RESULTS OF PENETRATION TESTS IN 2022

Positive Technologies

ptsecurity.com

Contents

About the research

A company's protection system needs to be checked from the outside. First of all, it is necessary to check whether an external or internal attacker can perform a successful attack and trigger business-critical events. This can be achieved by conducting a penetration test.

> A penetration test, or a pentest, is a simulation of real attacker actions. We recommend paying special attention to techniques that have proved successful in a penetration test and taking these conclusions into account when building protection, monitoring, and incident response systems at your company.

The analysis is based on 53 internal and external penetration tests conducted at 30 organizations in the second half of 2021 and the first half of 2022. For the research, we selected only those tests in which no significant restrictions were imposed on pentester actions and the project scope was sufficient to get an objective assessment of the security level. The study included only organizations that allowed Positive Technologies to use anonymized data for research purposes.

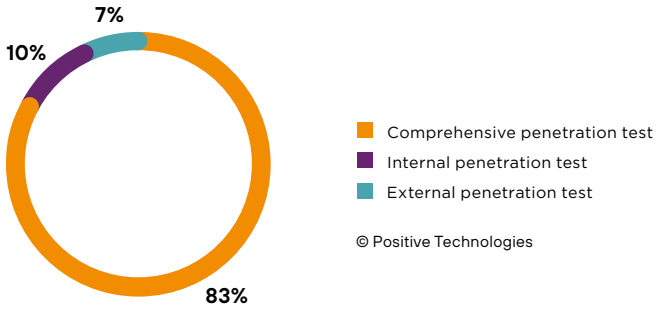


Figure 1. Percentage of conducted penetration tests

12 red/blue team exercises

In total, Positive Technologies performed: nine assessments that included verification of business-critical events

Most of the tested organizations (63%) are financial and manufacturing companies, as well as government institutions.

> 57% of tested companies are among the largest companies in Russia by sales volume according to RAEX-600.

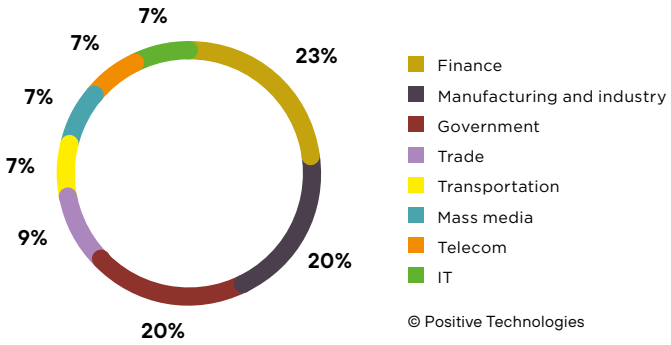


Figure 2. Distribution of tested companies by industry

The report includes only attacks on companies' infrastructure; it did not include social engineering attacks or attacks on wireless networks. Please note that finding the maximum possible number of vulnerabilities is not the objective of a penetration test. The reports on conducted penetration tests include vulnerabilities exploited by pentesters to achieve the goals of these assessments or detected while searching for attack vectors. Each chapter contains relevant security recommendations.

The research includes the MITRE ATT&CK heat map, which shows popular techniques and sub-techniques that were successfully used by Positive Technologies' pentesters. This map can be especially useful for quick incident response and infosec specialists, because the pentesters imitated the actions of real attackers.

Main results

96% of companies proved to be vulnerable to external attacks. The remaining 4% is made up of one company where pentesters managed to access a buffer zone between the Internet and the intranet (DMZ). It is worth noting that this company had undergone multiple penetration tests in the past and had done thorough work on mistakes.

100% of companies were vulnerable to having control of infrastructure fully taken over from the inside.

On average, it took pentesters **five days and four hours** to access the internal networks of organizations, and another **five days** to get the maximum privileges in the infrastructure. In **84%** of organizations, even a low-skilled attacker would be able to penetrate the LAN.

In total, we were able to confirm the feasibility of **89%** of events specified by the companies as business-critical. On average, it took **nine** days to verify the feasibility of a business-critical event. In total, real attackers would need a month to trigger all **89%** of business-critical events. In some cases, attackers did not even need maximum privileges in the domain. Most business-critical events that pentesters managed to trigger were related to potential reputational damage (**61%** of events), regulatory sanctions (**57%**), and financial loss (**39%**). Business-critical events are defined by each organization individually: for example, for a software developer, it is usually a supply chain attack; for a bank—theft of money above a defined threshold, theft of customer personal data, disruption of services; for government agencies—shutting down of a critical information system and leaks of citizen data.

During external penetration tests, **74%** of organizations proved to be vulnerable to employee domain credential compromise, and in **90%** of organizations attackers would be able to access sensitive information.

In **7%** of the organizations, pentesters found traces of compromise, which means that these companies had already been hacked by attackers before.

Critical vulnerabilities related to password policy flaws were detected in **70%** of organizations. **67%** of companies had vulnerabilities related to lack of updates, and **53%** of companies contained critical vulnerabilities in web application code.

Companies' security level

The level of protection against external and internal attacks in the tested companies was in most cases low: many confirmed attack vectors aimed at accessing critical resources were found, and potential attackers would not even need to be highly qualified to apply these vectors. In internal penetration tests, 96% of organizations were assessed as having a low level of security. As for external attacks, the situation was slightly better: 68% of organizations had a low level of security, and in 32%, this level was below average.

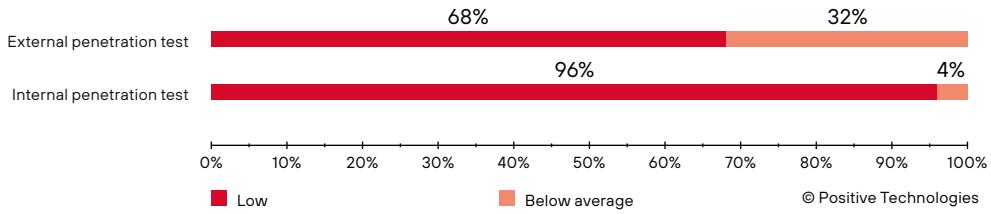


Figure 3. Security level of tested organizations (percentage of organizations)

> Overall security level is an expert assessment that takes into account the number of detected attack vectors including potential ones, the importance of compromised resources, as well as the complexity of attack vectors and the required attacker qualifications.

A strong sign of high-level information security in a company is the use of result-oriented security. The first step toward result-oriented security is preparing a list of business-critical events that make it impossible for a company to function normally. Next, it is necessary to identify the target and key systems in a company's infrastructure. Setting specific objectives of a penetration test (assets to be accessed) allows us to test the security of target and key systems. If your organization already has a mature information security system supported by a sufficient budget, the next step is to verify whether attackers can trigger business-critical events at your company.

By default, the purpose of an external pentest is to gain access to a company's internal network, while the main objective of an internal pentest is to obtain maximum privileges in a company's infrastructure.

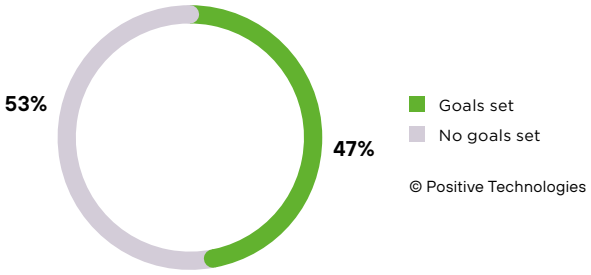


Figure 4. Projects in which specific goals were set versus projects without a goal

47% of the organizations set specific goals of a penetration test; **27%** of them wanted to check whether their business-critical events could be triggered. For example, software developers usually test the possibility of supply chain attacks on their customers. In this case, pentesters look for ways to access developers' servers and application source code in order to check and, if found, demonstrate the possibility of introducing a special code fragment into the final product version. If the code is successfully introduced, it means that a real attacker can introduce malicious code into this company's product in the same way.

