Penetration testing: Protect critical assets using an attacker’s mindset

Identify critical vulnerabilities using the tools, techniques and practices criminals use

IBM Security

Table of contents

Executive summary

Defending businesses from cyber criminals is becoming even more important as the amount of valuable data and regulation designed to protect it increases. Out of 183 penetration tests IBM X-Force Red performed between August 2017 and November 2018, 1,099 vulnerabilities were identified, with 12 percent ranked high or critical.[1] If criminals were able to exploit just one vulnerability of that 12 percent, the impact on a business might be detrimental.

Chief information officers, chief information security officers and others in charge of securing their businesses often find identifying and fixing critical vulnerabilities a formidable challenge. Threats target networks, hardware, applications, devices and employees from inside and outside their organizations. From its penetration testing engagements, X-Force Red determined weak or default passwords and hardcoded credentials represented 50 percent of the reasons for system compromise. Between October 2017 and November 2018, the team sent 1,176 phishing emails to client organizations; 198 people clicked the link and 196 people submitted valid credentials.[2]

With limited budgets, resources and time to address such threats, some organizations opt to use automated tools to test their environments. However, those tools aren't designed to find unknown threats, which are oftentimes the ones that slip through the cracks and succeed.

Manual penetration testing is designed to help uncover the most critical known and unknown vulnerabilities across organizations' environments. Testing can occur on anything and everything from networks, applications, hardware and other systems to ATMs, cars, planes, IoT devices and more. More organizations are recognizing the value of manual testing. For example, the percentage of banks that requested X-Force Red to conduct ATM testing increased 300 percent from 2017 to 2018.[3] Penetration testing can help organizations build in security during product design and beyond, maintain compliance with regulatory standards and protect sensitive data.

Security challenges that align with the need for penetration testing

Security weaknesses proliferate in businesses for several reasons. Companies fail to follow best security practices and allow employees, contractors and vendors unlimited access to all their assets. This access occurs no matter the assets' level of importance nor the role of people accessing them. Complicating matters, more valuable data than ever before flows through networks, devices, applications and people, much of it in silos across business units. This complex infrastructure makes it challenging to understand threats to and vulnerabilities within their most important assets.

Additionally, the types of threats range from criminal groups to nation states and from lone wolves to malicious and non-malicious insiders. Many criminals are using more sophisticated tools, techniques and practices than ever before, stealthily bypassing security controls and conning personnel into releasing sensitive data.

Total tests	Total findings	Critical and high risk
183	1,099	136

Figure 1. Of 183 tests performed from August 2017 through November 2018, X-Force Red found 1,099 vulnerabilities. Of those vulnerabilities, 136 or 12 percent were high or critical.[4]

Regulatory requirements also add to the pressure and complexity surrounding data protection. For example, security requirements set by the Payment Card Industry Data Security Standard (PCI DSS) apply to any organization that handles payment card transactions. Regardless of size or number of transactions, every business that falls into this category must complete some level of compliance with the PCI DSS.

Another regulation, the General Data Protection Regulation (GDPR), requires organizations to protect the personal data and privacy of European data subjects. Failing to comply with the GDPR can cost an organization up to 20 million euro or 4 percent of global annual turnover, whichever is higher.

Daily business pressures also create vulnerabilities. Tight deadlines for turnaround and market delivery of goods and services can take priority over data security. Mergers and buyouts can cause a company to inherit more data flaws during reorganization.

Considering these factors, a business that wants to be proactive in data protection should consider incorporating penetration testing.

What penetration testing provides

A penetration test is an attack and exploitation simulation designed to uncover a specific target's security weaknesses. Hackers perform these tests with the tools, techniques and practices criminals might use to break into an environment and compromise valued assets.

Penetration tests can occur internally or externally. The process assesses the potential to access sensitive data and exploit system flaws. The tests rank the findings as critical, high, medium or low. Results ranked as critical or high are likely events that can compromise a system more than just theoretical threats.

Organizations that conduct penetration testing gain an understanding of which assets are vulnerable to an attack and what types of vulnerabilities exist. Penetration testers also show how a criminal would exploit vulnerabilities. The testers can then help organizations fix those weaknesses before criminals find them. The offensive engagement helps an organization stay ahead of criminals.

