused the affected routers to send traffic to the malicious server instead of the bank's

[4] The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) — a research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. CERT Polska is the first Polish computer emergency response team. For more information see http://www.cert.pl/o-nas/langswitch_lang/en.

[5] Team Cymru Inc. is a specialized Internet security research firm dedicated to making the Internet more secure. For more information see http://www.team-cymru.org/about-us.html.

server. The traffic between user and the malicious server was sent unencrypted and therefore credentials and TANs (transaction authentication numbers) were intercepted and the server could modify the data sent. This along with socially-engineered SMS messages allowed the attackers to steal money from the users' bank accounts.

As with The Moon malware, this attack can only be performed with remote management enabled on the router. There are several ways how an attacker could change DNS settings on a victim device, e.g. Cross-Site Request Forgery or authentication bypass. However, CERT Polska claimed that it was not clear which vulnerabilities were exploited in this case.

3.4.3 DNS settings of over 300,000 SOHO routers compromised

In February 2014 Team Cymru published a report in which they analysed an attack on SOHO routers they started investigating earlier in January [18]. They detected over 300,000 routers with compromised DNS settings. The devices were set to send DNS requests to two malicious servers that were under the control of the attackers. As with the Polish banking attack, the DNS settings could be altered in several ways. The report lists three vulnerabilities that were disclosed lately and are good candidates for that. First of them is vulnerability to password guessing that could be used to log in to web interface of those routers that enable remote management. The second one is authentication bypass vulnerability called "ROM-0" that was found in ZyXEL's ZynOS in January 2014 and the third one is Cross-site Scripting vulnerability on several TP-Link routers that was found in October 2013.

Both this attack and the Polish banking attack altered DNS settings and the same vulnerabilities could be exploited to compromise the routers. However, there are some differences end the Team Cymru believe they are separate.

3.5 Summary of vulnerability categories

Analysis of attacks on SOHO routers from past few year shows that mass attacks with the highest impact commonly exploit authentication bypass, password guessing vulnerabilities and web vulnerabilities like Cross-site Request Forgery. This corresponds with the choice of weakness categories in the CWE section. The choice includes three web vulnerabilities and it might not look adequate to pay such attention to web security when talking about home routers but the truth is that these vulnerabilities belong to those that are

the most serious ones and can have fatal consequences. They can be exploited when attacker has access to router's web interface and that means when remote access is enabled or the attacker is in the router's local network. Although most home routers have remote access disabled by default, it turns out that many administrators enable it and therefore expose their devices to possible attacks. Remote management should be left disabled unless necessary and if enabled adequate restrictions should be done to eliminate the risk. Administrators should also ensure they do not use default passwords and change them to secure ones.

4 Tools

The goal of the thesis is to propose a set of tools for evaluating security of SOHO routers. The chosen set contains tools for port scanning, performing denial of service attacks and testing vulnerabilities of web interfaces of the routers. All the chosen tools are free for use what makes them available to anyone, however, it has significant cost to functionality, documentation and support. This chapter provides review of the tools. It focuses on ease of use, level of maintenance, documentation and whether the tools have GUI. Summary table evaluating the tools is provided at the end of the chapter.

4.1 Nmap

Nmap is a free and open source (GNU GPL) utility for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics [19]. Nmap was first released in 1997 and its author is Gordon “Fyodor” Lyon. Besides him, many other people made valuable contributions to development of the tool.

Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OSX. Classic Nmap is a command-line tool, however, Nmap suit includes GUI and results viewer called Zenmap.

Documentation is available on Nmap homepage [19]. It provides all the necessary information about configuration options and is very easy to understand.

4.2 Slowloris

Slowloris is a command line tool written by Robert "RSnake" Hansen in 2009 and it was presented at Defcon 17 [20] a few weeks after its release. Originally it was written in Perl but later versions in other languages, such as python (PyLoris), PHP and exe version were written by other authors.

The tool performs low bandwidth denial of service attack. It keeps sending incomplete http POST requests until the web server runs out of resources.

The script is available on ha.ckers.org[6] [21] including manual. The manual explains how the script performs the denial of service attacks and describes configuration options. Following the manual the tool is very easy to use.

4.3 Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for potentially dangerous files/programs, checks for outdated versions of servers and version specific problems. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software [22]. It is written by Chris Sullo and David Lodge and the first version Nikto 1.00 Beta was released in 2001.

It is a command line tool written in Perl and it should run on any system that supports basic Perl installation. It has been tested on Windows, Mac OSX and various Linux and Unix installations. Documentation is available on the Nikto homepage [22].

