Vulnerabilities on the corporate network perimeter

Results of automated security assessment

ptsecurity.com

Contents

What is automated security assessment 3

About the research 3

Key findings 4

Statistics: something to think about 5

Dropping the dead weight: services inventory 6

Root of evil: outdated software versions and insecure protocols 9

Vulnerability types 11

- Arbitrary code execution 12
- Denial of service 12
- Escalation of privileges 13
- Information disclosure 14

Conclusions and recommendations 15

MaxPatrol 8 scan modes 16

What is automated security assessment

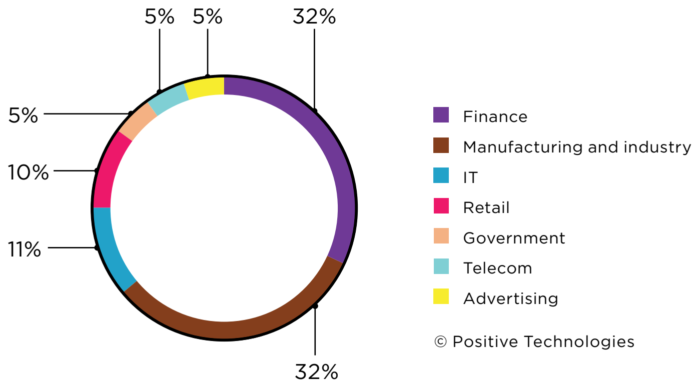
A proper security assessment of corporate infrastructure takes time and requires highly qualified security experts. Security assessment tools can help to fill this need. These tools are special systems that automatically detect open network ports and available services, software vulnerabilities, as well as configuration flaws in equipment, servers, and protection tools. Modern security assessment tools offer scan modes suited for particular tasks, such as network scanning, system checks, and compliance control.

Automated security assessment is a preventive measure: it reduces exposure to potential attacks by detecting weak spots. This kind of assessment saves time and minimizes the chance of human error.

About the research

In this report, we will share the results of automated security assessment of the network perimeter of selected corporate information systems. Scanning was performed using the MaxPatrol 8 vulnerability and compliance management system in Pentest mode. More details on MaxPatrol 8 scan modes can be found at the end of this document.

The report consists of the company's 19 most representative projects from 2019 and the first half of 2020. Criteria for inclusion were client consent to publishing of scan results in depersonalized form and the absence of significant restrictions by the client on scanning scope. A total of 3,514 hosts were scanned, including network devices, servers, and workstations.



© Positive Technologies

Figure 1. Tested systems, by industry

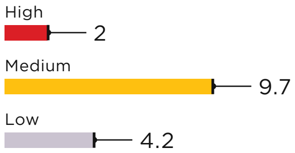
This research is of particular interest for vulnerability management experts. We will take a closer look at services most frequently available on the network perimeter and discuss security lapses detected with the help of automated scanning. We will also provide statistics regarding the vulnerabilities to reflect their level of risk and whether there are publicly available exploits for them. Risk levels were determined based on Common Vulnerability Scoring System (CVSS) version 2. Verification of the vulnerabilities was not performed.

Key findings

- Our experts detected high-risk vulnerabilities on external network resources of 84 percent of tested companies.
- Even a low-skilled attacker could exploit 10 percent of vulnerabilities by using a ready public exploit.
- Half of vulnerabilities can be eliminated by installing software updates.
- Systems at 26 percent of companies are still vulnerable to WannaCry encryption malware.
- At 74 percent of companies, SSH is available for direct connection from the Internet. One fifth of software vulnerabilities involved OpenSSH errors, which may allow attackers to obtain control over network perimeter resources or breach the company's local network.
- All the companies' perimeters have hosts vulnerable to the SWEET32 attack, and 84 percent of companies are still vulnerable to the POODLE attack. If attackers succeed in exploiting these vulnerabilities, they can extract confidential data from encrypted connections.

Statistics: something to think about

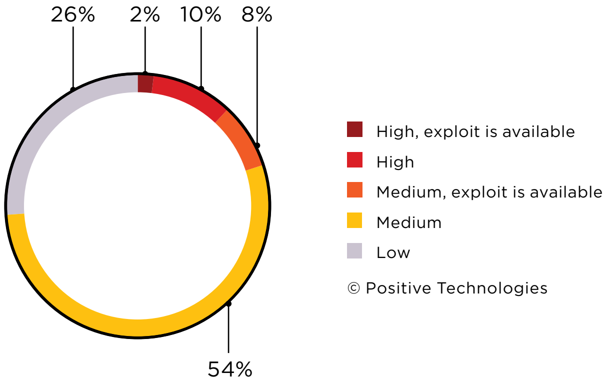
1. Automated security assessment revealed 9,483 vulnerabilities on 599 hosts. The detected vulnerabilities are caused by the absence of recent software updates, outdated algorithms and protocols, configuration flaws, mistakes in web application code, and accounts with weak and default passwords.



