ACROS Penetration Test -
A Friendly "Advanced Persistent Threat" Simulation

Frequently Asked Questions

1. What is ACROS Penetration Test?

ACROS Penetration Test is a realistic "friendly" simulation of an "**Advanced Persistent Threat**" attack on an IT system – corporate IT infrastructure, electronic bank, power plant network, stock trading system etc. Our highly skilled team of security experts assumes the role of a motivated group of professional hackers and attempts to accomplish a variety of agreed-upon "mission objectives" (also called "goals" or "flags"), such as getting access to target network, executing unauthorized transactions, obtaining secret corporate information, demonstratively damaging production capabilities or disabling networks. Although we're using numerous commercial and in-house tools, our success is mainly a product of our resourcefulness, ability to quickly understand how unknown systems work, to hide our actions from all sorts of intrusion/anomaly detection systems by "flying below the radar", ability to quickly find and exploit previously unknown vulnerabilities in systems and applications, to penetrate security mechanisms such as firewalls or content filters, to propagate covertly through the target network, to gather intelligence data and elevate privileges – and mostly, to use these skills efficiently while steering the attack towards the specified mission objectives.

An ACROS Penetration Test is conducted exactly like a real attack by a skilled, motivated adversary – only without the damage. We find the weakest links in the target system's security and use all our knowledge, skills and capabilities to try to achieve exactly what deployed security measures and policies are there to prevent.

2. What isn't ACROS Penetration Test?

ACROS Penetration Test is not merely a superficial scanning of a system's perimeter with automated tools – although many vendors also give such automated services the name "penetration testing." Vulnerability scanning is a "hygienic" service and is very useful for managing the known vulnerabilities on more exposed systems, where even low-level attackers are likely to find them if you don't find them first. Limited automated vulnerability scanning often (but not necessary) represents a small part of attacker's activity in ACROS Penetration Test, for instance in the early stages of the mission, and can mostly be considered intelligence gathering.

3. What is the purpose of ACROS Penetration Test?

The purpose of our penetration test is manifold:

- A successful penetration mission gives the customer a highly valuable experience: A realistic APT-like attack with zero damage and an opportunity to gain deep insight into the attacker's activity, his thinking and methods used in the attack.
- A penetration test is a perfect opportunity to test corporate security mechanisms – both in the area of protection and intrusion detection.
- People are "tested" as well: Are they following the security policies, does their behavior endanger the security of the system they're an integral part of?
- A penetration test can show that the current policies are not suitable for efficient protection of the system.
- Numerous vulnerabilities are usually discovered in the target system during a penetration test. Some can be used for accomplishing mission objectives, others can't. We document all these vulnerabilities in detail and report them to the customer, along with efficient recommendations for eliminating them.

- In our experience, a successful penetration test is the most efficient tool for raising the security awareness among users, administrators, support staff, and up to the highest managerial levels. Few things can be as impactful as showing that catastrophic objectives actually were (not just *could have been*) accomplished with a modest budget in relatively short timeframe.
- A penetration test helps evaluate – or re-evaluate – security risks the attacked system is facing, and provides convincing, objective arguments for future investments in information security.
- A successful penetration test provides strong arguments for budgeting additional investments in security.
- Finally, ACROS Penetration Test provides an answer to the most important question in information security: *Is your mission-critical security strong enough to stop a skilled attacker?*

4. What isn't the purpose of ACROS Penetration Test?

Most importantly, a penetration test is not a systematic and comprehensive security audit of the target system. The vulnerabilities it uncovers are merely a side-product of the test, although they often turn out to be highly severe. It would be wrong to assume that a penetration test has uncovered all highly discoverable vulnerabilities in the system: in order to systematically identify a system's vulnerabilities, a comprehensive security audit (another service, also provided by our company) needs to be performed, where the mission objective is entirely different: namely, to find as many and as severe vulnerabilities as possible.