Nikto is very easy to use, it provides output that is easy to understand it and is suitable for testing vulnerabilities of the web servers of SOHO routers.

4.4 w3af

w3af is a web application attack and audit framework. The project's goal is to create a framework to help secure web applications by finding and exploiting all web application vulnerabilities. It is developed using Python and licensed under GPLv2.0. [23]. The project was created in 2006 and is leaded by Andres Riancho.

Linux, BSD and Mac platforms are supported. The framework should work on Windows as well, however, the current version was not tested on Windows and the installation process is not supported due to its complexity.

The framework can be used via both console and GUI (graphical user interface). It can be downloaded from w3af homepage [23] where documentation is available as well.

The framework provided usable results from only few router scans. The problem was caused by the fact that routers have restricted CPU and memory

[6] The source could be downloaded from the URL by the end of 2014 but is not available anymore. The script is available in Appendix B.

resources and they tend to fail during the scans due to overload. Reducing scan load by disabling some of the plugins and lowering the number of requests sent per minute helped solve this in some cases. However, there were also problems with the framework itself. It was crashing permanently and a bug was found[7].

4.5 Nessus

Nessus is proprietary vulnerability scanner developed by Tenable Network Security [24]. The "Nessus" Project was started by Renaud Deraison in 1998 [25].

The tool is cross-platform and is licenced under GPL (2.2.11 and earlier). It is available in four versions each supporting a different range of features depending on price. All versions but Nessus Home are paid. The Home version supports web application scanning and therefore it is sufficient for the purpose of the thesis. Besides web application scanning it supports features like vulnerability scanning, configuration audit, and malware detection.

Documentation is available on Tenable Network Security homepage [24].

Nessus is user friendly and easy to configure. However, the web application scanner does not output scanned URLs and therefore it cannot be verified whether authentication was successful for a particular scan.

4.6 Revok

Revok is an online web application security scanner licenced under GNU AGPLv3, which automatically finds vulnerabilities and weaknesses of a given web application and provides remedy advice. It currently supports applications with no authentication, basic authentication, and form-based authentication [26]. It is developed by Revok Team in Red Hat and the first version was released in 2013.

Revok performs vulnerability and security hardening checks on OWASP Top 10 vulnerabilities and it supports auto-detection of authentication type and login URL. Compared to other web vulnerability scanners that provide complex configurations it is very easy to use. However, the simplicity sometimes comes at cost to functionality.

[7] The bug was found in rfi (remote file inclusion) audit plugin. An unexpected exception was raised.

Revok binary package for download along with documentation are available on Revok homepage [27]. The documentation is very brief and provides only basic information about the tool's configuration options. If one wants to set more advanced options it is probable he would not find it in the documentation.

4.7 Evaluation of the tools

The following table summarizes the results of the review of the tools.

Table 4.1: Evaluation of the tools

Tool	Free	GUI	Ease of use	Documentation	Maintenance
Nmap	✓	✓	easy	very good	last update in 2014
Slowloris	✓		very easy	good	no updates since release
Nikto	✓		easy	very good	last update in 2012
w3af	✓	✓	complex configuration options	good	regular updates
Nessus	✓[8]	✓	easy	good	regular updates
Revok	✓	✓	very easy	sufficient	regular updates

[8] Nessus Home is free. Other versions of Nessus are paid.

5 Evaluation of SOHO routers supplied by ISPs

This chapter presents results of evaluation of chosen SOHO routers that were supplied by Internet Service Providers (ISP) in Slovakia and Czech Republic in 2014. The evaluation was done using the proposed methodology.

5.1 Methodology for evaluation

The chosen routers were tested using the tools described in the previous chapter. All the routers were tested in default factory settings[9]. The following table lists the routers along with their default IP addresses and default credentials.

Table 5.1: Routers

Router model	**Default IP address**	**Default username**	**Default password**
GREENPACKET CPE INDOOR DX350	10.1.1.254	admin	admin
ZyXEL VMG1312-B30B	10.0.0.138	admin	admin
ZyXEL Prestige 660HN-T3A	10.0.0.138	admin	admin
D-Link DSL-2641R	192.168.1.1	admin	admin
D-Link DIR 600	192.168.0.1	admin	[blank]
ADB VV3212	192.168.1.1	admin	13ftun9d
Technicolor TC 7200	192.168.1.1	admin	admin
CISCO EPC 3010	192.168.100.1	[blank]	[blank]

For each router some basic information is stated including firmware version, type of WAN connection, default security mode used, and Internet Service Provider (ISP) who it was supplied by. Outputs and reports from the scans are available in Appendix C.