© Positive Technologies

Figure 2. Average number of vulnerabilities per host, by risk level

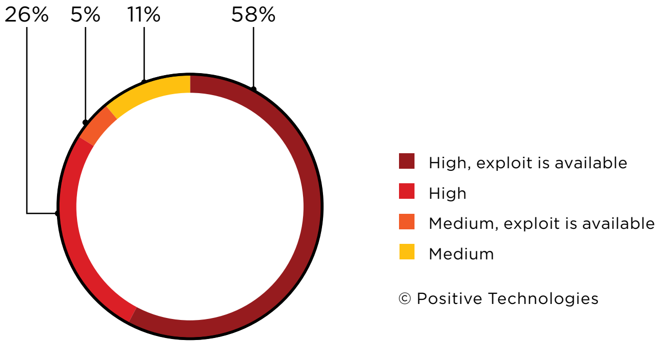
2. Publicly available exploits are available for 10 percent of vulnerabilities, which means that attackers can exploit them without professional programming skills or experience in reverse engineering.



© Positive Technologies

Figure 3. Severity of vulnerabilities and availability of exploits (percentage of all vulnerabilities)

3. Our research revealed high-risk vulnerabilities at 84 percent of companies. High-risk vulnerabilities having a publicly available exploit are present at 58 percent of companies.

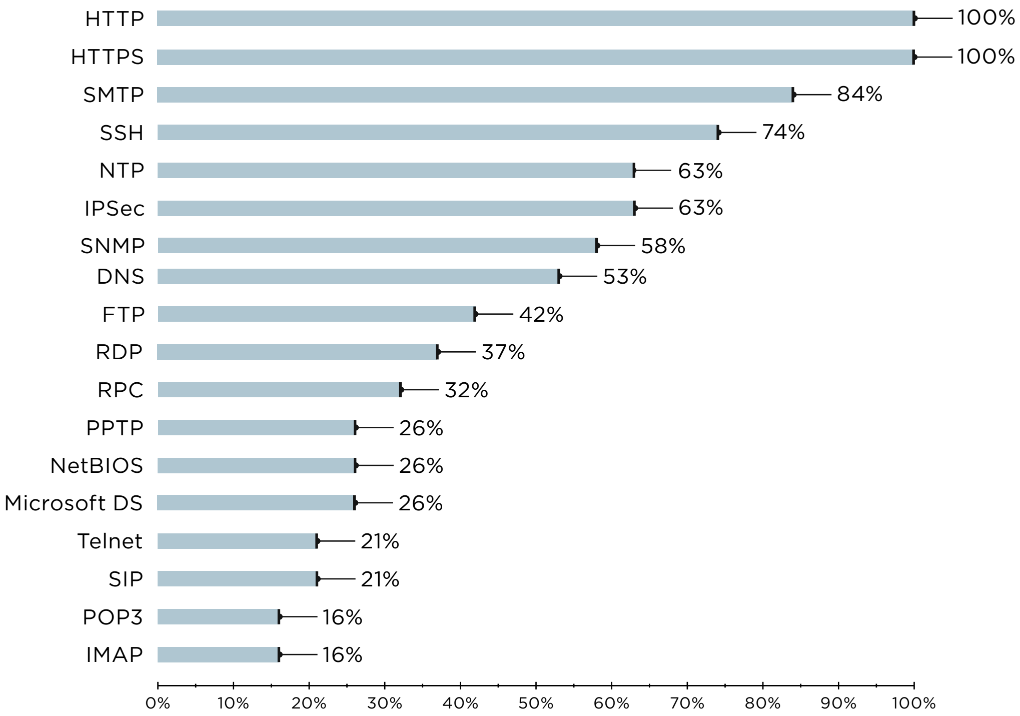


© Positive Technologies

Figure 4. Severity of vulnerabilities and availability of exploits (percentage of companies)

Dropping the dead weight: services inventory

On some hosts, automated scanning revealed no vulnerabilities. It is important to note, however, that such hosts had only a few services available and were protected by recent software updates and a secure configuration. That is why we believe that building a secure perimeter must start with taking an inventory—detecting and disabling active services that are not being used. We will take a closer look at services available on the perimeter of most companies and their security flaws.



© Positive Technologies

Figure 5. Services on the network perimeter (percentage of companies)

The research found that 26 percent of companies have TCP port 445 open at hosts with external network interfaces. This combination puts companies at risk of infection with WannaCry.