To describe attacks, experts around the world use the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) matrix. We analyzed attack vectors used by pentesters and placed the 80 most commonly used techniques on the MITRE ATT&CK heat map. All the techniques and sub-techniques on this map are worth looking at, because a penetration test is a simulation of a real attack. Armed with knowledge about the approaches attackers may use, it is possible to ensure preventive protection and keep tabs on security incident monitoring and response. In particular, the exploit public-facing application technique deserves special attention. In internal penetration tests, this technique was successfully applied in all the tested organizations, and in almost all cases pentesters exploited web application protection flaws. Real-life attackers use a similar approach, securing your web applications is a must.

MITRE ATT&CK heat map

Initial Access

- Exploit Public-Facing Application
- External Remote Services
- Supply Chain Compromise
- Compromise Software Dependencies and Development Tools
- Valid Accounts
- Default Accounts
- Domain Accounts
- Local Accounts

Execution

- Command and Scripting Interpreter
- JavaScript
- PowerShell
- Python
- Unix Shell
- Windows Command Shell
- Container Administration Command
- Scheduled Task/Job
- At
- Scheduled Task
- Software Deployment Tools

Persistence

- Account Manipulation
- SSH Authorized Keys
- Create Account
- Domain Account
- Local Account
- External Remote Services
- Scheduled Task/Job
- At
- Scheduled Task
- Server Software Component
- Web Shell
- Valid Accounts
- Default Accounts
- Domain Accounts
- Local Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
- Sudo and Sudo Caching
- Access Token Manipulation
- Create Process with Token
- SID-History Injection
- Token Impersonation/ Theft
- Domain Policy Modification
- Group Policy Modification
- Exploitation for Privilege Escalation
- Scheduled Task/Job
- At
- Scheduled Task
- Valid Accounts
- Default Accounts
- Domain Accounts
- Local Accounts

Defense Evasion

- Access Token Manipulation
- Create Process with Token
- SID-History Injection
- Token Impersonation/ Theft
- Deobfuscate/Decode Files or Information
- Domain Policy Modification
- Group Policy Modification
- Exploitation for Defense Evasion
- Impair Defenses
- Disable or Modify System Firewall
- Downgrade Attack
- Indicator Removal on Host
- File Deletion
- Indirect Command Execution
- Masquerading
- Double File Extension
- Masquerade Task or Service
- Modify Registry
- Use Alternate Authentication Material
- Pass the Hash
- Pass the Ticket
- Web Session Cookie
- Valid Accounts
- Default Accounts
- Domain Accounts
- Local Accounts

Credential Access

- Adversary-in-the-Middle
- ARP Cache Poisoning
- LLMNR/NBT-NS Poisoning and SMB Relay
- Brute Force
- Credential Stuffing
- Password Cracking
- Password Guessing
- Password Spraying
- Credentials from Password Stores
- Password Managers
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Web Cookies
- OS Credential Dumping
- /etc/passwd and /etc/shadow
- Cached Domain Credentials
- DCSync
- LSA Secrets
- LSASS Memory
- Security Account Manager
- Steal or Forge Kerberos Tickets
- AS-REP Roasting
- Golden Ticket
- Kerberoasting
- Silver Ticket
- Steal Web Session Cookie
- Unsecured Credentials
- Bash History
- Cloud Instance Metadata API
- Container API
- Credentials in Files
- Credentials in Registry
- Private Keys

Discovery

- Account Discovery
- Domain Account
- Email Account
- Local Account
- Cloud Infrastructure Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Permission Groups Discovery
- Domain Groups
- Local Groups
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery

Lateral Movement

- Exploitation of Remote Services
- Lateral Tool Transfer
- Remote Service Session Hijacking
- SSH Hijacking
- Remote Services
- Distributed Component Object Model
- Remote Desktop Protocol
- SMB/Windows Admin Shares
- SSH
- VNC
- Software Deployment Tools
- Use Alternate Authentication Material
- Pass the Hash
- Pass the Ticket
- Web Session Cookie

Collection

- Adversary-in-the-Middle
- ARP Cache Poisoning
- LLMNR/NBT-NS Poisoning and SMB Relay
- Archive Collected Data
- Archive via Utility
- Data from Configuration Repository
- Network Device Configuration Dump
- SNMP (MIB Dump)
- Data from Information Repositories
- Code Repositories
- Confluence
- Sharepoint
- Data from Local System

Command and Control

- Application Layer Protocol
- Web Protocols
- Data Encoding
- Non-Standard Encoding
- Standard Encoding
- Encrypted Channel
- Asymmetric Cryptography
- Ingress Tool Transfer
- Protocol Tunneling
- Proxy
- External Proxy
- Internal Proxy
- Remote Access Software

Heat map of tactics, techniques and sub-techniques used by pentesters

Percentage of companies in which these techniques and sub-techniques were used:

<20% 21% 41% 66% 100%

Results of external penetration tests

In 96% of organizations, attackers would be able to breach the network perimeter and penetrate the internal network. The remaining 4% is a banking company where pentesters managed to access a buffer zone between the external and internal networks (DMZ). This company had undergone multiple penetration tests in the past and had done solid work on eliminating mistakes.

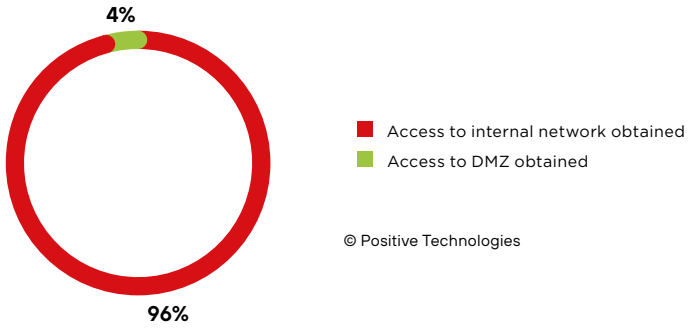


Figure 5. Results of external penetration tests (percentage of organizations)

At 96% of companies, our pentesters accessed the internal network.

On average, it takes five days and four hours to penetrate a company`s internal network, and the fastest attack took just one hour.

In 57% of the companies, a penetration vector consisted of no more than two steps[1]; on average, penetration would require four steps.

[1] A step in an attack is an action in which attackers obtain data or privileges needed to proceed further with the attack

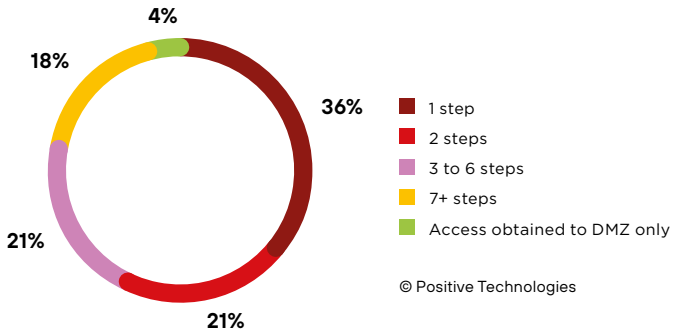


Figure 6. Minimum number of steps to penetrate the local network (percentage of companies)

Low complexity vectors were detected in 53% of organizations, which means that even low-skilled attackers armed with only public tools could conduct a successful attack on these companies.

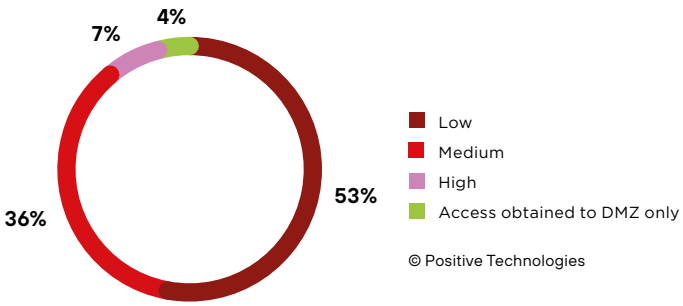


Figure 7. Minimum complexity of internal network penetration vectors (percentage of organizations)

Methods of internal network penetration

The main entry points were vulnerabilities and flaws in web application configurations: such vectors were identified at all companies without exception (DMZ was also accessed by exploiting web application flaws).