With penetration testing, users have the opportunity to bypass the limitations of vulnerability scanning. Scanning will find known flaws but may miss scenarios where criminals can link multiple vulnerabilities for an attack. Techniques that a criminal knows beyond a data center will likely escape detection from scanning, too. Scanning might be incompatible on some systems and hardware components. Manual testing can help detect vulnerabilities missed by scanning.

Performing penetration testing in-house has its own restrictions. The amount of testing needed to detect critical vulnerabilities can overwhelm a small staff. Security teams likely won't know about threats attacking other similar businesses, since their sole focus is on their specific organization. Turnover and skills shortages can also hamper an in-house team's effectiveness.

Outside penetrating testing teams can test essentially anything and everything. They combine manual testing and automated tools to increase effectiveness in finding known and unknown vulnerabilities. They can scale more easily since they have larger teams and more expertise. Outside penetration testing teams also get a broader view of the threat landscape since they perform testing for many organizations. Typically, these groups have their own research teams and threat intelligence feeds, as well.

Additionally, many in-house testing teams don't have expertise in automotive, IoT devices and ATMs and treat them the same as working with computers. These verticals require specific testing expertise, techniques and tools that outside penetration testing teams can provide.

IBM solution: IBM X-Force Red penetration testing services

X-Force Red penetration testing services from IBM Security offer clients the skills, scale and scope to help them find and fix the most dangerous vulnerabilities. The X-Force Red team includes hundreds of hackers with decades of experience breaking into organizations using the same tools, techniques, practices and mindset as criminals. Experienced specialists and developers understand how to build code and devices, and how attackers can compromise them. In an ad hoc or subscription service, the testing methods the X-Force Red team uses include virtual and onsite manual testing and automated scanning.

Clients using X-Force Red penetration testing services range from international brands to smaller operations across virtually all industries. Regardless of size, the X-Force Red team can test essentially any network, application, hardware, personnel or device an organization wants. The team can perform testing on products during development and after they're on the market. X-Force Red has performed penetration testing for hundreds of organizations and counting.

The X-Force Red team sells its services using a "gift-card-like" format. As part of its subscription services, clients pay a fixed rate every month and can change what they want tested at any time. The duration of testing varies depending on the size of the environment and areas tested, such as the number of lines of codes.

Consultations can help customers determine which kind of testing is best for their needs. At the end of the testing, the X-Force Red team presents a report of findings, methodology used and remediation recommendations. Clients learn about the most severe vulnerabilities that, if exploited, might impact the business the most and what they need to remediate those weaknesses quickly.

The X-Force Red team tests applications, networks, humans, hardware and more. The team can also test ATMs, cars and embedded and IoT devices.

Application testing

Applications are the heart of many businesses. If critical applications go down, the business stops, as well.

To protect their applications, some organizations rely on automated security controls. However, those controls can only address automated attacks. Only humans can detect and address manual, human-based attacks.

Other organizations use application firewalls; however, those miss logic flaws—what the application is doing and why—which criminals often bypass and exploit. Additionally, applications might have malware, which can infect organizations' systems when installed.

The X-Force Red team performed 24 application tests for organizations between August through November 2018. The findings include the following:

153
Number of vulnerabilities found

20
Number of vulnerabilities found that were high or critical

13%
Percentage of vulnerabilities found that were high or critical

71%
Percentage of high or critical vulnerabilities found by the X-Force Red team in its application tests

Total tests	Total findings	Critical and high risk
24	**153**	**20**

Figure 2. For application testing, 24 tests performed from August through November 2018 found 153 vulnerabilities. Of those vulnerabilities, 20 tests or 13 percent were high or critical.

To mitigate these flaws, the X-Force Red team manually tests applications to identify vulnerabilities in security processes and controls that developers may have overlooked. Testers validate known and “as of yet unknown” vulnerabilities and remove false positives.

The X-Force Red team can also perform an application source code review. Clients can provide their source code to enable more time- and cost-efficient testing.

More boards of directors are requiring application security testing since critical applications are what keeps the business running. At the same time, more industry compliance mandates are starting to require penetration testing, such as the PCI DSS. X-Force Red application testing helps clients address compliance mandates and build in security before and after applications are released to the market.