Nmap tool was used to find out which ports are open on the routers from both LAN and WAN side and to gain information about the operating system running on the devices. Figure 5.1 shows testing architecture for scanning ports on the LAN and also for performing scans with all other tools.

[9] Some of the tested routers required password change during the initial setup so they were not tested with default passwords. In addition to this, blank credentials had to be changed because some of the tools do not allow blank fields within authentication configuration.

Figure 5.2 and Figure 5.3 show architecture for performing port scans from the WAN side[10].

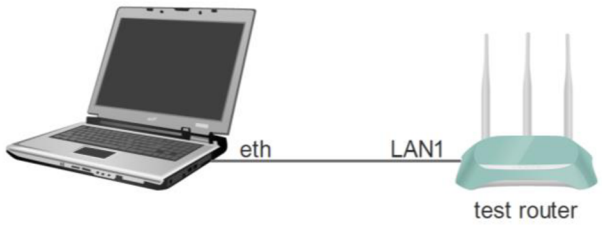

Figure 5.1: LAN Architecture

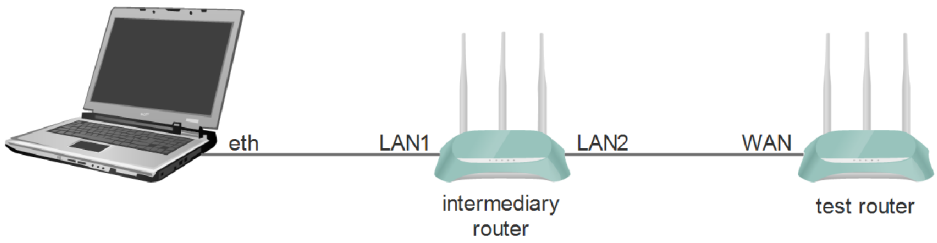

Figure 5.2: WAN Architecture (Ethernet)

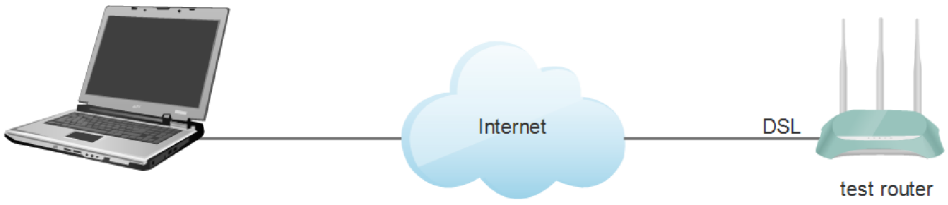

Figure 5.3: WAN Architecture (DSL)

To run the Nmap scan on the LAN the following command was issued via command line:

nmap –A host-ip-iddress

When scanning ports from the WAN side Nmap was run with *–sS* or *–Pn* arguments instead of *-A*.

[10] Routers with Ethernet type WAN connection were tested using an intermediary router. Thanks to access to DSL connection to the Internet also routers with DSL WAN type could be tested. Router with other types of WAN connection were not tested.

Open ports on the LAN are listed for each router separately and open ports on the WAN are summarized at the end of the chapter as for most routers the results of the scans were the same.

Slowloris tool was used to test whether the devices are resistant to the slow denial of service attack. To perform the attack the Slowloris script was run with the following options:

perl slowloris.pl –dns host-ip-address –port 80 –test

If the web interface of the router stopped responding after the script execution the attack was considered successful.

Nikto tool was used to scan we servers of the routers for security problems. Most of the issues detected were reported including OSVDB[11] identifiers. The following command was run:

nikto –h host-ip-address

w3af, Nessus and Revok tools were used to scan web interfaces of the routers for web application vulnerabilities.

w3af was configured to use all its audit plugins and a web_spider crawl plugin[12]. Authentication methods were set individually for each router depending on the method the particular device used. Html reports were generated for each router scan and are available in Appendix C. For some of the tested routers the number of plugins enabled had to be reduced because they seemed not to have enough CPU and memory resources for such extensive scans and they tend to fail during the scans.

Nessus web scanner was configured with basic authentication if supported by the particular router. If the router used a non-standard authentication method no authentication was configured and only login URL was scanned.

The problem with Nessus is that the scans do not list the URLs scanned and therefore it cannot be verified whether the authentication process was successful. It is not clear whether the tool scanned all the site or only the URL set as target (typically the login URL).

---

[11] OSVDB is an independent and open sourced web-based vulnerability database. Its goal is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. The database is available at http://osvdb.org/.

[12] All w3af plugins used are listed in html reports for each router separately. Descriptions of the plugins are available on the w3af homepage http://w3af.org/plugins.