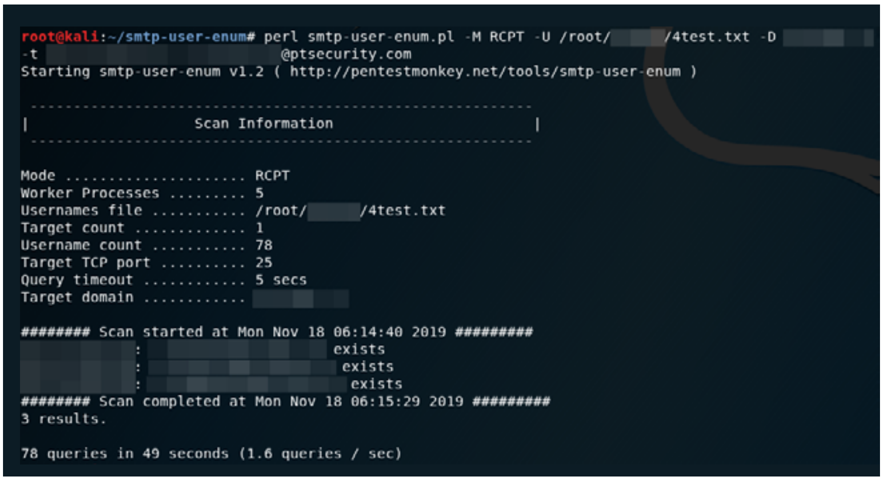
Analysis revealed remote access and administration interfaces, such as SSH, RDP, and Telnet, on numerous resources. These interfaces allow any external attacker to conduct brute-force attacks. At one company, scanning revealed an open Telnet port and the account Cisco:123456. Attackers can bruteforce such weak passwords in a matter of minutes and then obtain access to network equipment with the privileges of the corresponding user before proceeding to develop the attack further. Moreover, the host may fall victim to a botnet brute-force attack and, if the attack succeeds, become part of the botnet. For example, the Dark Nexus botnet exploits known vulnerabilities in device software and bruteforces Telnet credentials, after which the compromised devices are used for DDoS attacks.

How to protect remote administration of servers

Limit access to the interfaces used to manage the list of IP addresses allowed on your internal network. Do not use Telnet, as it transmits credentials in cleartext. Use SSH for server administration. To make SSH connections more secure:

- *Use public key authentication.*
- *Use a non-standard port to protect from mass automated attacks.*
- *Block SSH access for the root account.*

At 84 percent of companies, TCP port 25 is open with the SMTP email service available on the perimeter. Data is transmitted in cleartext via SMTP, which means that just like HTTP, attackers can intercept traffic and read corporate emails. In addition, insecure configuration of mail servers may leak corporate email addresses. IT administrators often fail to disable support for the VRFY, EXPN, and RCPT TO commands. As a result, attackers can bruteforce email addresses based on the SMTP server's responses. Attackers can even automate this process by using a ready-made publicly available utility. The collected corporate email addresses can be used to bruteforce credentials for network perimeter resources or remote access to the internal network, or to send phishing emails.



```
root@kali:~/smtp-user-enum# perl smtp-user-enum.pl -M RCPT -U /root/[redacted]/4test.txt -D [redacted]
-t [redacted]@ptsecurity.com
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... RCPT
Worker Processes ......... 5
Usernames file ........... /root/[redacted]/4test.txt
Target count ............. 1
Username count ........... 78
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ [redacted]

######## Scan started at Mon Nov 18 06:14:40 2019 #########
[redacted]: [redacted] exists
[redacted]: [redacted] exists
[redacted]: [redacted] exists
######## Scan completed at Mon Nov 18 06:15:29 2019 #########
3 results.

78 queries in 49 seconds (1.6 queries / sec)
```

Figure 6. Bruteforcing of corporate email addresses with RCPT

At 42 percent of companies, there are FTP servers available for connection on the network perimeter. If an FTP server is protected with a weak password, attackers who have bruteforced credentials will not only access files, but also try to push on with the attack. In one penetration test, automated scanning revealed an open network port on a perimeter host with the vsFTPd FTP server running. By using previously collected information about the system in question, our experts brute-forced the FTP username and password. Once connected, the experts found the web application files and uploaded a web shell, which gave them the ability to execute OS commands on the host.

At two companies, anonymous access to FTP servers is possible, which creates the risk of providing access to sensitive files by mistake. A more serious threat arises when the system allows uploading files to an FTP server without authentication: in this case, attackers have more opportunities for malicious actions. For example, they can use an FTP server as a staging point for malware.

Even robust password protection cannot offer full protection, since outdated FTP implementations contain numerous known vulnerabilities. In addition, credentials are transmitted via FTP in cleartext, which is why we recommend using secure versions such as FTPS or SFTP.

Every tested company had TCP network ports 80 and 443 open on the perimeter. As a rule, these network ports have applications running on Apache HTTP Server, Apache Tomcat, Nginx, and other web servers. By identifying a web server and its version, attackers can select relevant exploits. Our research proved that 16 percent of web server vulnerabilities have publicly available exploits.