Network testing

Using technologies from third-party vendors might put company networks at risk. Vendors may not follow security policies and procedures. And companies may install these technologies without following best security practices.

Additionally, some companies may lack encryption on internal communications or other applications across the network. With these deficiencies, criminals can crack passwords and access companies’ servers, virtual machines, customer data, database backups and more.

The X-Force Red team can help identify these issues using manual network penetration testing. The assessment measures the security of devices from a network perspective, focusing on exposed services, configurations and infrastructure. The testing identifies opportunistic attacks criminals may run and vulnerabilities that scanners might not detect.

Using the same tools, techniques, practices and mindset as criminals, X-Force Red testers break into organizations’ network infrastructure to identify vulnerabilities. The team identifies flaws, such as if the network hosts have an active trust relationship with another host that’s susceptible to an attack. Testing typically occurs during business hours when employees use the network and can respond immediately when remediation is needed quickly. Projects typically take one to two weeks depending on the size of the network.

With network testing, clients learn how to make programmatic changes designed to help strengthen protection throughout their networks and across their entire infrastructure. Network testing also helps security leaders understand where to invest their resources to minimize risk the most.

Personnel testing

While more companies are conducting security awareness training, some still don’t educate their employees at all or frequently enough. Even the best security controls can’t prevent some attacks directed at employees.

As mentioned earlier, X-Force Red found that weak or default passwords and hardcoded credentials were the top reasons for a compromise. Another challenge is combatting phishing, where criminals send emails persuading employees to reveal personal information.

The X-Force Red team uses social engineering techniques to create similar ruses employed by criminals. Testers analyze which personnel interacted with malicious emails. They also perform vishing, or voice-phishing, exercises to see what sensitive information employees divulge over the phone to an unverified individual.

Other testing can include loading USB drives with fake content and tricking users to plug in the device. For physical security testing, the X-Force Red team assesses policies and procedures by trying to access secure areas and sensitive information on company property. Something as simple as a box of donuts can get X-Force Red hackers in the door.

When testing ends, the X-Force Red team provides a prioritized list of custom recommendations to help mitigate vulnerabilities identified.

Hardware testing

Criminals who want to compromise a device often have few obstacles. They can buy the same model, break inside, find its vulnerabilities and use that knowledge to exploit flaws exposing their target. Many hardware devices lack encryption for stored data and have functionality information left on the device during production. Criminals can find one device model, retrieve default credentials and compromise a target's device using the same credentials.

X-Force Red testers review how products are built from start to finish. The testing aims at anything electronic and the enclosure or housing that makes up part of the device. X-Force Red testers also help select and implement parts and controls so that security is built into the product instead of being an afterthought.

The X-Force Red team offers two types of hardware testing. For "white box" testing, clients provide design documentation, source code and design schematics. The X-Force Red team reviews the source code and data flowing in and out of the system and identifies vulnerabilities in product implementation and external libraries. For "black box" testing, the X-Force Red team reverse engineers products to recreate design documentation. This process tests for vulnerabilities within a product's lifecycle, including source code and implementation.

ATMs, the IoT and automotive-specific testing

The X-Force Red team has decades of experience testing ATMs, cars, the IoT, point-of-sale and other devices. Testers focus on researching, testing and providing guidance for securing these systems during design and beyond. The X-Force Red team has a global view into these systems' flaws and exploits and can provide hands-on assistance where needed.

Consider ATMs. Their omnipresence in disparate locations with thousands of dollars in physical cash entices criminals.

From January through October 2018, the X-Force Red team found the top security issues for ATMs were a lack of full-disk encryption and poor locks on cabinets. One tester broke an ATM cabinet lock in 20 seconds.

Banks recognize the severity of these threats as shown by the following figure:

300%

Percentage of increase from banks requesting the X-Force Red team to conduct ATM testing 2017 – 2018. In the Asia Pacific alone, there was a fivefold increase in ATM testing requests.