5. Why is another vendor offering a penetration test at a much lower price?

Many vendors are offering automated scanning of Internet-facing servers or scanning of internal networks under the name of "penetration testing," making it difficult for customers to distinguish between the services offered. ACROS Penetration Test is a realistic intrusion simulation by an intelligent, creative and highly skilled attacker, targeting your crown jewels and not giving up until he acquires them or runs out of time. Many other "penetration tests" are little more than automated surface scratching exercises, sometimes with manual analysis of the results, and do not resemble an actual attack in any meaningful way. These two types of services, while both useful, are therefore dramatically different in purpose as well as in effect.

An efficient method for determining what type of penetration testing a vendor is offering is to see if the test includes setting potentially catastrophic mission objectives which the vendor would actually (not just theoretically) try to achieve. Vulnerability scanning services do not include setting such mission objectives, as they're focused on finding a few types of already known vulnerabilities. ACROS Penetration Test, in contrast, is aimed at actually achieving the very goals – mission objectives – that the customer sets in advance. Just like the real attacker does.

6. What are some typical mission objectives in ACROS Penetration Test?

In our penetration test, it makes sense to define the most potentially catastrophic objectives you can imagine. Some typical mission objectives set by our customers are: accessing sensitive information in the main database, obtaining confidential documents from high-level executives' computers, acquiring control over SCADA devices or machines, gaining administrative access to a Windows NT domain or a SAN system, disabling network connectivity, obtaining unauthorized access to personal data, unauthorized withdrawal of funds from a bank account, accessing the list of corporate customers or vendors, gaining remote access to a critical internal network, disabling the main database, obtaining sensitive e-mail, accessing accounting data, destruction of backup data, disablement or defacement of the corporate web site, accessing confidential product documentation or source code, and identity theft.

7. What types of attackers do you simulate?

On the highest level, the choice of attacker you want us to simulate is between an external and internal attacker. An external attacker is typically someone who has no non-public access to your system, and no non-public information about it. An internal attacker is typically someone with access and privileges of a (usually low-privileged) employee in your company. Some customers decide to have us simulate and external attacker first, and an internal attacker later in the penetration test.

We can play the role of both types of attackers or any other attacker your unique situation may require us to play.

8. Do you actually disable networks or services when a mission objective so specifies?

Certainly not. The mission objectives that could possibly interfere with your business processes or incur any kind of business damage will only be accomplished "demonstratively", meaning that we'll stop before the last step and describe to you what could have been done at that point by a real attacker. For example, instead of actually disabling your network, we can obtain remote administrative access to the network's main routers, which would allow us to effectively shut down the network. For less critical services, you can authorize us to actually perform a coordinated short-term disablement at a mutually agreed-upon time.

9. How many mission objectives does a typical penetration test include?

A typical penetration test of a large corporate IT system includes 7-10 mission objectives, but it can contain many more if a system is complex, heterogeneous or distributed, or fewer if the test should be focused on just a couple of specific goals.

10. How many mission objectives do you usually accomplish?

On average we accomplish nine out of ten mission objectives in a penetration test.

11. How do you set the price for an ACROS Penetration Test?

The fixed price we set for the penetration test mainly reflects our assessment of the total effort required and potential travel-related costs. These depend on the mission objectives set, our assessment of the target's strength (resilience to attacks), the limitations set by legislations and the customer, the amount of reporting and coordination required, and on whether the customer wants an on-site presentation at the end.

Each penetration test requires a variety of "intelligence-gathering" activities: collecting information about the target network, services, employees, equipment, vendors, internal policies, etc. These initial activities are roughly the same regardless of the number of mission objectives.

In contrast, the number, as well as the apparent difficulty of mission objectives has a non-linear effect on the amount of effort we need to invest in order to accomplish them. For instance, some mission objectives act as a springboard to others: obtaining target network access (objective A) allows us to come one step closer to the main database system (objective B). Nevertheless, each mission objective does require its amount of effort, and some are more difficult to achieve than others.

The vulnerabilities we discover in the target system during a penetration test are also largely independent of the number and type of mission objectives. We analyze and document all of them in detail, whether or not we find them helpful for accomplishing the set objectives.

Finally, writing up the project report and preparing the presentation requires a relatively fixed amount of effort.