Revok requires the target URL to be set and it tries to detect authentication method itself. By default Revok runs all modules available but there is a possibility to select the modules to be run. All the scans were run with all modules selected. However, during most of the scans many errors were issued and some modules were skipped. For more details see scan reports available in Appendix C. Security issues reported are divided to Vulnerabilities and Security Hardening.

With most routers authentication method auto-detection failed and authentication had to be set manually. The tool then generated a login page picture and asked to mark the fields for username and password. The scans with the authentication set manually did not report the sitemap of the web interfaces of the routers what indicates that the authentication was not successful.

5.2 Devices

In this section the results of the scans are reported for each device. As not all of the vulnerabilities and security issues revealed by the scans were covered in the third chapter, there is a brief description provided for each of them when they first occur in within the scan report.

5.2.1 GREENPACKET CPE INDOOR DX350

Table 5.1: GREENPACKET CPE INDOOR DX350

Firmware version	v2.8.9.5-g1.4.6-gp
WAN type	WiMAX
Security mode	WEP
Internet Service Provider	Slovanet (SK)

Nmap

Operating system: Linux 2.6.9 - 2.6.33

Open ports on LAN: 22/ssh, 23/telnet, 80/http, 443/ssl/http, 2601/zebra, 5060/sip, 6789/ibm-db2-admin, 9000/cslistener, 9999/abyss

Slowloris

DoS was successful.

Nikto

The scan reported a single security issue:

- The anti-clickjacking X-Frame-Options header[13] is not present.

w3af

Basic authentication was detected in server header. Login credentials and login URL were configured within basic authentication option. However, it seems like the tool was not able to authenticate against the router's web interface as only URLs that do not require authentication were scanned. Despite unsuccessful authentication several vulnerabilities were found. An unhandled error was reported.

Vulnerabilities

- Guessable credentials: The scan detected login URL and found that a correct user and password combination is admin/admin.
- Cross-Site scripting
- ReDoS (Regular Expression Denial of Service) [28]

Nessus

Basic authentication was set and the scan revealed several vulnerabilities.

Vulnerabilities

- Cookie Injection Scripting: The web server fails to sanitize request strings with malicious JavaScript. Exploiting this vulnerability may allow an attacker to inject arbitrary cookies. It can also leverage in session fixation attack[14].
- HTML Injections: Exploiting HTML Injection may allow an attacker to execute arbitrary HTML in a user's browser.
- Cross-Site Scripting
- Web Server Uses Plain Text Authentication Forms

[13] Using X-Frame-Options header prevents clickjacking attacks [https://www.owasp.org/index.php/Clickjacking].

[14] Session fixation attack is a class of session hijacking. The flaw is exploited by fixing an existent session ID on the victim's browser, and then hijacking the validated session ID after victim is authenticated.

Revok

The tool automatically detected form authentication and login credentials were set. The authentication seems to be correct as many URLs that require authentication were found and directory structure of the site was revealed. Several security issues were found.

Vulnerabilities

- Access Admin Pages: http://10.1.1.254/power_user/ URL is accessible without a need to authenticate. Accessing the URL issues download of a file.

Security Hardening

- Brute Force: It appears that the site does not have any mitigation method to prevent from brute-force attacks on login pages.
- SSL/TLS Misconfiguration: Target URL does not appear to support SSL.
- Anti-reflection (XSS): It appears that the site does not use X-XSS-PROTECTION header to mitigate reflected XSS attacks.
- Frame busting: Use multiple transparent or opaque layers to trick users into clicking on another page when they were intending to click on the top level page. Advice: send the x-frame-options.

5.2.2 ZyXEL VMG1312-B30B

Table 5.2: ZyXEL VMG1312-B30B

Firmware version	1.00(AAQS.1)
WAN type	Ethernet, xDSL[15]
Security mode	WPA2-PSK
Internet Service Provider	O2 (CZ)

Nmap

Operating system: No exact OS matches for host.

Open ports on LAN: 21/ftp, 22/ssh, 23/telnet, 80/http

[15] When performing port scans from the WAN side the router was connected to the Internet via ADSL.

Slowloris

DoS not successful.

Nikto

The Nikto scan had very extensive output. Besides the anti-clickjacking X-Frame-Options header missing it reported multiple issues belonging mostly to the following vulnerability categories: command execution, sensitive data disclosure, cross-site scripting, directory traversal, and authentication bypass.

w3af

Basic authentication was configured. However, multiple errors with description "[Errno 104] Connection reset by peer" were reported and it indicates that the tool was not able to authenticate against the router. Besides this, the scan found no URLs but the target URL set. No vulnerabilities were reported.