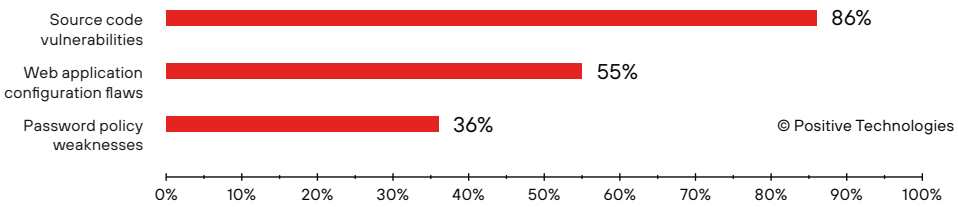


Figure 8. Protection flaws that allowed pentesters to access a LAN (percentage of organizations)

It took our pentesters only one hour to discover the vulnerability that was subsequently used in an attack aimed at gaining access to the LAN. This attack was the fastest of all attacks in the 2021–2022 penetration tests.

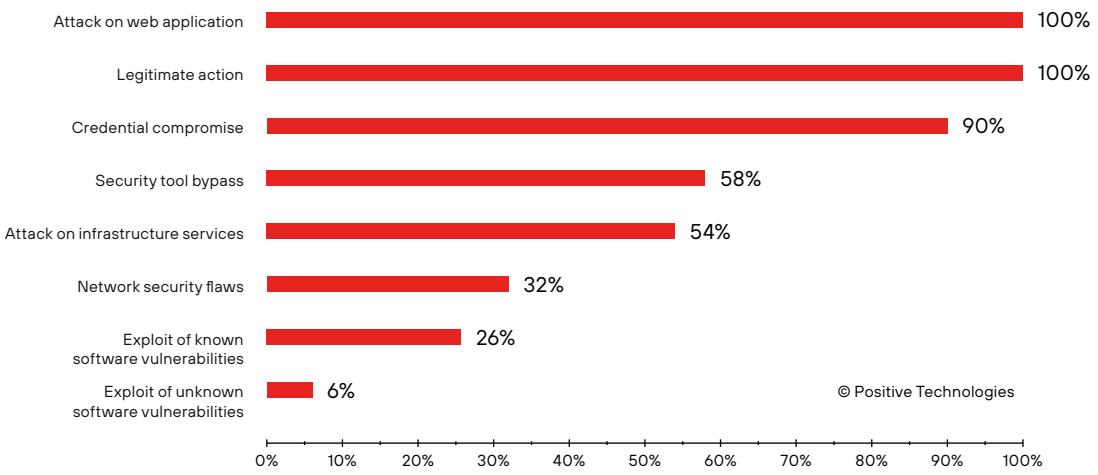


Figure 9. Successful attacks in external penetration tests (percentage of organizations)

Legitimate actions are performed by ordinary users and system administrators as part of their routine life and job. However, legitimate actions can also be part of an attack vector. It is not easy for an information security specialist to tell which legitimate events have been initiated by criminals. Legitimate actions include changing user passwords; remote connection to system resources; collecting information about a network, domain, and users; creating a memory dump of the lsass.exe process; or uploading files to a server using application's built-in functions.

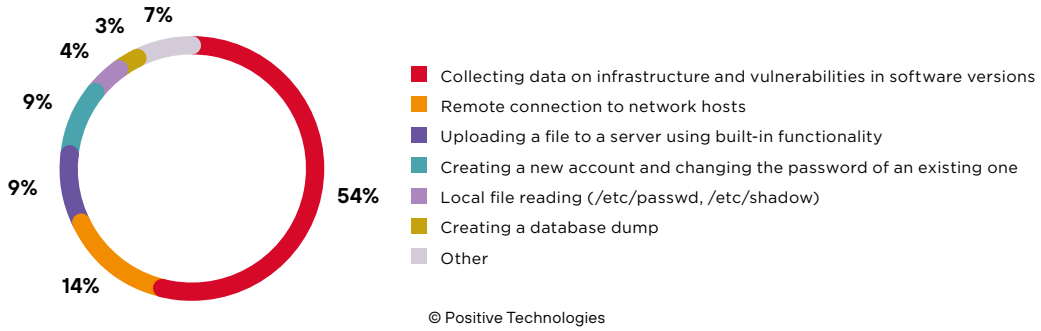


Figure 10. Legitimate actions that allowed pentesters to perform attacks during external penetration tests

To distinguish between legitimate actions and those initiated by attackers, user activity should be strictly monitored, especially when it comes to users with elevated privileges, such as system administrators.

We also recommend implementing two-factor authentication to protect critical resources. Two-factor authentication makes it much more difficult for attackers to move laterally within a network and reduces their ability to affect target and key systems of the company.

Web application vulnerabilities

At least one attack vector related to exploitation of vulnerabilities or web application configuration flaws (Exploit Public-Facing Application) was detected in every tested organization. The most common attack vector was exploitation of vulnerabilities in CMS Bitrix: these vulnerabilities were used by attackers to access the internal networks of 10 organizations. Figure 11 shows one such attack vector.

> 1C-Bitrix, whose vulnerabilities allowed attackers to access internal networks in most tested organizations, releases security updates when needed, for example for CVE-2022-27228. We recommend regularly checking for security updates and installing them promptly.

For recommendations on how to implement a vulnerability management process, see this article.

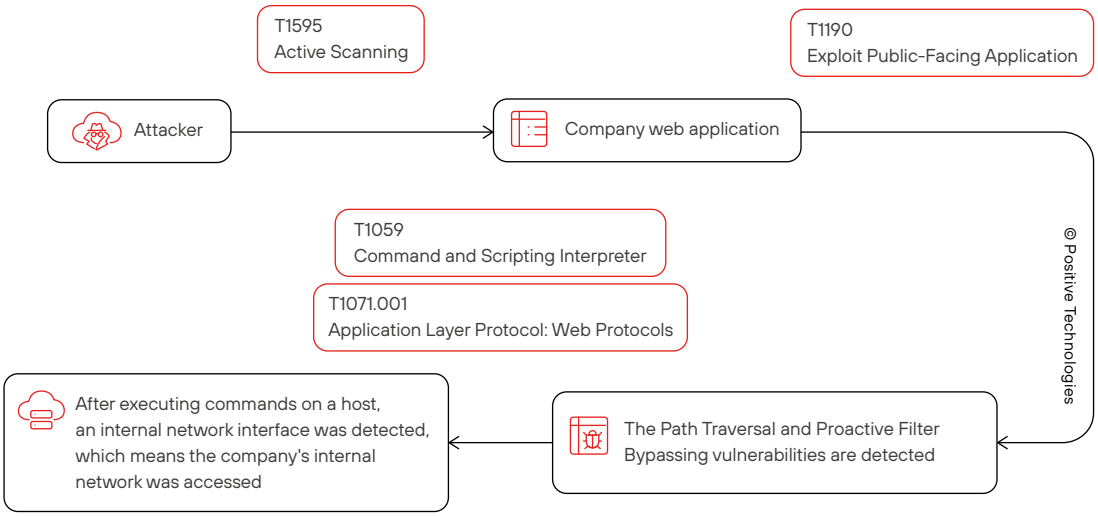


Figure 11. An example of an attack exploiting vulnerabilities in Bitrix CMS in order to penetrate an organization's internal network

The second most common network penetration point was vulnerabilities in Microsoft Exchange. WebTutor rounds out the top three. Our pentesters exploited such vulnerabilities in five organizations in total.

Check for updates and install them timely.