It makes sense to populate the list of mission objectives with many potentially catastrophic scenarios, as opposed to cutting it down to two or three items. Once we, "the attacker", invest our effort in the intrusion, it is easier (and less costly) to target some additional objectives within the scope of this attack than, for example, in a separate attack months later (whether performed by us or another team). Each additional accomplished mission objective means a higher impact of the penetration test.

12. What methods are you using during the penetration test?

First of all, we're limited by the legislation of our home country, Slovenia, and the European Union, and by the laws of the country/ies the target system resides in. Our next limitation is our code of ethics, which guides us throughout our penetration testing activities. Additionally, the customer can set their own limitations as to the methods we're allowed to use.

Other than that, we're using both our in-house and commercial tools, reverse engineering, protocol analysis, special communication tools for piercing through the firewalls, source code analysis, password cracking, "war dialing" (scanning phone lines), placing custom "Trojan horses" on target computers, keyboard and mouse sniffing, network traffic monitoring, exploiting application-level vulnerabilities (like SQL injections or buffer overflows), physically accessing the target network, and much, much more.

13. Do you practice "social engineering"?

Social engineering is an extremely powerful attack technique, which we regularly employ. Oftentimes, this is the very technique that provides us with access to the target network or a protected service. However, customers sometimes wish us to focus on technical (i.e., non-human) ways to achieve our objectives, or to limit the social engineering efforts to a minimum level. While we warn the customer that any such limitations provide a further deviation from the reality of an actual attack, we naturally refrain from using any techniques our customers don't want us to use.

14. Will you put malicious software in our system?

The software we occasionally put in customers' systems (keyboard sniffers, network monitors, covert communication software etc.) is entirely developed by our company and is also merely a simulation of actual malicious software. We make sure that our software doesn't do any damage to your data or services, and completely remove it at the completion of the project if not sooner. Our penetration testing tools are not self-propagating, allowing us to maintain an accurate list of their deployment at all times, and to remove them when they're no longer needed.

15. How do you obtain access to the target system?

We prefer accessing the target system via Internet. When this is not possible, we try to gain access via modems in the target network, both known/authorized ones and those set up by administrators for convenient access from home, or via wireless network. In some cases, physical access – for example, a visit by a "network administrator" to a smaller branch office – might be the easiest way of obtaining access to the target network.

16. How do you assure the highest level of realism in a penetration test?

The high level of realism – i.e., the similarity between the penetration test and a real attack – is crucial for the business impact of the project. This is accomplished by:

- Making sure that as few people as possible are aware of the test being performed.
- Allocating enough time for the test (we recommend 60 days or more); this way, even those knowing about the test won't be able to act significantly more cautiously for its entire duration. Besides, some attack methods like social engineering and so-called "mine planting" require quite some latent time in order to succeed.
- Using as many different methods as possible; we're using all methods a real attacker would, except for those excluded by legal and ethical limitations, or prohibited by the customer.
- Having a vast knowledge of attack methods and techniques, including the latest information on vulnerabilities in software and hardware used in the target system.
- Being able to find new, unknown vulnerabilities both in general and custom-made software and hardware during the penetration test.

17. Are you in contact with the customer throughout the penetration test?

Of course, if the customer wants us to. Some customers prefer minimum interaction, while others want regular reports of our activities and progress. In the latter case, we notify the customer about the accomplished objectives, discovered vulnerabilities and our progress as we go, while in the former case we only provide this information in the final report and presentation. Naturally, we also need to be in contact with the customer for coordinating any potentially dangerous activities such as disabling a service or network – that is, if the customer desires to go beyond demonstrative proofs for such mission objectives.

18. Is it better for us that you accomplish the objectives, or that you don't?

It should be in your interest that we perform the penetration test as realistically as possible, and that you respond to the results, as this will allow you to increase the strength of your security where the weak links have been identified.

The more mission objectives are accomplished, the higher is the business impact (i.e., the value) of a penetration test. The accomplished objectives clearly show that an attacker we are simulating could have achieved catastrophic results with limited budget and low initial access, while the unaccomplished ones could either confirm accurate protection of sensitive targets, or reflect inadequate attacker's skills (or simply be a result of misfortunate circumstances for the attacker). Our high rate of accomplished objectives is a guarantee that an ACROS Penetration Test will be an excellent investment in your security.