Nessus

Basic authentication was set. No vulnerabilities were found.

Revok

Authentication method auto-detection failed and only URL set as target was found. Multiple plugins were skipped because of errors. Only few security issues were found.

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Misconfiguration: Communication between browser and server is not secured with SSL/TLS (Secure Sockets Layer/ Transport Layer Security).

5.2.3 ZyXEL Prestige 660HN-T3A

Table 2.3: ZyXEL Prestige 660HN-T3A

Firmware version	1.02(VUQ.0)
WAN type	ADSL
Security mode	WPA2-PSK
Internet Service Provider	O2 (CZ)

Nmap

Operating system:	No exact OS matches for host
Open ports on LAN:	21/ftp, 23/telnet, 80/http, 5555/http

Slowloris

DoS not successful.

Nikto

The Nikto scan reported the following issues:

- Cookie SESSIONID created without the httponly flag.
- The anti-clickjacking X-Frame-Options header is not present.

w3af

Basic authentication was detected. However, when configuring w3af to use basic authentication it seems it cannot authenticate against the router successfully and therefore only the login page is scanned. Analysing traffic sent during the authentication process a URL that could be used to perform authentication bypass was found[16]. The URL is sufficient for the web server to consider the host to be authenticated. With this URL set as target there is no other authentication configuration needed and the tool scans all the site.

Vulnerabilities

- Cross-Site Request Forgery

Nessus

Basic authentication was configured.

Vulnerabilities

- RomPager HTTP Referer Header XSS: The remote RomPager HTTP server is affected by cross-site scripting vulnerability.

Revok

Form authentication was detected. Credentials and login URL were configured. It seems like the authentication was not successful as logs show no

[16] OWASP ZAP tool was used as a proxy to intercept the traffic [29]. The URL found contains login credentials encoded in base64.

crawling result and no sitemap was generated. Several modules were skipped due to errors. Several security issues were reported:

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Misconfiguration

5.2.4 D-Link DSL-2641R

Table 5.4: D-Link DSL-2641R

Firmware version	OR_1.02
WAN type	ADSL
Security mode	WPA/WPA2 (auto)
Internet Service Provider	Orange (SK), Netbox (CZ)

Nmap

Operating system: Linux 2.6.9 - 2.6.33

Open ports on LAN: 80/http, 49152/upnp

Slowloris

DoS successful.

Nikto

The scan reported a single security issue:

- The anti-clickjacking X-Frame-Options header is not present.

w3af

Basic authentication was detected. However, when running the scan with basic authentication configured Errors 104 (Connection reset by peer) and 111 (Connection refused) were reported. This indicates that the authentication was not successful and only the URL set as target was scanned.

Vulnerabilities

- Potential buffer overflow

Nessus

Basic authentication was configured.

Vulnerabilities

- Web Server Uses Plain Text Authentication Forms

Revok

Authentication method auto-detection failed and only URL set as target was found. Multiple plugins were skipped because of errors. Only few security issues were found.

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Mis-configuration

5.2.5 D-Link DIR 600

Table 5.5: D-Link DIR 600

Firmware version	2.16
WAN type	Ethernet
Security mode	Disabled
Internet Service Provider	Orange (SK), Netbox (CZ)

Nmap

Operating system: Linux 2.6.33 (D-Link DIR-645 WAP)

Open ports on LAN: 53/domain, 80/http, 49152/upnp

Slowloris

DoS not successful.

Nikto

The scan reported a single security issue:

- The anti-clickjacking X-Frame-Options header is not present.

w3af

Basic authentication was detected and set. It seems like the authentication was successful as the scan reported several URLs that require authentication. The scan suddenly crashed and caused the test laptop to crash as well. No report was generated, however, I managed to copy and paste logs displayed within the tools GUI before the crash. The logs copied are available in Appendix C. No vulnerabilities were reported.

Nessus

Basic authentication was set. No vulnerabilities were reported.

Revok

Authentication method auto-detection failed and only URL set as target was found. Multiple plugins were skipped because of errors. Only few security issues were found.

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Mis-configuration

5.2.6 ADB VV3212

Table 5.6: ADB VV3212

Firmware version	VV3212_SLT_3.1.0.0012 - main
WAN type	ADSL[17], Active Ethernet[18]
Security mode	WPA2-PSK
Internet Service Provider	Slovanet (SK)

Nmap

Operating system: Linux 2.6.18 - 2.6.31

Open ports on LAN: 53/domain, 80/http, 443/ssl/https

[17] ADSL connection was used when performing port scans from the WAN side.
[18] Active Ethernet is a technology used to connect the device to optical network.