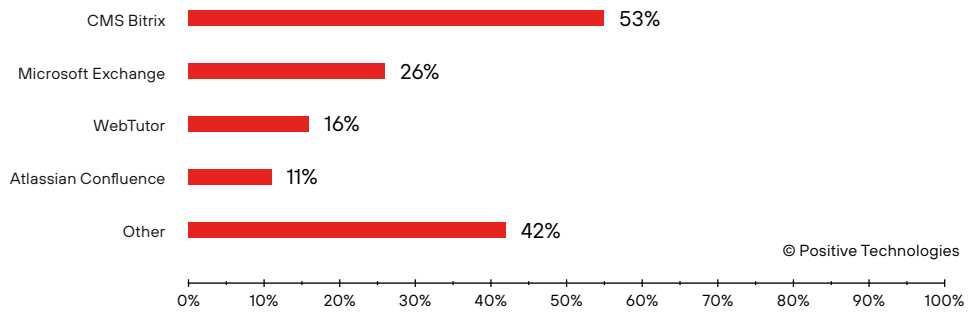


Figure 12. Vulnerable software that served as a point of entry into the network (percentage of organizations)

14% of LAN penetration vectors that exploited vulnerabilities in web applications included exploitation of zero-day vulnerabilities. Four zero-day vulnerabilities were detected in external penetration tests.

Zero-day vulnerabilities in Bitrix CMS were exploited in four organizations. Other zero-day vulnerabilities were detected in video conferencing software and a CRM system. Positive Technologies adheres to the principles of responsible disclosure of vulnerability information. Software manufacturers are informed about all detected vulnerabilities.

In most cases, critical vulnerabilities were related to weak password requirements and a lack of software updates. Critical vulnerabilities in web application code were detected in 53% of the tested companies.

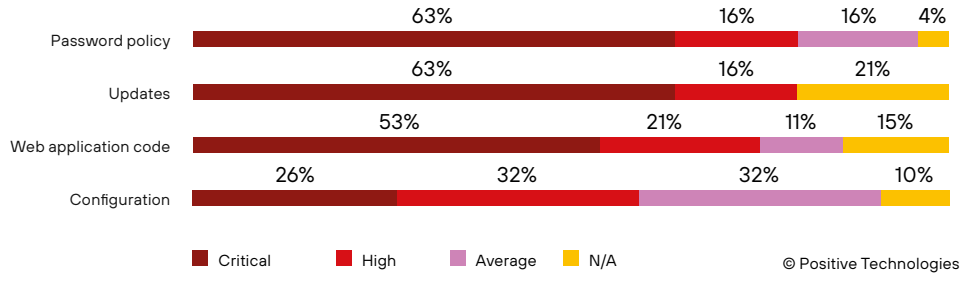


Figure 13. Maximim vulnerability severity by category (percentage of organizations)

Perimeter vulnerabilities

96% of organizations were vulnerable to attacks on internal network resources, and in nine out of 10 organizations, a potential attacker could gain unauthorized access to sensitive information.

To protect the perimeter, perform security assessment of web applications regularly.

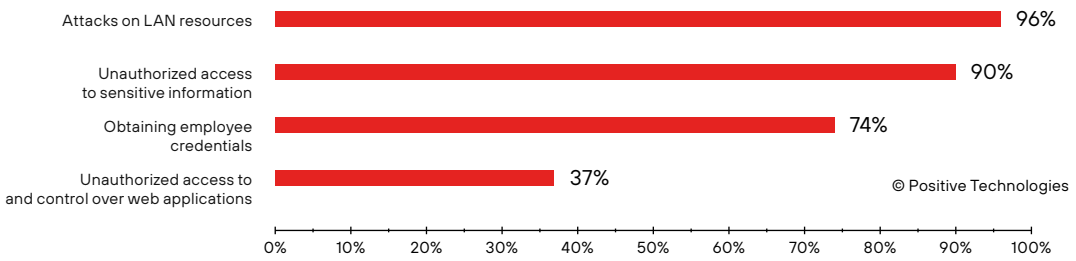


Figure 14. Common security threats identified in external penetration tests (percentage of organizations)

Confidential information to which attackers could gain access included trade secrets. Attackers can use this information to demand a ransom for non-disclosure or to sell it to the victim's competitors.

In addition to accessing a company's internal network, an attack on a network perimeter may cause other negative consequences, such as web application defacement, modification of information on official resources, injection of malicious code to attack the victim's customers, theft of employee credentials, and access to corporate resources and mail followed by spam and phishing.

Brief conclusions of external penetration tests

We recommend paying special attention to password policy and web application security. These two factors allowed us to access the internal networks of many organizations. Detailed recommendations on setting up a secure password policy can be found in the chapter "Password policy flaws". To protect web applications, Positive Technologies recommends conducting regular security assessments, implementing a vulnerability management process, and using application-level firewalls to protect against attacks.

Results of internal penetration tests

An internal penetration test assesses how well the IT infrastructure is protected from attacks conducted by an internal attacker who can connect to a company's LAN.

In 100% of tested companies, we managed to gain control over the domain.

It usually takes five days to obtain maximum privileges in an organization`s domain, and the quickest attack was performed in just one hour. On average, nine steps were required to obtain maximum privileges in the domain.

It took an average of 10 days to trigger a non-tolerable event.

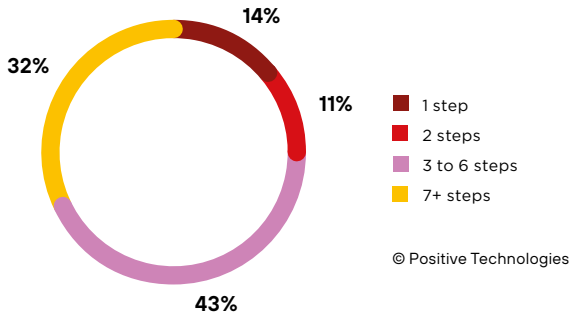


Figure 15. Minimum number of steps needed to gain the maximum privileges in the domain (percentage of organizations)

On average, each organization had two high, medium, and low-complexity vectors for obtaining maximum privileges in the domain. One of the organizations had five low-complexity vectors for obtaining maximum privileges in the domain.

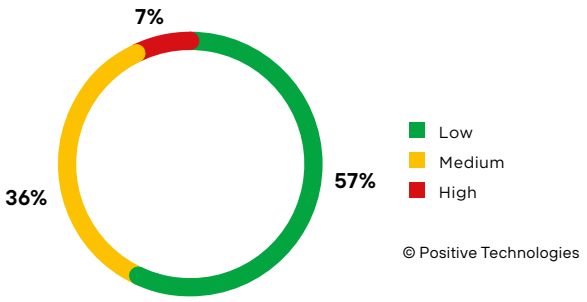


Figure 16. Minimum complexity of attack vectors aimed at obtaining maximum privileges in the domain (percentage of organizations)

> At 57% of the tested companies, there was a simple way to gain control over the infrastructure.

Attackers would need only basic knowledge of how to attack information systems and could use publicly available exploits or automated software to perform attacks.

> The attack vector complexity depends on the attacker qualification required to perform an attack and the number of actions needed to achieve the goal.

In one organization, pentesters managed to compromise the domain administrator's account as early as during an external penetration test. Password policy turned out to be a weakness not only in this organization: critical and high-risk vulnerabilities related to password policy flaws were detected in 85% of organizations. In 60% of companies, pentesters found critical and high-risk vulnerabilities related to the use of outdated software versions.

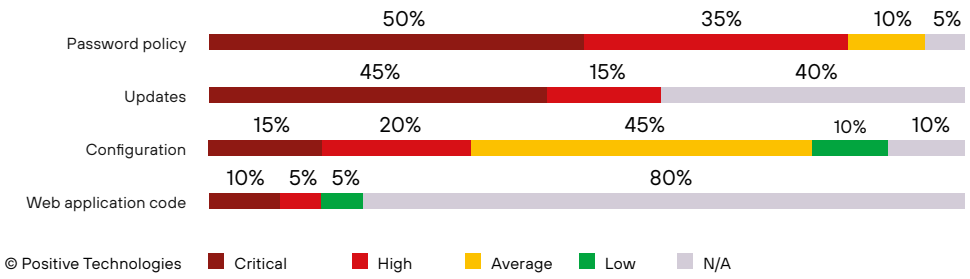


Figure 17. Vulnerabilities and security flaws detected during internal penetration tests by severity level (percentage of organizations)

In one company, an external attacker could use the Autodiscover service in Microsoft Exchange to collect information about the organization and then bruteforce credentials to penetrate the LAN and gain maximum privileges in the domain (see Figure 18). After accessing the server in the internal network, the attacker could obtain domain administrator privileges in just two steps.