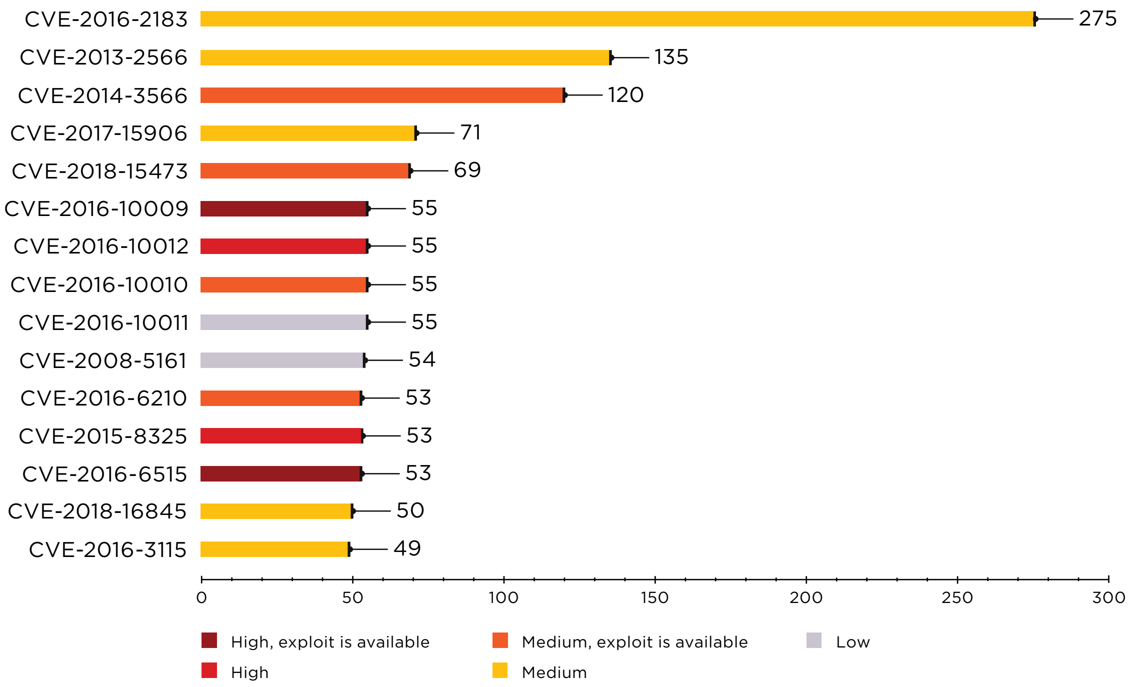
The availability of TCP network port 80 means that data can be exchanged via the HTTP protocol. HTTP traffic is transmitted without encryption, meaning that attackers can intercept it, for example, by tricking a victim into connecting to a fake access point. If credentials are transmitted by using the Basic method (in Base64 encoding), attackers can easily decode them and obtain the victim's password for accessing the web application.

Vulnerabilities by popular services, risk level, and availability of exploits

Service	High, exploit is available	High	Medium, exploit is available	Medium	Low
Web services	24	609	344	3659	1507
Remote access	110	192	234	452	441
Domain name service (DNS)	36	183	21	227	15
Email	—	10	102	598	437
VPN services	—	—	12	30	24
File services	—	—	4	49	19
Other services	—	7	14	72	51

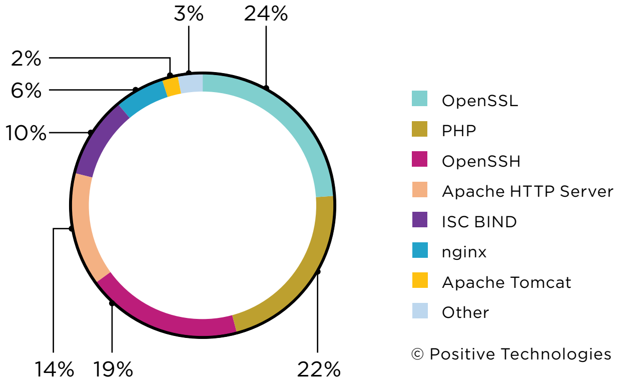
Root of evil: outdated software versions and insecure protocols

In our automated security assessment of network perimeter, almost half of detected vulnerabilities (47%) can be fixed by installing the latest software versions. All companies had problems with keeping software up to date. At 42 percent of them, we found software for which the developer had announced the end of life and stopped releasing security updates. For example, 32 percent of companies still use PHP 5 applications, even though support for that language ended in January 2019. The oldest vulnerability found in automated analysis was 16 years old.



© Positive Technologies

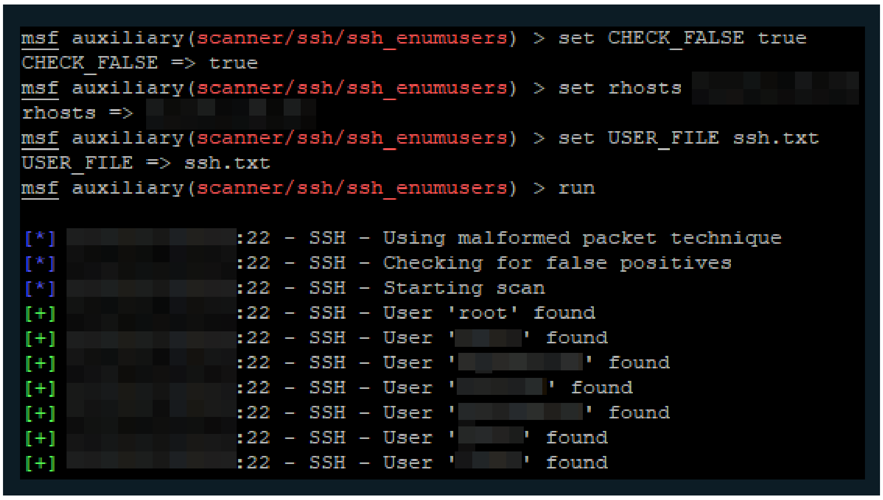
Figure 7. Most common vulnerabilities on the network perimeter (number of hosts)



