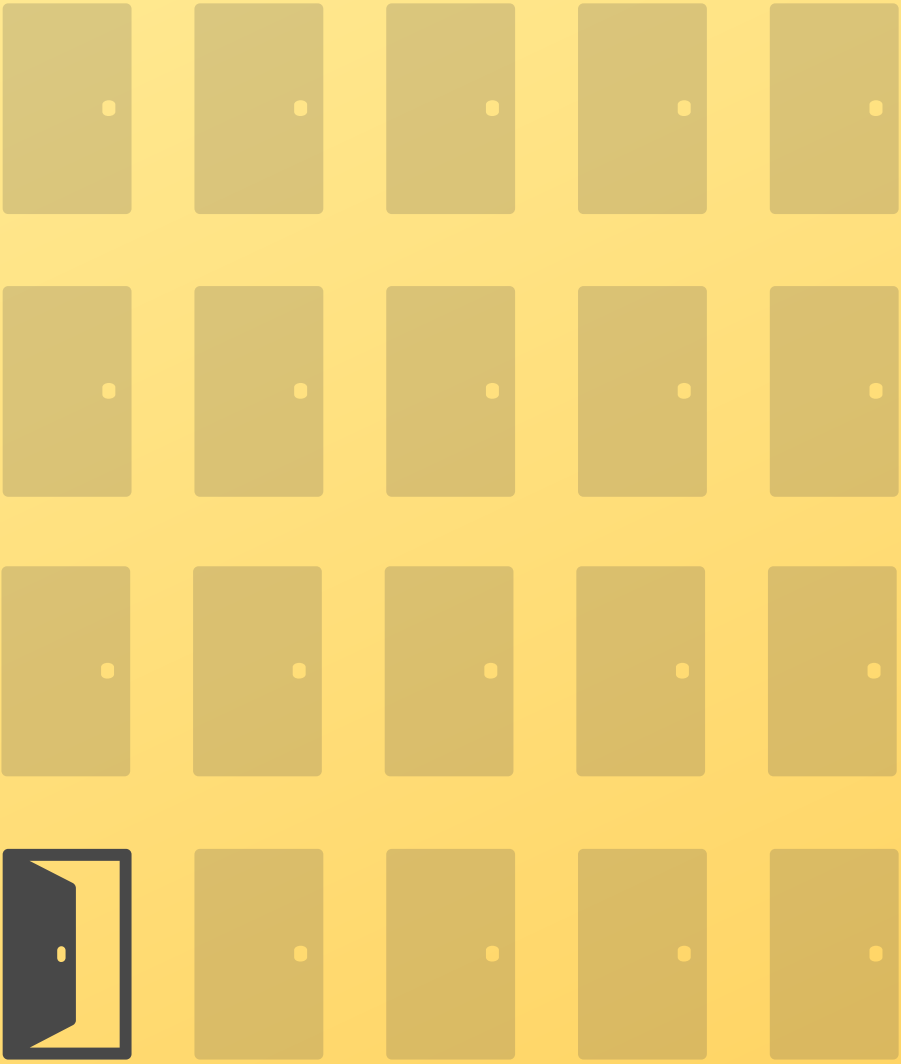

Pentest Best Practices Checklist

sqreen

INTRODUCTION

Damn, but security is hard.

It's not always obvious what needs doing, and the payoffs of good security are at best obscure. Who is surprised when it falls off our priority lists?

Running a first (or even your 100th) Pentest can be a daunting experience, but it shouldn't feel like a chore. We'd like to offer a little help if you don't mind. And by « help » we don't mean « pitch you our product »—we genuinely mean it.

Sqreen's mission is to empower engineers to build secure web applications. We've put our security knowledge to work in compiling an actionable list of best practices to help you get a grip on your penetration tests. It's all on the following pages.

We hope your find if useful. If you do, share it with your network. And if you don't, please take to Twitter to complain loudly—it's the best way to get our attention.

The Sqreen Team
@SqreenIO
howdy@sqreen.io

SCOPE

✔ Why are you even doing a pentest?

The first question that one needs to answer is about the goals of the penetration test. Penetration tests can take several forms and can solve a lot of different problems (improving security, ensuring compliance, making some customers happy etc.). Make sure you are clear on the objectives. A pentest might not even be the right solution to your problem. Outcomes alignment with objectives is key to having a successful pentest.

Pentesting basics and requirements - http://bit.ly/2zUIXHD

What is a pentest? And why would I need one for my company? - http://bit.ly/2B8Cnze

Hidden costs of pen testing - http://bit.ly/2QJfmlj

✔ Know your pentests

Internal pentest vs. External pentest. Security audit vs. vulnerability assessment vs. penetration test vs. private bug bounty etc. The wordings can quickly become very confusing. Make sure you are aware of the different terminologies and use them properly to make sure you get what you want.