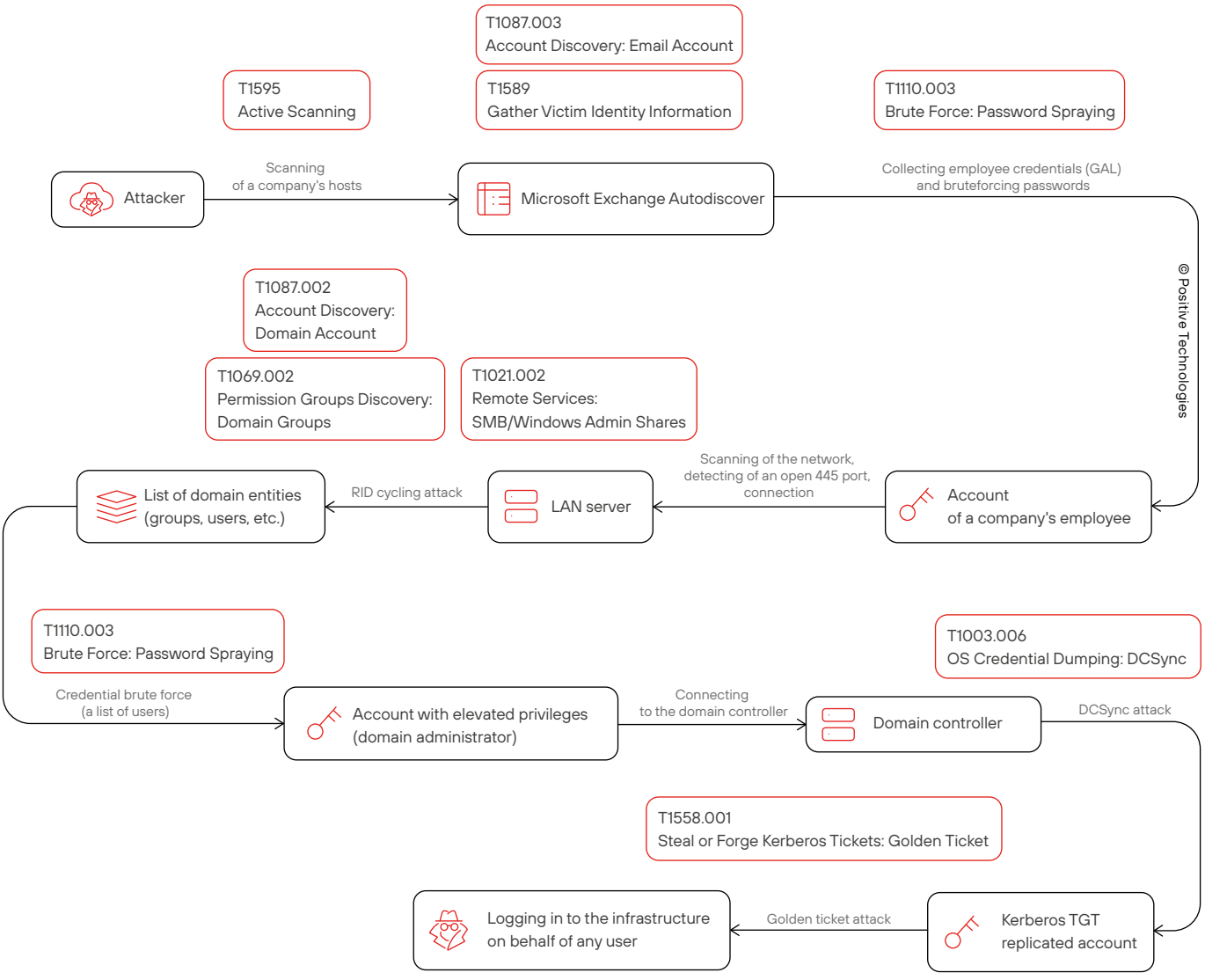


Figure 18. Example of an attack vector from penetrating the LAN to obtaining maximum privileges in the domain

Positive Technologies recommends implementing a strict password policy and using two-factor authentication to access critical resources.

In 93% of the organizations, our pentesters replicated the account krbtgt and obtained the NT password hash of the krbtgt user. With this data, real attackers can conduct a golden ticket attack and gain access to the network with any privileges. Our study revealed that a potential attacker could conduct a golden ticket attack in almost all the tested organizations. If successful, attackers can access any domain resources with any privileges. However, penetration tests normally have a strict framework agreed upon in advance with a company, which is why golden ticket attacks were not carried out.

> If the krbtgt account is compromised, the password for that account should be changed twice, and the incident should be thoroughly investigated. If it is impossible to determine whether an attacker is present in your system at the time of a check, we recommend reinstalling the operating system on the computers that may have been compromised.

What pentesters do in the internal network

In all tested organizations, pentesters conducted credential brute-force attacks to move laterally within an internal network and access various resources. They mainly used password spraying (49%) and password guessing (33%), and sometimes they used password cracking (16%) sub-techniques.

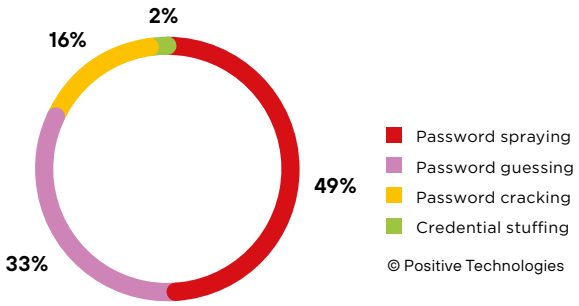


Figure 19. Credential brute force: percentage of sub-techniques used by pentesters

Password spraying is a password brute-force attack performed using a list of popular dictionary passwords and user IDs. Attackers take one password and start guessing an identifier for it. This method helps to avoid the account being blocked.

Password guessing is an attack that involves bruteforcing account passwords. To facilitate the task, password dictionaries, previously compromised passwords, and information about company password policy can be used.

Password cracking is an attack aimed at recovering a password using an existing hash sum or other obtained information, for example if reversible coding is used to store passwords.

In addition to brute force, pentesters collected credentials from regular user files (79%), replicated data from Active Directory (93%), found them in a memory dump of the lsass.exe process (68%), and obtained them in Kerberoasting attacks (36%).

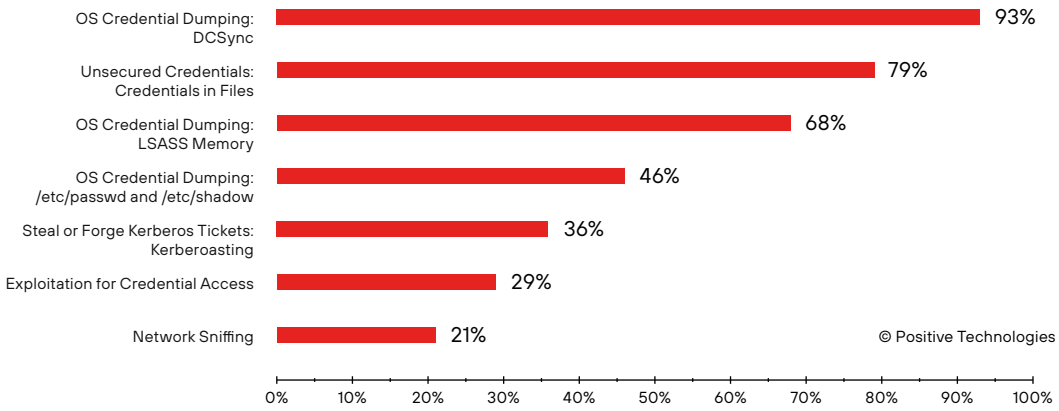


Figure 20. Methods of obtaining credentials (percentage of companies)

An example of a Kerberoasting attack is shown in Figure 21. Pentesters used vulnerabilities related to name spoofing in Active Directory (CVE-2021-42278) and spoofing requests to KDC (CVE-2021-42287). In both cases, exploitation was aimed at privilege escalation.