© Positive Technologies

Figure 8. Vulnerable software (percentage of vulnerabilities caused by use of out-of-date software versions)

Automated scanning revealed more than 1,000 vulnerabilities caused by outdated OpenSSH versions; 27 percent of them have publicly available exploits. For example, 58 percent of companies have vulnerability CVE-2018-15473 in OpenSSH versions prior to 7.7. The vulnerability allows learning the usernames of system users. For this, all attackers have to do is to send a specially crafted authentication request. If an identifier in the request does not exist in the system, the server will respond with an error message, and if the identifier exists, the connection will be interrupted without a response. This process can be automated using a publicly available tool. Our experts have exploited this vulnerability many times during penetration tests.



```
msf auxiliary(scanner/ssh/ssh_enumusers) > set CHECK_FALSE true
CHECK_FALSE => true
msf auxiliary(scanner/ssh/ssh_enumusers) > set rhosts [redacted]
rhosts => [redacted]
msf auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE ssh.txt
USER_FILE => ssh.txt
msf auxiliary(scanner/ssh/ssh_enumusers) > run

[*] [redacted]:22 - SSH - Using malformed packet technique
[*] [redacted]:22 - SSH - Checking for false positives
[*] [redacted]:22 - SSH - Starting scan
[+] [redacted]:22 - SSH - User 'root' found
[+] [redacted]:22 - SSH - User '[redacted]' found
[+] [redacted]:22 - SSH - User '[redacted]' found
[+] [redacted]:22 - SSH - User '[redacted]' found
[+] [redacted]:22 - SSH - User '[redacted]' found
[+] [redacted]:22 - SSH - User '[redacted]' found
[+] [redacted]:22 - SSH - User '[redacted]' found
```

Figure 9. Exploitation of vulnerability CVE-2018-15473

Insecure versions of the SSL/TLS protocol and outdated versions of the OpenSSL cryptographic library made up 16 percent of all vulnerabilities. Each tested company has hosts vulnerable to the SWEET32 attack (CVE-2016-2183) and 84 percent of companies are vulnerable to the POODLE attack (CVE-2014-3566). To perform such attacks, attackers must be able to intercept and modify information between the client and the server. By successfully exploiting the vulnerability, attackers can recover encrypted data, such as HTTP cookies. It is possible to prevent SWEET32 attacks by abandoning the use of block encryption algorithms with 64-bit block lengths (Blowfish, DES, 3DES). To protect from POODLE, stop using SSL version 3. If that is not possible, enable the TLS_FALLBACK_SCSV mechanism.

Over half (53%) of companies have hosts vulnerable to the DROWN attack. The attack is possible because of vulnerability CVE-2016-0800 in the implementation of the SSL version 2 protocol. Under certain conditions, an attacker can obtain session keys transmitted in SSL sessions and thus obtain access to all encrypted information.

At two companies, scanning revealed servers vulnerable to the Heartbleed vulnerability (CVE-2014-0160) in OpenSSL 1.0.1. This big-name vulnerability was all over the headlines in 2014. Heartbleed allows extracting private encryption keys and user passwords from server RAM. The vulnerability has a ready-made exploit.

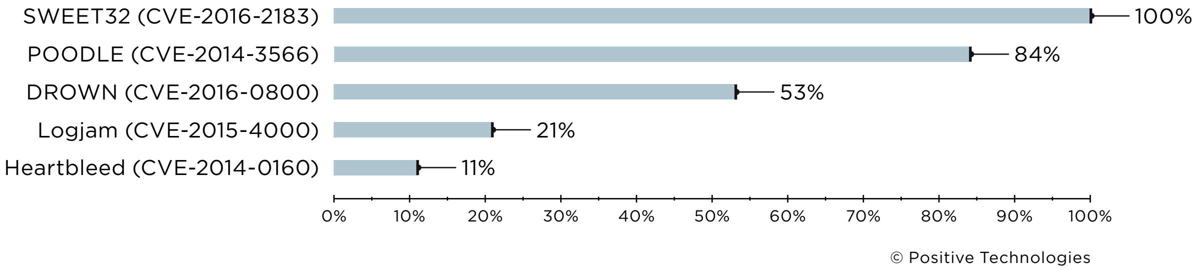


Figure 10. Known SSL/TLS and OpenSSL vulnerabilities (percentage of companies)

Code vulnerabilities oblige software developers to regularly release security updates and companies to keep their installed software up to date. We matched each such vulnerability with software weaknesses from the Common Weakness Enumeration (CWE) list. The result: 30 percent of vulnerabilities detected in outdated software versions and web application code are among the most dangerous program code errors according to MITRE (2019 CWE Top 25 Most Dangerous Software Errors). The MITRE rating includes the most common critical errors that can be easily found and exploited by attackers in order to steal information, cause denial of service, or obtain full control over a vulnerable application.