Learn more about the different terminologies:

What is pentesting? - http://bit.ly/2QQmJOt

What is vulnerability assessment? - http://bit.ly/2FyqPcS

What it is a security audit? - http://bit.ly/2qNGZEM

What is the difference between pentesting and vulnerability assessment? - http://bit.ly/2RWXIRM

✔ Enumerate likely threats

If your pentest goal is about uncovering vulnerabilities then you need to perform a risk assessment of your business. You don't need to be a security expert to reflect on this. Just think about the places that can hurt you the most. Are you collecting sensitive data? Are you running legacy applications? etc.

Assess the risks before a pentest - http://bit.ly/2DG7tAt

Performing a security risk assessment - http://bit.ly/2Thk2qv

---

✔ Define the pentesting scope

As your resources are most probably limited, whether it is time, budget or expertise, define the scope of the pentests you would like to perform. Based on the previously threats list or risks map, determine in which areas vulnerabilities if exploited will most likely hit your business directly or indirectly (e.g: loss of revenue if web application is down, damage to your reputation following user data theft...)

✔ Determine a budget

There's the $50 "script-kiddie" on Fiverr and there's the hundred thousand dollars pentest. Your budget is an important discriminating factor and it has to be aligned with your objectives and the value of your assets. Eventually, you end up getting what you paid for (in most cases...). If you are looking to find critical vulnerabilities in a very complex architecture or if you are interested in reassuring your customers with a big brand by putting a seal of approval on your security practices; you will need to pay the price.

✔ Prepare the pentest environment

Pentests can and should be conducted on production environment, however certain limits should be set for the testing team. The most obvious one being never to run DoS attacks or fuzzing on production. If testing cannot be performed on the production environment, set up an environment that is absolutely identical to production and create user accounts for the pentesters, depending on the decided testing style. If the tests need to be done on production directly, schedule them in such a way as to avoid slowing the network response time for the company and your customers.

PentestBox (Windows) - http://bit.ly/2Tj92J8

Kali Linux - http://bit.ly/2DDKYMR

✔ Launch scanners before

Pentests will reveal the ugly truth about your systems or your applications. However, if you already know some of your vulnerabilities and basic issues, take the time to run scanners and fix the issues instead of wasting valuable pentesting time and energy uncovering what you already know or could know with other automated tools.

✔ Review the organization's security policy

As regulations are more and more stringent, make sure to be compliant with the security policies and regulations especially when it comes to sensitive data handling.

Rules of engagement - http://bit.ly/2PxyIUa

✔ Notify your hosting provider

Inform yourself about which tests are allowed by your hosting or cloud provider, and request the appropriate authorizations before the tests.

AWS penetration testing - https://amzn.to/2QKbdUx

✔ Freeze developments in the pentest environment

The value of pentests is to test the system as a whole and not individual bricks of it. Pentests will uncover vulnerabilities within a context. If you change that context by deploying patches or new packages or changing hardware components, the results of the pentests could not be valid anymore. Unless you need to fix a critical customer bug, refrain from any release during the pentest duration. The security auditors are working with time limits, as opposed to most attackers, and are cutting corners to get their results. If you fix the issues they are exploiting, you make them waste their time, and thus your money.

EXPERTISE

✔ Find the right pentesters for the job

Finding good pentesters should be done via recommendation. Ask your friends, colleagues, investors, or even Hacker for recommendations. Make sure the suggestions fit with your objectives. Hiring pentesters without a strong recommendation and reputation is probably a no-go. Also, make sure that you have the right experts for your target domains: if you are looking to pentest your network you need a pentester that specializes in this field. An expert will know how the systems are built and their common weaknesses.

How to Choose a Pen Testing Service - http://bit.ly/2B89MtM

✔ The more trustworthy the company, the more trustful your clients are gonna be

Pentests are tools to uncover vulnerabilities but they are also reassuring your clients. So if you are going the extra length as to hire a pentester, you might as well get a good one. Remember that you will mostly get what you paid for. If you hire cheap, you will most probably get sloppy work. Check the pentesters credentials and talk to previous clients if possible.

Information Assurance Certification Review Board - http://bit.ly/2TbyujQ

✔ Define pentest methodology

Based on your target environment and objectives, define the testing style and the access that will be provided to the testers: no access to simulate external attacks or full access to simulate insider job. If you are relying on external testers, ask them what their methodology is and ensure your objectives are met. If you are doing the pentesting internally, make sure it is aligned with security frameworks and consists mainly of manual advanced testing and not only automated.