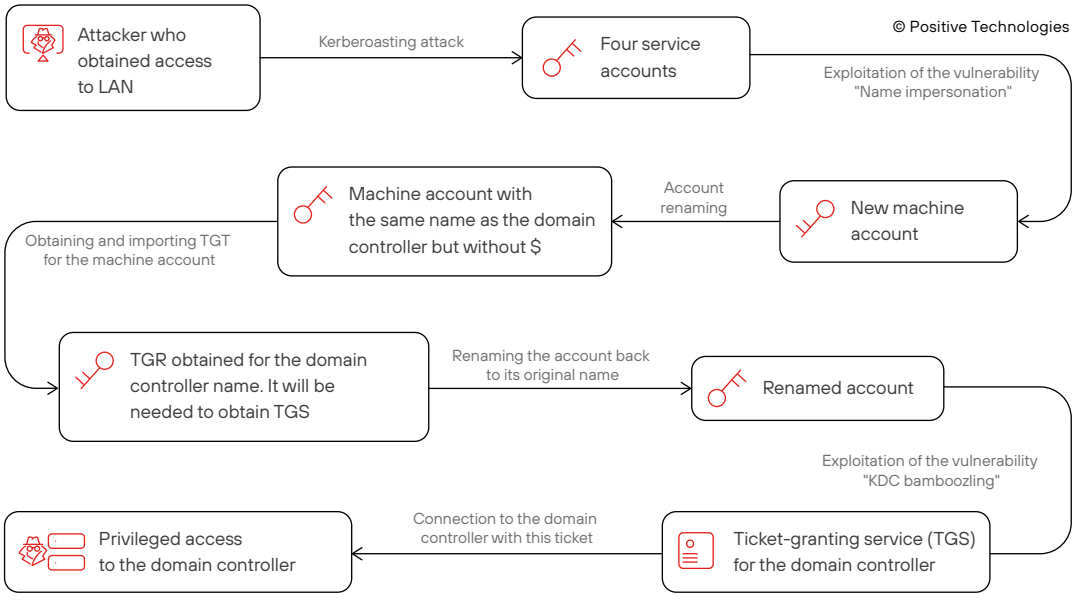


Figure 21. Example of an attack vector aimed at obtaining maximum privileges in the domain

To move laterally within an internal network and access resources, pentesters mostly used stolen pass-the-hash (93%) and pass-the-ticket (39%) authentication data, as well as connected to shared network resources (71%), RDP (61%) and SSH (57%) remote access protocols.

Use event monitoring systems to timely keep track of attacks.

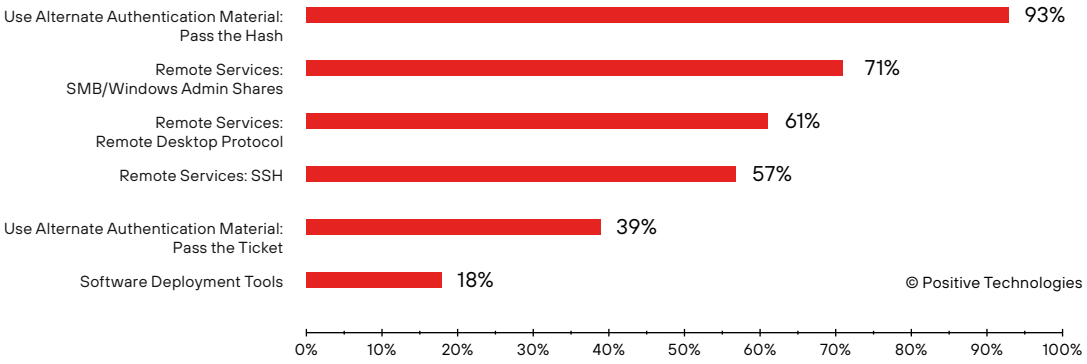


Figure 22. Main techniques used to move laterally within the internal network (percentage of organizations)

In order to elevate privileges in the infrastructure, attackers can use compromised local (68%) or domain (93%) user accounts or software vulnerabilities (89%). In 32% of organizations, pentesters used access token manipulation. For example, an attacker could duplicate an access token for a user and act on this user's behalf.

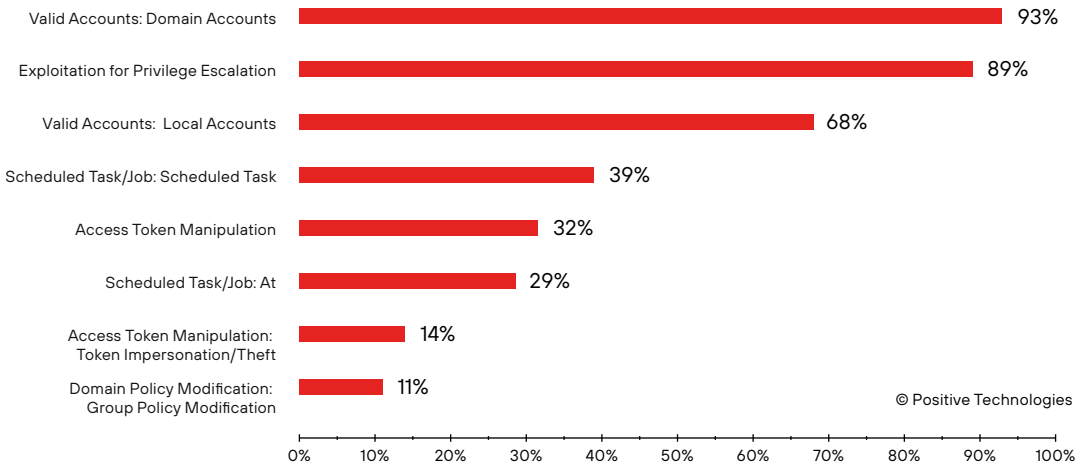


Figure 23. Main techniques and sub-techniques used by pentesters to elevate privileges (percentage of organizations)

Among successful attacks, the most frequently used techniques were credential brute force and legitimate actions: these methods were used in every tested organization.

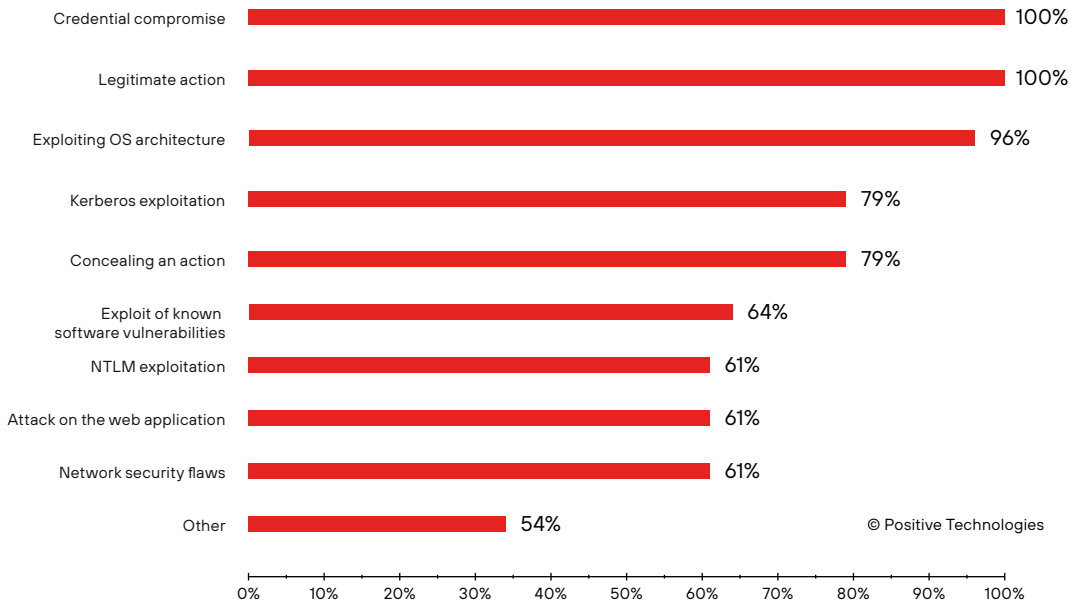


Figure 24. Successful attacks in internal pentests (percentage of organizations)

In most cases, legitimate actions included collecting data about network hosts and vulnerable software versions (used in 36% of all attacks). The second place belongs to file uploading (17%); by files we mean software that pentesters needed to perform attacks. The third most frequently used technique was remote connection to company resources (12%). For this, pentesters often used publicly available protocols, such as RDP and SSH.