Vulnerability types

For convenience, we have categorized all the detected vulnerabilities. These are the most common categories, for which vulnerabilities were identified at half or more of the tested companies.

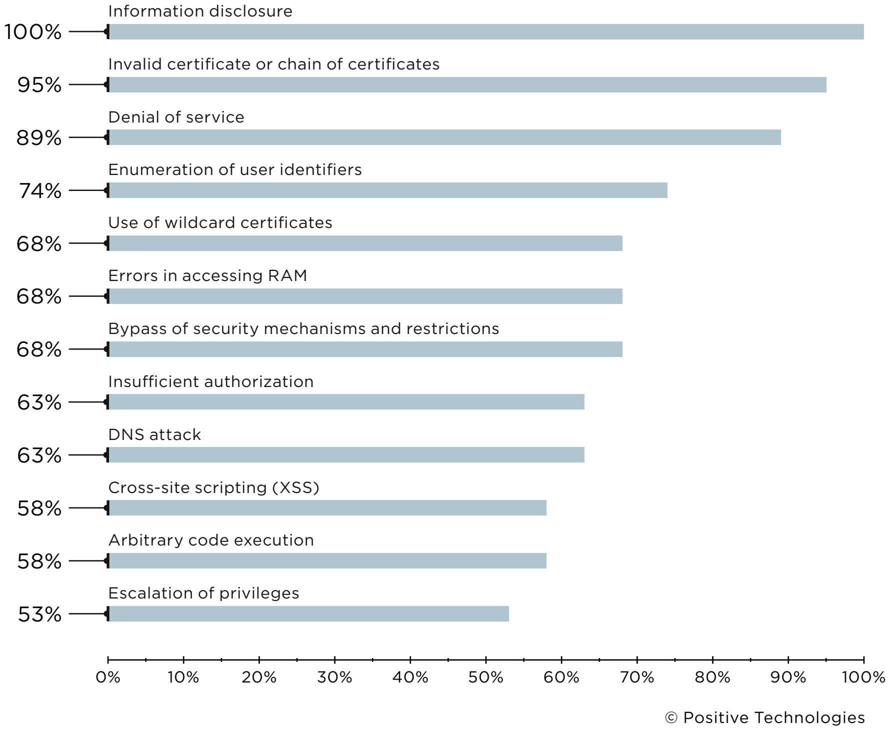


Figure 11. Most common vulnerability categories (percentage of companies)

Configuration flaws related to SSL certificates were present on a number of hosts at 95 percent of companies. Such flaws include certificates with an invalid signature, self-signed certificates, expired certificates, and chains of certificates based on a non-trusted certificate. Wildcard certificates are used at 68 percent of companies. Such certificates differ from regular ones in that they are issued not only for a domain name, but also for all subdomains of the next level. Use of wildcard certificates helps companies to save money and more easily keep certificates up to date. However, if a certificate is compromised, multiple applications (not just one) will be put at risk.

Vulnerabilities related to memory allocation and deallocation have been placed in the "Errors in accessing RAM" category. Depending on conditions and exploitation scenarios, these vulnerabilities may lead to such consequences as data damage, memory leaks, software crashes, or execution of arbitrary code.

Arbitrary code execution

Almost two thirds (64%) of detected arbitrary code execution vulnerabilities were of high severity. The most common vulnerability (detected at 37% of companies) was CVE-2017-12617 in Apache Tomcat. Attackers can use this vulnerability to upload a JSP file to a vulnerable server and execute code contained in this file.

There are public exploits for 16 percent of the detected arbitrary code execution vulnerabilities. An example of such vulnerabilities is CVE-2015-1635 (MS15-034) in Windows server versions. The vulnerability allows specially crafted HTTP requests to cause remote code execution with maximum system privileges. Fortunately, this dangerous vulnerability is rarely encountered today: it was detected on the servers of only two companies.

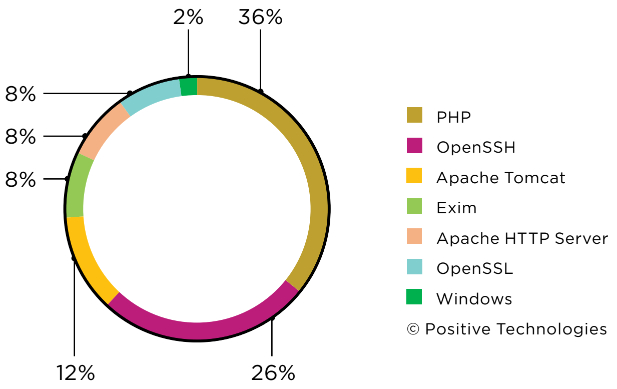
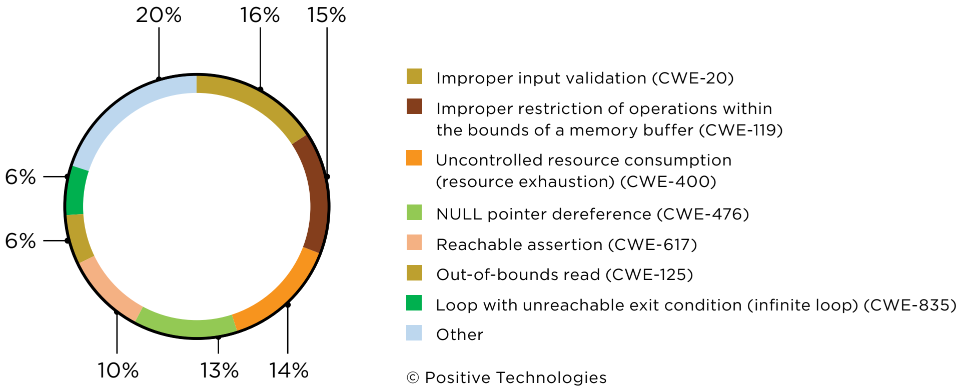