Penetration testing execution standard - http://bit.ly/2DGwkUL

OWASP testing guide - http://bit.ly/2FofhIN

Penetration testing guidance from Payment Card Industry Data Security Standard - http://bit.ly/2Q4Qhue

Best practices for pen testing mobile apps - http://bit.ly/2zb3EQ9

✔ Define pentest report format

Get a sample report to familiarize yourself with its content and ensure the metrics and content covers your objectives and areas of interest. If you have a risk management system and you want to integrate the findings in it, you might also want to ask the pentesting company for a CSV or XML format in addition to the PDF report they will deliver.

Penetration testing execution standard - Reporting - http://bit.ly/2DHa1hV

✔ Do not forget to cleanup the pentesting environment

The auditors should clean up the tested environment. This typically includes removing rootkits, backdoors, executables and scripts as well as any temporary files created. The user accounts created for the pentesters should be removed as well. If data were modified or deleted or if settings were changed, everything should be reconfigured back to its original state.

✔ Schedule for a next pentest

As your systems evolve quickly, the penetration test findings will soon be outdated and other vulnerabilities created. Some companies schedule to perform penetration tests regularly, such as once a year. You will need to figure out if pentests are the right tools for your needs and how often will you need to run them (depending on your applications release frequency, hardware and network upgrades, etc.)

How often should you pentest? - https://ibm.co/2OIANHD

7 Steps to Building a Yearly Pen Test Plan - http://bit.ly/2QLDVEC

MONITORING

✔ Implement a security monitoring solution

Security monitoring solutions are part of your security arsenal, you should implement them before embarking on the pentests. The pentesters will, by the way, be interested in knowing how far they could go until being detected by the Intrusion Detection Service (IDS) for example. You can use tools like Sqreen to prevent data breaches, protect your customers, stop business logic attacks and get full visibility on your security..

What is an intrusion detection system? - http://bit.ly/2qLtAx2

Intrusion detection critical but not as a standalone solution - http://bit.ly/2FpEI2l

✔ Implement a logging solution

Logs are the most precious assets to monitor the environment and to investigate a suspicious activity or a security breach. If you don't already have a logging solution set up, a centralised log platform enables to make the most out of the analytics capabilities and provides a view across all themes (applications, network, users, etc.). It will be useful in registering pentests activities and impacts on your systems and applications.

Logging Cheat Sheet - http://bit.ly/2NUIvPu

What is log management and how to choose the right tools? - http://bit.ly/2Q8SGkO

Centralized Logging on AWS - https://amzn.to/2M4iOub

Top 7 Success Factors for Setting Up Centralized Logging - http://bit.ly/2NSv4zn

✔ Closely monitor your exception tools

Ask your team to pay extra attention to exception management and error handling systems as they will provide valuable information on the pentest impacts. Your team should be kept up to date on the current pentests to be able to discern if the errors come from usual user activity or as a result of the pentest.

✔ Monitor your security monitoring tool

Your security monitoring tools should pick up the activity from the pentests. However, you might have real attacks occurring at the same time. Make sure your team is up to date on the performed pentests to be able to distinguish the attacks.

Sqreen - http://bit.ly/2MDSMTm

REMEDIATION

✔ Ensure you have an uncorrupted backup of your data and system configurations

There is a risk that the pentest knocks down your systems, and deletes or modifies your data as any real attack would, so you should make sure that you have backups ready should this happen. No professional pentester can guarantee that there will be zero risk of system failure or data deletion and modification, especially if the testing takes place in production environment.

✔ Start reserving time for after the pentest

Make sure you and key people from your team will be available after the pentests to study the report and fix the vulnerabilities uncovered by the pentests.

✔ Do not patch vulnerabilities during the tests

Ask the pentesters to inform you on the most critical vulnerabilities during the test, but don't patch them right away as you would be modifying the pentest environment, rather use the time to define a fix and schedule it to be rolled out as soon as the pentests are done and the results are understood.

✔ Make sense of the pentest report

Once you receive the pentest report, share the technical version promptly with your team. If you have trouble understanding it, call the security auditors and do not hesitate to request a clarification meeting should you still have trouble (that's OK, these guys are security auditors, not professional writers!).
Ensure the report is understood by your team. If it isn't by everyone, organize a test session to reproduce the issue with the team (at Sqreen, we call it hack nights and it comes with beers & pizzas).

✔ Prioritize the report findings

The auditors will sort the vulnerabilities given their technical criticity. Review this prioritization to ensure it is also compatible with the business direct or indirect impacts. You can use Sqreen to easily differentiate between real vulnerabilities and false positives.

✔ Make sure you got alerted about the critical attacks during the pentest.