Slowloris

DoS not successful.

Nikto

The scan seemed to freeze so it had to be stopped forcibly. Before it started to freeze it reported a single security issue:

- The anti-clickjacking X-Frame-Options header is not present.

w3af

Authentication method is not basic. Login credentials are sent to the web interface of the router within a POST request body. No authentication was configured. The scan froze repeatedly and no reports were generated.

Nessus

As the basic authentication method is not used no authentication was configured. No vulnerabilities were found.

Revok

Authentication method auto-detection failed and only URL set as target was found. Multiple plugins were skipped because of errors. Only few security issues were found.

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Mis-configuration

5.2.7 Technicolor TC 7200

Table 5.7: Technicolor TC 7200

Firmware version	STD6.01.12
WAN type	Coax
Security mode	WPA/WPA2 (auto)
Internet Service Provider	UPC (CZ)

Nmap

Operating system:	Cisco embedded, Motorola embedded, Scientific Atlanta embedded
Open ports on LAN:	80/tcpwrapped

Slowloris

DoS successful.

Nikto

The scan reported a single security issue:

- The anti-clickjacking X-Frame-Options header is not present.

w3af

Authentication method is not basic. Login credentials are sent to the web interface of the router within a POST request body. No authentication was configured and therefore the scan reports Errors 104 (Connection reset by peer).

Nessus

As the basic authentication method is not used no authentication was configured.

Vulnerabilities

- Web Server Uses Plain Text Authentication Forms

Revok

Authentication method auto-detection failed and only URL set as target was found. Multiple plugins were skipped because of errors. Only few security issues were found.

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Mis-configuration

5.2.8 CISCO EPC 3010

Table 5.8: CISCO EPC 3010

Firmware version	epc3010-v302r12901-100129cs
WAN type	Coax
Security mode	none
Internet Service Provider	Slovanet (SK)

Nmap

Operating system: Wind River VxWorks

Open ports on LAN: 80/http

Slowloris

DoS successful.

Nikto

The Nikto scan reported the following issues:

- Cookie SESSIONID created without the httponly flag.
- The anti-clickjacking X-Frame-Options header is not present.

w3af

Authentication method is not basic. Login credentials are sent to the router's web interface within a POST request body. No authentication configured within w3af and therefore the scan reports Errors 104 (Connection reset by peer).

Nessus

As the basic authentication method is not used no authentication was configured.

Vulnerabilities

- Web Server Uses Plain Text Authentication Forms

Revok

Authentication method auto-detection failed and only URL set as target was found. Multiple plugins were skipped because of errors.

Vulnerabilities

- Session Fixation

Security Hardening

- SSL/TLS Misconfiguration
- Cookie Attributes: Secure flag: Cookies without Secure flag is allowed to be transmitted through an unencrypted channel which makes it susceptible to sniffing.
- Strict MIME Type: MIME (Multipurpose Internet Mail Extensions) type mismatch found or nosniff header missed. This increases exposure to XSS attack.
- Cookie Attributes: HttpOnly Flag

5.3 Evaluation results summary

In this subchapter the results of chosen SOHO routers evaluation will be analysed. Summary of open ports and services found on the routers will be provided and detected vulnerabilities will be recapped. At the end problems encountered during the testing will be discussed.

5.3.1 Open ports

Scanning ports on LAN showed that most routers use HTTP and not HTTPS. Many routers support Telnet which does not support encryption and only two routers have SSH enabled. Some routers support services that are known to be vulnerable, such as UPnP. Some have ports open for many other services that are not common and are hardly essential. From the WAN side most of the scans detected no open ports and reported that all the scanned ports were filtered.

The most frequent services that were found on the open ports are summarized in the following table.

Table 5.9: Open ports - services

	HTTP	HTTPS	Telnet	SSH	DNS	FTP	UPnP
GreenPacket CPE indoor DX350	✓	✓	✓	✓			
ZyXEL VMG1312-B30B	✓		✓	✓		✓	
ZyXEL Prestige 660HN-T3A	✓		✓			✓	
D-Link DSL-2641R	✓						✓
D-Link DIR-600	✓				✓		✓
ADB VV3212	✓	✓			✓		
Technicolor TC7200							
CISCO EPC3010	✓						

5.3.2 Detected vulnerabilities

All tested routers use HTTP for the web interface authentication and therefore credentials are sent in plaintext.