Figure 12. Vulnerable software (percentage of detected arbitrary code execution vulnerabilities)

Denial of service

Denial of service vulnerabilities are mainly related to input validation errors, incorrect memory handling (errors in handling stack variables, heap variables, or pointers), and uncontrolled resource allocation. For example, OpenSSH vulnerability CVE-2016-6515 is caused by the lack of restrictions on the number of characters when entering a password. By using a publicly available exploit, attackers can send a password thousands of characters long, overloading the device processor. Exploitation of this and similar vulnerabilities can disrupt availability of services on the network perimeter, which can lead to financial and reputational losses.

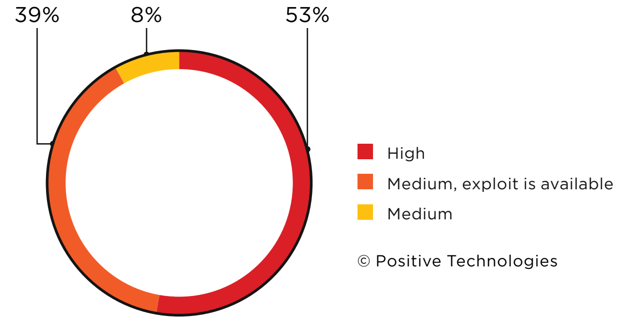


© Positive Technologies

Figure 13. Software errors and flaws capable of causing denial of service (percentage of denial of service vulnerabilities)

Escalation of privileges

On the network perimeter, 53 percent of companies harbor software vulnerabilities that allow attackers who have accessed a host with the rights of an ordinary user to escalate privileges. Over a third of these vulnerabilities have publicly available exploits. For example, if a host uses an OpenSSH version prior to 7.4, attackers who have bruteforced credentials can obtain maximum privileges by using a publicly available exploit for vulnerability CVE-2016-10010. With maximum privileges, attackers can edit and delete any information on the host, which creates a risk of denial of service (DoS). On web servers, these vulnerabilities may also lead to website defacement, unauthorized database access, and attacks on clients. In addition, attackers can pivot to target other hosts on the network. For example, privileges of the root user allow viewing password hashes of other users from the file /etc/shadow. Recovering these passwords can be helpful for attempting to connect to other services.



© Positive Technologies

Figure 14. Privilege escalation vulnerabilities by risk level and availability of exploits

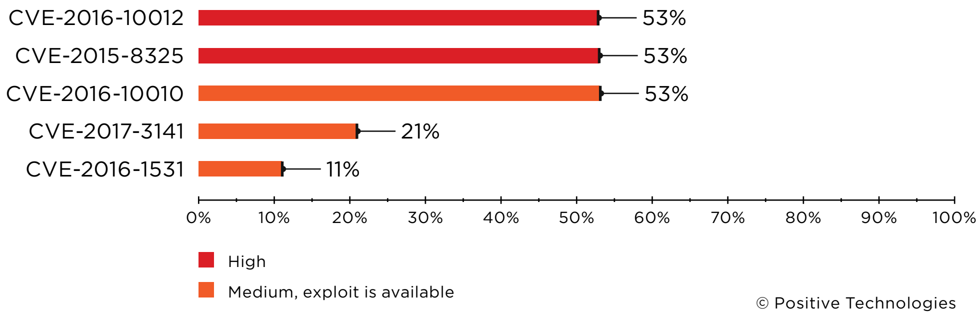


Figure 15. Five most dangerous privilege escalation vulnerabilities (percentage of companies)

Information disclosure

Another issue found at all tested companies was disclosure by hosts of technical information: examples include the contents of configuration files, routing to the scanned host, OS versions, and supported protocol versions. The more information about the system attackers can collect, the higher the chance of a successful attack. The culprit is insecure configuration of services. Of companies with the NTP service available on the network perimeter, 92 percent had not configured systems to ignore information packets. By requesting NTP variables, attackers can then identify the OS version, NTP software version, processor type, and time settings. SNMP connections are allowed at 58 percent of companies. SNMP is normally used to monitor various settings of network devices. Unfortunately, this interface can be a threat to perimeter security. At two companies, the SNMP Community String had the value "public" with read-only permissions. In these cases, attackers can use the snmpwalk utility to obtain detailed information about the system for subsequent attacks.