The increase is partially because of a warning from the FBI about the proliferation of ATM "cash-out" attacks. The following figure illustrates this threat:

FBI warning: Cash-out attacks

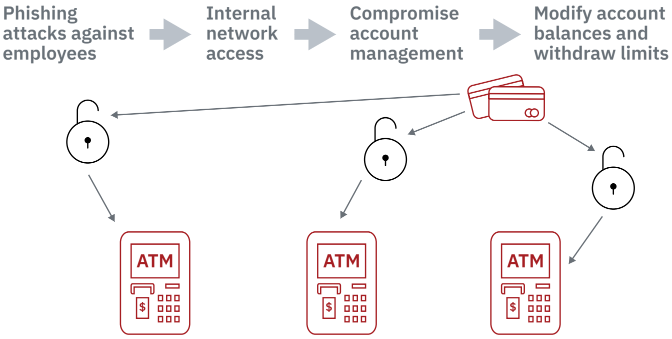
Phishing attacks against employees
Internal network access
Compromise account management
Modify account balances and withdraw limits
ATM
ATM
ATM

Figure 3. In "cash-out" attacks, criminals manipulate withdrawal limits and create fraudulent ATM cards to take out cash, potentially draining a customer's entire account.

The X-Force Red team offers clients onsite ATM testing, virtual testing and one other option. Clients can ship ATMs — and the IoT, automotive-specific devices and similar electronics — to X-Force Red Labs for testing.

X-Force Red has four labs located in Austin, Texas and Atlanta, Georgia in the United States, Hursley in the United Kingdom and in Melbourne, Australia. Inside the labs, testers pull apart specific hardware devices to identify weaknesses. They assess the hardware's composition, interaction with software and related matters. X-Force Red testers also establish product objectives, create security requirements and model threats to uncover vulnerabilities. They can help companies fix security flaws before products are on the market to avoid potential financial losses and brand damage.

The X-Force Red portal

For all clients, the X-Force Red portal provides convenient, direct and protected communication and collaboration with testers. Using the portal, which is a cloud-based platform, clients can request tests in one encrypted form. Clients can contact testers directly from the portal with any questions or comments at any time, avoiding the exchange of emails and phone calls.

The X-Force Red portal enables faster remediation in real time. Traditionally, testers write their reports one to two weeks after concluding the project. This lag time means clients must wait for the findings, giving criminals more time to attack, all while new vulnerabilities may appear. Using the X-Force Red portal, testers submit findings when identified, offering the client the opportunity to view and remediate vulnerabilities quickly. By providing one view of testing progress and findings, the portal helps clients and testers keep each other apprised of the situation.

The interactive reports entered into the portal contain key findings about vulnerabilities, evidence of exploitation and detailed guidance for prioritization and remediation. When entering reports into the portal, X-Force Red allows security leaders to determine who has permission to see the results. Clients can isolate sections of the report into segments so that individuals see only vulnerabilities within their scope. Throughout the process, security leaders remain in control of determining fixes for their organizations.

The X-Force Red portal acts as a central repository for all reports for clients. Organizations performing multiple tests can monitor, track and review all reports in real time. Clients receive a historical record to compare the flaws found and improvements made over time.

The portal also has its own security controls, which include Secure Sockets Layer (SSL), encryption, two-factor authentication and more.

Conclusion

The proliferation of potential lawsuits, financial losses and brand damage stemming from security breaches means organizations need to be proactive in protecting their most valued assets. With IBM X-Force Red penetration testing services, clients can identify and fix critical vulnerabilities before criminals exploit them. X-Force Red testers have decades of experience identifying and exploiting flaws using the same tools, techniques and practices as criminals. Because of their attacker mindset, X-Force Red testers also find new ways to compromise organizations that criminals may not have tried. As a result, organizations that use X-Force Red penetration testing services to find and fix critical flaws across their infrastructures can develop controls to help them strengthen their security measures to stay ahead of criminals.

For more information

To learn more about penetration testing, please contact your IBM representative or IBM Business Partner, or visit **ibm.com/security.**

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2019

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

1. X-Force Red penetration testing findings, August 2017 – November 2018.
2. X-Force Red penetration testing findings, October 2017 – November 2018.
3. X-Force Red ATM testing presentation, November 2018.
4. X-Force Red penetration testing findings, August 2017 – November 2018.