Out of the CWE categories described in chapter 3 several vulnerabilities were detected including Cross-Site Scripting (CWE-79), Cross-Site Request Forgery (CWE-352), Path Traversal (CWE-22) and issues with permissions and access controls (CWE-264). Besides these, many occurrences of vulnerabilities that belong to Session Fixation (CWE-384) and OS Command Injection (CWE-78)[19] categories were found.

The scans revealed that some routers were missing protections against Cross-Site Scripting, such as X-XSS-PROTECTION headers, and MIME type mismatch that increases exposure to XSS attacks was detected. Mitigations against clickjacking attacks are also missing (X-Frame-Options headers are not present).

Several router were found to be vulnerable to slow denial of service and regular expression denial of service attacks [28].

Detected vulnerabilities are summarized in tables in Appendix A.

[19] CWE-78 category is also called as command or code execution.

5.3.3 Problems encountered during testing

In some cases the tools for testing web application vulnerabilities were not able to authenticate successfully against the tested routers. That was partially caused by lack of configuration options in some of the tools. Also the routers tested might have some kind of protection against automated scans (e.g. they could verify user agent). If the authentication process was successful within all the scans more vulnerabilities would be probably found.

Some web application vulnerability scans (mostly those performed by w3af) caused the tested routers to crash due to lack of memory and CPU resources.

The web application vulnerability scanners turned out not to be suitable for testing SOHO routers due to problems with authentication and the scans were too extensive and were causing some of the routers to crash.

6 Conclusion

The thesis introduced SOHO routers and described the role they play in SOHO networks. Security issues that originate in design and implementation of a typical SOHO router were described. These security issues leverage to vulnerabilities that can be exploited by attackers.

Vulnerabilities in general are introduced and standards that help unify vulnerability identifiers, descriptions, and categories are presented. The theses described several vulnerability categories that are the most common ones within the field of SOHO routers. Attacks on these devices from the past few years are analyzed to help understand seriousness and impact of distinct vulnerability categories.

The thesis proposes a set of tools for testing vulnerabilities of SOHO routers. Review of the tools is provided. Following the proposed methodology the selected tools were used to evaluate security of a sample of SOHO routers supplied by Internet Service Providers (ISP) in Slovakia and Czech Republic. Although several problems with the selected tools were encountered many vulnerabilities were revealed. The amount of the vulnerabilities found indicates that SOHO routers cannot be considered secure enough. Security of SOHO routers is often underestimated and should be paid more attention.

The thesis introduces the topic of security of SOHO routers and covers the most important vulnerability categories. However, there are several other categories that have significant cost to security and they could be covered in future research. Also more tools for evaluating security of the routers could be reviewed as those used within the thesis turned out not to be completely suitable for this purpose.

7 References

[1] Independent Security Evaluators. SOHO Network Equipment. *https://securityevaluators.com/knowledge/case_studies/routers/soho_techreport.pdf*. [Online; accessed 02-May-2015].

[2] MITRE Corporation. *http://cwe.mitre.org/*. [Online; accessed 02-May-2015].

[3] Bradley Mitchell. What Is a SOHO Router (and Network)?. *http://compnetworking.about.com/b/2010/11/13/what-is-a-soho-router.htm*. [Online; accessed 10-May-2015].

[4] Rapid7. Security Flaws in Universal Plug and Play. *https://hdm.io/writing/originals/SecurityFlawsUPnP.pdf*. [Online; accessed 02-May-2015].

[5] Ang Cui, Salvatore J. Stolfo. A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan. *http://ids.cs.columbia.edu/sites/default/files/paper-acsac.pdf*. [Online; accessed 02-May-2015].

[6] Tripwire Vulnerability and Exposure Research Team (VERT). SOHO Wireless Router (In)security. *http://www.tripwire.com/register/soho-wireless-router-insecurity/showMeta/2/*. [Online; accessed 02-May-2015].

[7] NIST. Term: Vulnerability. *http://fismapedia.org/index.php/Term:Vulnerability*. [Online; accessed 10-May-2015].

[8] Software Protection Initiative. The Three Tenets of Cyber Security. *http://www.spi.dod.mil/tenets.htm*. [Online; accessed 10-May-2015].

[9] Mitre Corporation. Common Vulnerabilities and Exposures (CVE) Dictionary. *http://cve.mitre.org/*. [Online; accessed 02-May-2015].

[11] Steve Christey. PLOVER - Preliminary List Of Vulnerability Examples for Researchers. *https://cwe.mitre.org/documents/sources/PLOVER.pdf*. [Online; accessed 02-May-2015].

[12] Mitre Corporation. CWE Glossary. *http://cwe.mitre.org/documents/glossary/*. [Online; accessed 02-May-2015].