The most common vulnerabilities that can lead to disclosure of confidential information (CVE-2016-2183, CVE-2014-3566, CVE-2013-2566) are related to outdated SSL/TLS versions. Some vulnerabilities are related to the use of insufficiently strong cryptographic mechanisms and weak keys. SSL certificates of 68 percent of companies use SHA-1 and MD5 hash functions. There are well-known attacks aimed at exploiting collisions in these algorithms, allowing attackers to compromise the certificate. Certificates of 53 percent of companies use RSA keys with a length of 1024 bits or less. A weak secret RSA key in SSL/TLS allows an attacker to intercept a session by masquerading as a legitimate server. The recommended NIST length of an RSA key is at least 2048 bits.

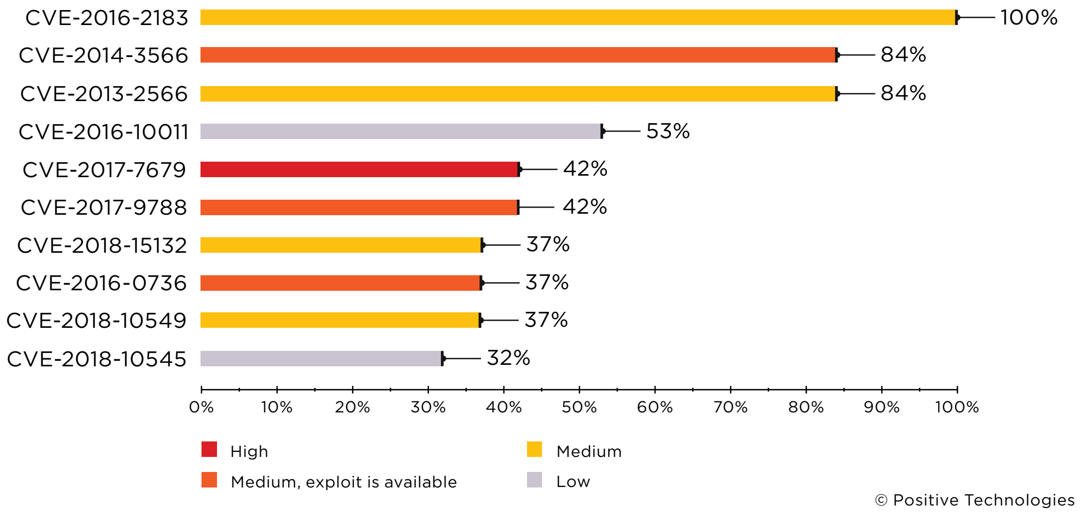


Figure 16. Common software vulnerabilities related to information disclosure (percentage of companies)

Conclusions and recommendations

Network perimeters of most tested corporate information systems remain extremely vulnerable to external attacks. Our automated security assessment proved that all companies have network services available for connection on their network perimeter, allowing any Internet user to bruteforce credentials to these services and exploit software vulnerabilities. In external penetration tests by our experts in 2019, 61 percent of successful attack vectors that breached the perimeter included bruteforcing of passwords.

Even in 2020, there are still companies vulnerable to Heartbleed and WannaCry. The most frequent vulnerabilities detected during automated assessment date back to 2013–2017, which indicates a lack of recent software updates. We recommend minimizing the number of services on the network perimeter and making sure that accessible interfaces truly need to be available from the Internet. If so, ensure that these interfaces are configured securely and install updates to patch any known vulnerabilities.

Often, it is not so easy. International vulnerability databases annually publish information about thousands of new flaws. In addition, corporate IT infrastructures inevitably go through changes, each of which potentially entails a security risk. All this makes vulnerability management a complex task that requires proper instrumental solutions. With modern security assessment tools, companies can go beyond automating resource inventories and vulnerability searches to assess security policy compliance across the entire infrastructure.

However, each vulnerability flagged during automated scanning must be verified. Each confirmed vulnerability is a threat: since an intruder could pick any of the potential attack vectors, it is important to remediate them all. In this regard, scanning only gives a general idea of the company's state of security. To get a complete picture, it is vital to combine automated scanning with penetration testing.

Therefore, automated scanning is only the first step toward achieving an acceptable level of security. Subsequent steps should include verification, triage, and remediation of risks and their causes. This should be a recurring process that will help to minimize the risk of successful attacks against corporate infrastructure.

MaxPatrol 8 scan modes

The MaxPatrol 8 vulnerability and compliance management solution has three scan modes: Pentest, Audit, and Compliance.

Pentest mode performs typical network scanning tasks: inventory, banner checks (analyzing messages transmitted by applications), fuzzing, and bruteforcing of credentials. Also included: special checks for web application and database security. This mode requires minimum knowledge of the tested system (black-box method).

Audit mode generates an inventory of hardware and software, OS settings, services, databases, applications, and security tools. It identifies vulnerabilities, misconfigurations, and uninstalled updates. This mode uses capabilities available to internal attackers with access to scanned hosts.

Compliance mode allows checking compliance with international standards, industry guidelines, and corporate policies. This mode includes Audit mode checks, such as identification of host software, but also contains additional checks to verify whether a scanned object complies with requirements.

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.