19. How are the results of the penetration test presented?

A detailed final report, handed over to the customer at the completion of the project, contains a daily log of our activities, accomplished objectives and discovered vulnerabilities – including the recommendations for their elimination. The flow of the penetration test is presented in a presentation to the project's contacts, customer's administrators, other people "involved" (often unwittingly) with the test, high-level executives, managers and auditors. The ultimate impact on the security awareness can be achieved by revealing at the presentation how users have "helped" us with their actions, for example, by leaving a backup script containing an administrative database password in a shared folder, or by helping us install a remote control tool or a keyboard sniffer on their workstation.

If possible and desired, we present exploitations of selected vulnerabilities in live demonstrations during the presentation.

20. Do you clean up the system after the attack?

All our modifications to the target system – installing attack tools, creating new users, setting up "traps" and down to creating files on workstations or servers – are carefully documented, allowing us to restore the original system state at the end of the test.

21. How do you protect your customers' sensitive information?

We begin with setting up an encrypted communication channel with the customer, preferably PGP or S/MIME based e-mail, which we use throughout the project for exchanging any information with the customer. All customer data inside our company is stored on encrypted disks locked with strong passphrases. We don't extract sensitive information from the target system unless absolutely necessary for our work: for example, if one of our objectives is to obtain confidential documents from your CEO's notebook, we'll show you the listing of all files on that notebook's disks and prove to you that we could have also obtained any files from it without actually obtaining any sensitive files. If that doesn't convince you, we'll extract a single sensitive document of your choosing, send it encrypted to you, and destroy our local copy. Once the project is completed, we'll wipe all files that contain any sensitive information from - or about - the target network. We don't want to keep your sensitive documents as they only present an unnecessary burden to our operations as well as an undue exposure for you.

Furthermore, all project data is only accessible to the participating team members – usually two or three experts. When we need help from our experts outside the project team, we provide information to them on a "need to know" basis. To formally support our efforts in protecting the customers' information, all participating experts routinely sign project non-disclosure agreements before obtaining access to any project information.

Even though "movie scenes" in which a hired hacker brings a suitcase full of customer's confidential documents or hundreds of thousands of dollars in "stolen" money to the presentation can seem exciting and appealing, we believe stunts like this would present an undue and irresponsible endangerment of customer's sensitive information in an actual penetration test. We don't do that unless explicitly requested by the customer.

Finally, we're striving to maintain the maximum possible trustworthiness of our employees. Apart from the obvious fact that we don't ever employ ex-criminals or convicted hackers, we use pre-employment and annual background screening procedures including police and court record reviews for making sure our employees can be entrusted with highly sensitive information.

22. Why should we choose your company?

ACROS Security has been providing application security analyses to leading software vendors, financial institutions, governments and high-tech industry since 1998.

- We have **talented security experts** trained at "thinking like attackers", which is one of the most important skills a successful security analyst must have. And it is this very skill, combined with our constantly updated knowledge of security technologies, vulnerabilities and attack techniques that makes us so efficient in discovering generic and specific vulnerabilities in various kinds of products.
- Our **security analysis services keep us sharp** in rapid targeted identification of vulnerabilities in widely diverse products, which is a critical skill in this demanding and highly realistic type of penetration test.
- On average, we accomplish **nine out of ten mission objectives**.
- We produce **no false positives**, meaning that your engineers will not have to sift through our reports looking for actual vulnerability information. Instead, they'll be able to focus on confirmed problems and their solutions.
- Our results are presented to executives and engineers differently, based on their respective points of interest.
- We generate most of our revenue in the U.S. market, providing our services to some of the most critical and demanding organizations. Large security solutions providers regularly hire our experts to perform security analyses on their products, which protect the ultimately critical information in banks, Fortune 1000 companies, governments, military and intelligence agencies throughout the world.

We firmly believe our services to be among the very best in the global market. Our customers' feedback regularly confirms this belief, and we'll gladly take an opportunity to prove it to you.

ACROS Security: Finding Your Digital Vulnerabilities Before Others Do.

Call +386 2 3000 280 for more information or send e-mail to security@acrossecurity.com.

www.acrossecurity.com