[13] Mitre Corporation. CWE-79. *http://cwe.mitre.org/data/definitions/79.html*. [Online; accessed 02-May-2015].

[14] Mitre Corporation. CWE-264. *http://cwe.mitre.org/data/definitions/264.html*. [Online; accessed 02-May-2015].

[15] Mitre Corporation. CAPEC-69. *https://capec.mitre.org/data/definitions/69.html*. [Online; accessed 02-May-2015].

[16] Johannes B. Ullrich. Linksys Worm "TheMoon" Summary: What we know so far. *https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633*. [Online; accessed 02-May-2015].

[17] CERT Polska. Large-scale DNS redirection on home routers for financial theft. *http://www.cert.pl/news/8019/langswitch_lang/en*. [Online; accessed 02-May-2015].

[18] Tripwire Study: 80 Percent of Best-Selling Small Ofice/Home Ofice (SOHO) Wireless Routers Have Security Vulnerabilities. 2013. WiFi/ WLAN [online]. 23(11): 14-15 [cit. 2015-05-18].

[19] Nmap – homepage. *https://nmap.org/*. [Online; accessed 02-May-2015].

[20] Sam Bowne, Robert Hansen. Hijacking Web 2.0 Sites with SSLstrip and SlowLoris. *https://vimeo.com/7618090*. [Online; accessed 02-May-2015].

[21] Robert Hansen. Slowloris. *http://ha.ckers.org/slowloris/slowloris.pl*. [Online; accessed 02-Dec-2014].

[22] CIRT. Nikto2. *https://cirt.net/nikto2*. [Online; accessed 10-May-2015].

[23] w3af – homepage. *http://w3af.org/*. [Online; accessed 02-May-2015].

[24] Tenable Network Security. Nessus Vulnerability Scanner. *http://www.tenable.com/products/nessus-vulnerability-scanner*. [Online; accessed 02-May-2015].

[25] Wikipedia. Nessus (software). http://en.wikipedia.org/wiki/Nessus_(software). [Online; accessed 10-May-2015].

[26] Revok FAQ. *https://github.com/Revok-scanner/revok/blob/master/docs/FAQ.md*. [Online; accessed 10-May-2015].

[27] Revok – homepage. *http://revok-scanner.github.io/revok/*. [Online; accessed 02-May-2015].

[28] OWASP. Regular expression Denial of Service – ReDoS. *https://www.owasp.org/index.php/Regular_expression_Denial_of_Service_-_ReDoS*. [Online; accessed 02-May-2015].

[29] OWASP. Zed Attack Proxy Project. *https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project*. [Online; accessed 02-May-2015].

Appendix A

Summary of evaluation of the SOHO routers

This appendix contains tables that summarize results of evaluation of the chosen SOHO routers.

	nikto		w3af					Nessus				
	httponly flag	X-Frame-Options	XSS	CSRF	ReDoS	Guessable Credentials	Buffer overflow	XSS	HTML Injections	Cookie Injection Scripting	RomPager HTTP Referer Header XSS	Plain text authentication forms
GREENPACKET CPE INDOOR DX350		✓	✓		✓	✓		✓	✓	✓		✓
ZyXEL VMG1312-B30B		✓										
ZyXEL Prestige 660HN-T3A	✓	✓		✓							✓	
D-Link DSL-2641R		✓					✓					✓
D-Link DIR 600		✓										
ADB VV3212		✓	-	-	-	-	-					
Technicolor TC 7200		✓										✓
CISCO EPC 3010	✓	✓										✓

Table A.1: Evaluation summary 1

	Slowloris	revok							
	DoS	Session Fixation	Access admin pages	Brute Force	SSL/TLS Misconfiguration	Anti-reflection (XSS)	Frame busting	Strict MIME Type	Cookie Attributes (httponly flag, secure flag)
GREENPACKET CPE INDOOR DX350	✓		✓	✓	✓	✓	✓		
ZyXEL VMG1312-B30B		✓			✓				
ZyXEL Prestige 660HN-T3A		✓			✓				
D-Link DSL-2641R	✓	✓			✓				
D-Link DIR 600		✓			✓				
ADB VV3212		✓			✓				
Technicolor TC 7200	✓	✓			✓				
CISCO EPC 3010	✓	✓			✓	✓		✓	✓

Table A.2: Evaluation summary 2

Appendix B

Slowloris script

This appendix contains slowloris.pl script. It is available on the enclosed CD.

Appendix C

Scan reports

This appendix contains reports and log files from the scans performed with *Nmap*, *Nikto*, *w3af*, *Nessus*, and *Revok* tools. It is available on the enclosed CD. The reports are grouped by the tools.