Scan the report to make sure you were informed about all the critical attacks performed during the tests and what their impacts were. These attacks might have uncovered critical vulnerabilities, but could also have impacted your system and modified or deleted your data.

✔ Allocate resources to fix vulnerabilities

You probably would like to assign a dedicated taskforce to tackle the vulnerabilities uncovered. Make sure to allocate sufficient time and appropriate expertise for this task. Use Sqreen to get a Stacktrace on the identified vulnerabilities and fasten the remediation cycle.

✔ Re-Test after the fix

Some pentesting contracts can offer a re-testing phase at no additional cost after the vulnerabilities have been fixed to validate that the remediation effort has been successful. It is useful to re-test in order to close the findings and ensure the remediation actions did not open other vulnerabilities.

COMMUNICATION

✔ Communicate with your team

Tell your team a security test is going to be performed. You may gasify this and play to see how long they take to find out the pentest has started. You should also communicate the test ending date. Also, set up a communication channel between the pentesters and your team (yourself included) to ensure communication during the pentests goes smoothly and information do not get lost in translation.

✔ Make sure you are available

Pentesters will have questions during the tests, and will need to discuss with you the leads they are pursuing. Appoint a single point of contact within your team and make yourself available for the critical questions. You should schedule regular quick meetings to understand their progress (if they are lost or steadily advancing). They have limited time and to make the most out of this pentest, you should help them.

✔ Check your team members' attitude

Pentests are not light exercises, they should be taken seriously, make sure your team is aware of their importance. However, make also sure that your team is not unnecessarily stressed out by them or taking the tests as a bad reflection on their job, but is rather open to improvement recommendations.

✔ Communicate with your manager

Cybersecurity is increasingly taking center stage within the companies, since they became aware of the serious impacts on the business. Consequently, security tests are often a big deal all the way up to the CEO and the board who are attentive to the projects and waiting for the results. Without being technical, be transparent and report regularly on the progress so that they are not surprised by the final report. Identify beforehand some key indicators you could consistently report on so that the board members can follow the trends between the presentations.

How CISO should address their boards about security - http://bit.ly/2K6oJiX

Getting CISO and CEO to talk same language - http://bit.ly/2PYLY3z

How to talk 'security' to the board (YouTube) - http://bit.ly/2Q2j0jr

LESSONS LEARNED

✔ Review the vulnerabilities with the team

Some vulnerabilities uncovered by the pentesters within the scope of the pentest could exist in your other systems. Reflect with your team to find out if similar vulnerabilities can exist elsewhere and if you could fix them simultaneously.

✔ Review the vulnerabilities to ensure they have not been exploited

Use the logs to investigate if the uncovered vulnerabilities have been exploited. If that is the case, you should find out the extent of the damage done, report on it to your manager and take appropriate remediation actions.

✔ Adapt your processes to make sure vulnerabilities do not occur again

The pentests should have long-lasting effects in your company. They uncover vulnerabilities in the systems but they should make you question why those vulnerabilities occurred, since they are only symptoms and not root causes. Take the time to reflect on how you could improve your processes to avoid similar vulnerabilities in the future.

✔ Create training and update onboarding and offboarding

Take the time to understand the lessons learned from the pentests, and include them in the employees training curriculum, whether they are technical or non-technical employees. Make sure to update employees onboarding and offboarding packages and processes as well.

Security training by PagerDuty - http://bit.ly/2PM7AgM

✔ Evaluate penetration testing effectiveness

Have the pentests achieved the goals you set? What could have been done differently/better? The frustrating part about penetration tests is that when they find vulnerabilities, it is bad news, but the absence of discoveries does not mean absence of vulnerability. Do not judge the pentest by how little or how many vulnerabilities were uncovered.

Penetration testing is a reference point not a strategy - http://bit.ly/2qLB8jm

What makes a good application pentest? - http://bit.ly/2B8NYy0

✔ Make sure your Incident Response Plan covers the uncovered vulnerabilities

Review your Incident Response Plan in light of the findings to ensure it is well prepared for the vulnerabilities. Update the plan if needed, with detailed procedures and roles and responsibilities. Make sure to communicate it to your team and other stakeholders within the organization and schedule simulations training.

How to improve your incident response plan - http://bit.ly/2B8owJ8

How an Effective Incident Response Plan Can Help You Predict Your Security Future - https://ibm.co/2zfm8Pg

Working incident response - http://bit.ly/2K5HUZZ

sqreen

Protect your customers' sensitive data.

Sqreen provides visibility and protection over most threats targeting applications with no overhead on engineering teams.

Get visibility over attackers trying to exploit your apps, APIs and microservices.

Reinforce your security with protection against the most common threats.

No overhead on engineering teams and no dedicated security expertise required.

Start your free trial at sqreen.io


sqreen