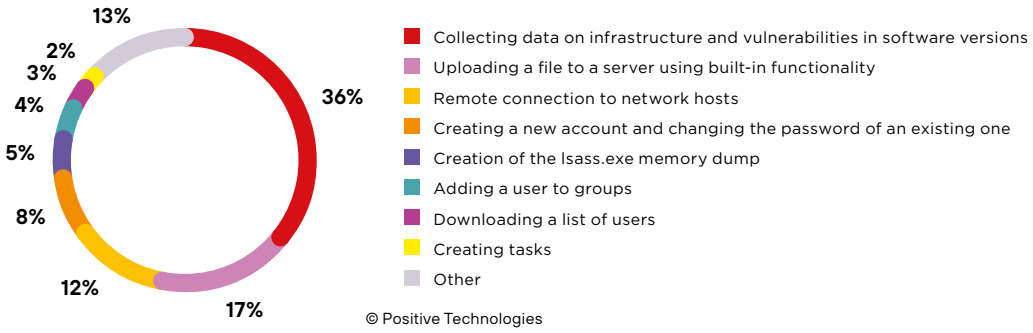


Figure 25. Legitimate actions in the system during internal penetration tests (percentage of all attacks)

The first five techniques in the list of the MITRE ATT&CK matrix below are related to credential brute force and use, as well as to the analysis of files and directories on the companies' servers. These techniques were used at all the tested organizations.

TOP 20 MITRE ATT&CK

№	Tactic	Technique	Sub-technique	Percentage of companies
1	Credential access	OS credential dumping		100%
2	Credential access	Brute force		100%
3	Discovery	File and directory discovery		100%
4	Persistence	Valid accounts		100%
5	Privilege escalation	Valid accounts		100%
6	Discovery	Account discovery		96%
7	Lateral movement	Use alternate authentication material	Pass the hash	93%
8	Credential access	OS credential dumping	DCSync	93%
9	Command and control	Application layer protocol	Web protocols	93%
10	Command and control	Ingress tool transfer		93%
11	Credential access	Unsecured credentials		93%
12	Execution	Command and scripting interpreter	Python	93%
13	Discovery	Permission groups discovery		89%
14	Discovery	Domain trust discovery		89%
15	Discovery	Network service discovery		89%
16	Initial Access	Exploit public-facing application		89%
17	Lateral movement	Remote services		89%
18	Execution	Command and scripting interpreter	PowerShell	86%
19	Lateral Movement	Exploitation of remote services		86%
20	Discovery	System network configuration discovery		82%

Vulnerabilities in internal networks and unacceptable attack consequences

In internal penetration tests, specialists managed to gain full control of domain resources in 100% of organizations. It was possible to access confidential information in 68% of the tested companies. Such confidential information included customer personal data and knowledge bases of the companies.

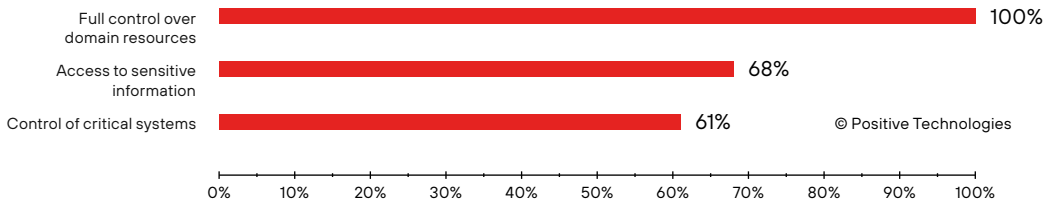


Figure 26. Top three security threats detected in internal penetration tests (percentage of organizations)

Software vendors turned out to be particularly vulnerable to supply chain attacks. As a result of such attacks, customer devices may be infected with malware, or sensitive information may be stolen by attackers.

In 47% of the studied companies, the specialists set specific pentest goals, and in 27% of the companies they verified whether business-critical events could be triggered. In most cases, such business-critical events included theft of critical information, access to the accounts of top managers, theft of funds, and shutdown of key business processes.

Interesting fact: it takes six days to disrupt an information system of a government organization and less than a month to steal money from a financial institution. In total, our specialists managed to trigger 42 out of 47 business-critical events specified by the tested companies. On average, it would take attackers **10 days** to trigger a business-critical event. Criminals would need two weeks to trigger 75% of business-critical events and a month to trigger 89% of such events.

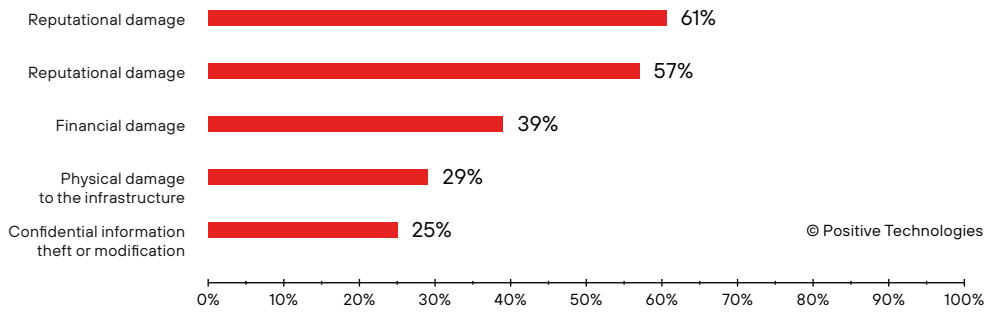
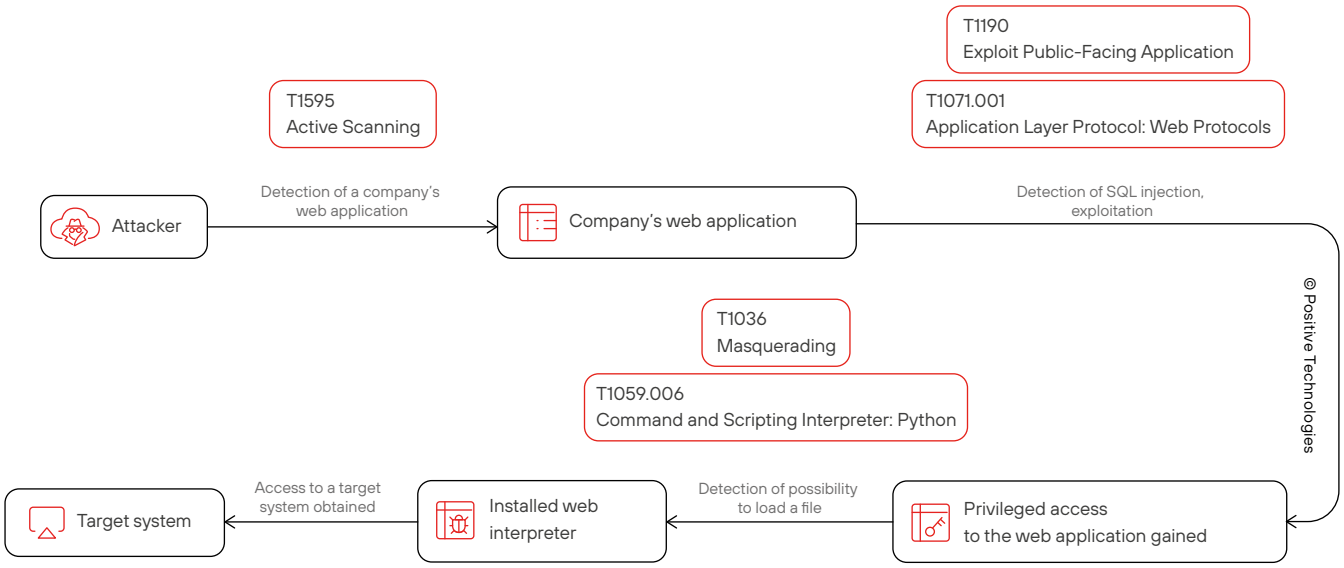


Figure 27. Main types of damage caused by the triggering of business-critical events (percentage of all verified events)

Unacceptable events may lead to reputational damage (61%), regulatory sanctions (57%), and financial loss (39%). One event can affect different aspects of company operations. For example, if attackers inject malicious code into a product, the targeted company may face reputational damage and lost profits due to customer churn, as well as fines and penalties.

In some cases, attackers did not even need maximum privileges in the domain in order to trigger a business-critical event. Figure 23 shows an example of one such attack.



Examples of consequences:

- Customer churn
- Financial damage
- Shutdown of a company's business operations
- Regulatory sanctions

Examples of systems:

Customer database
Accounting records
Customer—bank
Logistics
Customer support
Industrial process control

Attackers do not need maximum privileges in the domain in order to trigger a business-critical event

Figure 28. Example of an attack on a target system

The attack was carried out in two simple steps: 1) analyzing the web application, and 2) exploiting a vulnerability and uploading a web command line interpreter.

Brief conclusions of internal penetration tests

In all the tested organizations, our pentesters managed to obtain maximum privileges in the domain. They also verified whether non-tolerable events could be triggered and concluded that criminals would need a month to trigger 89% of events that would have a serious negative impact on company operations.

The most common techniques used by pentesters were brute force and subsequent use of employee credentials, as well as techniques aimed at analyzing infrastructure and user privileges, such as account discovery, permission groups discovery, and domain trust discovery. These techniques enabled pentesters to move silently within the infrastructure. Pay special attention to those techniques. Such attacks can be detected using event monitoring systems. By timely identifying an anomaly, you can save precious time and take measures to prevent an attack.

However, before implementing monitoring systems and building a vulnerability management process, focus on password policy: our pentesters managed to compromise employee domain accounts in 100% of organizations.

It is also vital to strengthen protection and monitoring not only for target[2] systems, but also for key[3] systems, because they are an intermediate link in an attack aimed at triggering a business-critical event.

[2] An information system whose compromise can lead to an unacceptable event for an organization

[3] An information system whose compromise would greatly simplify subsequent attacks on target systems

PASSWORD POLICY FLAWS

Top six most common passwords:

- admin
- 123456
- 123456Qwerty
- P@ssw0rd
- 123qweASD
- 12345678

Brute force time: one second

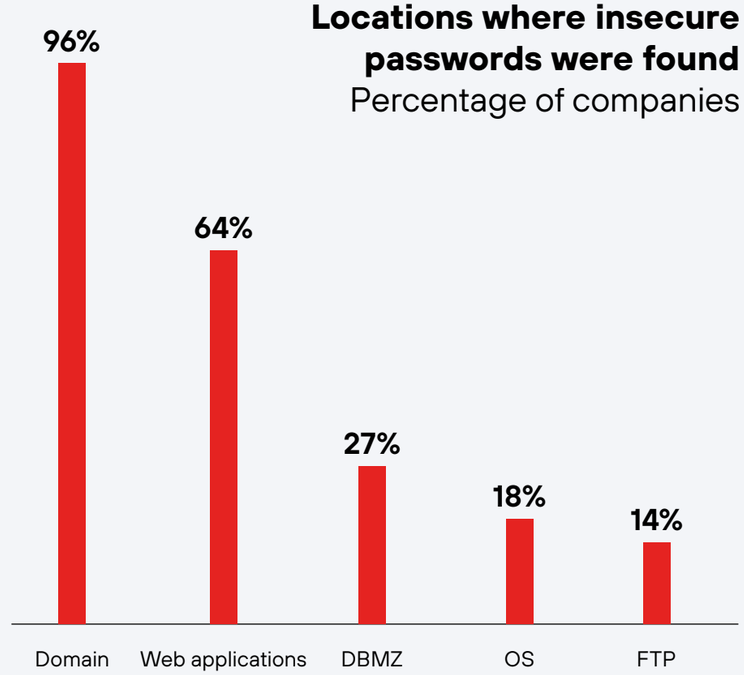
In **36%** of companies, administrator passwords consisted of combinations of adjacent keys

91%

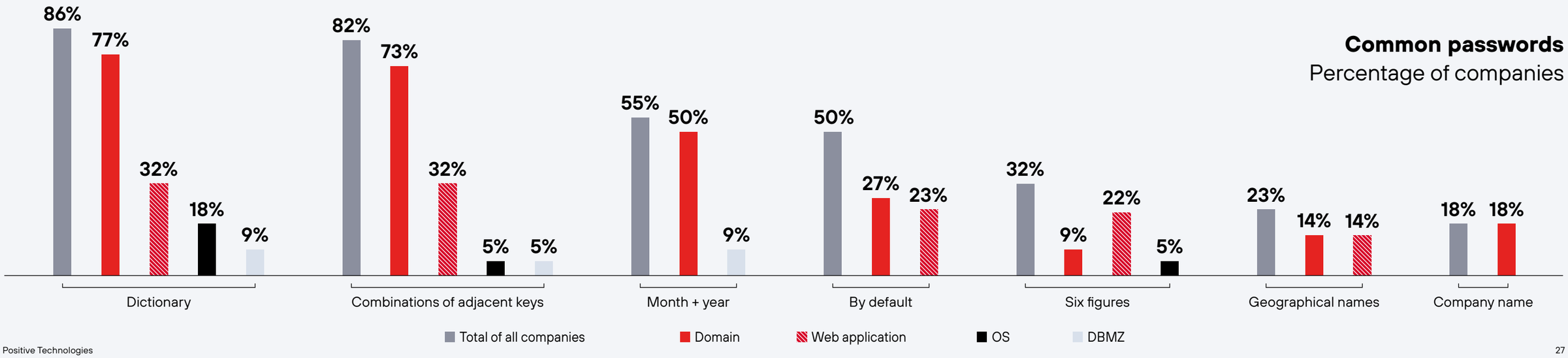
of companies are vulnerable to password policy vulnerabilities (critical and high-severity)

1qaz@WSX

Locations where insecure passwords were found
Percentage of companies



Common passwords
Percentage of companies



FLAWS

64% Weak and dictionary passwords

67% Short passwords

- Reuse of passwords
- Absence of two-factor authentication
- No password expiration

RECOMMENDATIONS

Set minimum password complexity requirements and avoid using dictionary passwords

Minimum password length should be 10 characters for ordinary users and 12 characters for privileged users

Use unique passwords for different accounts and resources. Prevent users from reusing at least three previous passwords.

Use two-factor authentication or the SSO (single sign-on) technology.

Download domain user password hashes and check for weak and dictionary passwords **********

Conclusion

Penetration tests usually demonstrate a low level of security of organizations, and these pentests were no different: A cyberattack can lead to negative consequences in every organization we tested. To combat this, companies can conduct regular security assessments and work on their mistakes to reach higher levels of performance and security. We recommend paying special attention to common security flaws and attack techniques mentioned in this report, and prioritize the security of target and key infrastructure systems. By regularly testing the efficiency of security measures at your company and checking whether your infosec specialists are ready to detect and counter attacks at early stages, you can head off unacceptable consequences before they occur.