PenTest magazine
Free Article
2/2011

PHYSICAL PENTESTING

A WHOLE NEW STORY IN PENETRATION TESTING

by Trajce Dimkov & Wolter Pieters

Physical Penetration Testing

A Whole New Story In Penetration Testing

Physical penetration testing plays an important role in assuring a company that the security policies are properly enforced and that the security awareness of the employees is on the appropriate level. In physical penetration tests the tester physically enters restricted locations and directly interacts with the employees to convince them to break a policy or provide credentials. The physical access and the direct interaction with the employees complicate the execution of the tests and have ethical, legal and safety implications.

When penetration testing is mentioned, the first thing management thinks of is trained security professionals behind their computers, hundreds of kilometers away, trying to penetrate the network of the company. And, in most cases they will be right. However, digital penetration tests are only one part of the whole story.

Information systems are not protected only by firewalls, encryption schemes and intrusion detection systems, but also by locks, fences, guards and policies on what the employees are allowed or forbidden to do. An adversary will not try to attack using only digital means, but will use the easiest way to achieve her target, whether that is social engineering an employee to obtain credentials, or physically entering the location where the information is stored.

Physical penetration tests are seldom done without social engineering, because when entering a location, it is imminent that the testers will have to interact with the employees, and use deception to reach their target.

Penetration tests that assess the effectiveness of the physical security mechanisms and the level of security awareness of the employees are named physical penetration testing using social engineering. Physical penetration tests are seldom done without social engineering, because when entering a location, it is imminent that the testers will have to interact with the employees, and use deception to reach their target.

Most of these tests also include elements from traditional penetration test. For example, in the first phase of the penetration test, the testers may use web tools to obtain an access card from an employee, which in the second phase is used to enter the premises of the organization. When the testers are inside the organization, they can use sniffers on the local network to obtain additional credentials or talk to employees, to escalate their privileges.

Physical penetration testing using social engineering requires more considerations than pure digital penetration testing. Methodologies for digital penetration testing strive to produce tests that are repeatable, reportable and reliable. These are reasonable requirements, because the companies want to have a step-by-step report of how the test was carried out and to be able to repeat the testing themselves. In addition, companies do not want tests that might interrupt their services during the penetration tests or tests in which the consequences cannot be anticipated.

Some of these requirements for a digital penetration tests are not possible in physical penetration tests, because these include the human element, making behavior depend on many influences and hard to predict. For example, although an employee can open the door for a tester during one test, it does not mean the employee will repeat this behavior the second time. Or, if a penetration

tester avoids the guards once, it does not mean during the second try she will not be spotted again.

Besides the problems with repeatability and reliability, the physical penetration tests also need to be *respectful* and *safe*. Measuring the resilience of an employee against social engineering in a physical penetration test is *direct* and *personal*. When the tester enters the facility of the organization and directly interacts with the employees, she either deceives the employee, trying to obtain more information about the goal, or urges the employee to help them, by letting the tester inside a secure area or giving the tester a credential. If these interactions are not done properly, they can upset the employees, violate their privacy or damage their trust toward the company and might lead to law suits and loss of productivity.

Contrary to digital penetration tests, where every step of the scenarios is approved ahead and testers cannot deviate from it, in physical penetration testing the tester has only a general scenario and they must continually modify it depending on how the situation evolves.

There are three main consequences from the personal interaction between the tester and the employee. First, the employee might be stressed by having to choose between helping a colleague and breaking the company policies. Second, the tester might not treat the employee respectfully, opening the company vulnerable to legal harassment lawsuits. Finally, when helping the penetration tester to enter a secure location, the employee who helped the tester loses the trust of the people who reside in the secure location.

A second consideration in physical penetration tests is *safety*. Contrary to digital penetration tests, where every step of the scenarios is approved ahead and testers cannot deviate from it, in physical penetration testing the tester has only a general scenario and they must continually modify it depending on how the situation evolves. In locations with armed guards or dogs, such as private properties, banks or museums, there is an additional risk the situation quickly escalates and results in injuries or victims. Although the majority of the penetration tests occur in office buildings, some of them are in hazardous environments. In nuclear, chemical or biological laboratories the tester needs to be very careful not to make actions that can harm the environment, the employees or themselves.

Methodologies For Physical Penetration Testing Using Social Engineering

In the last 3 years, together with colleagues from the computer science department, Andre van Cleef and Pieter Hartel, we worked on development on methodologies how to perform physical penetration tests using social engineering. The goal of the methodologies is to minimize the impact of the test to the employees and the productivity of the company, maintain the trust relationships among the employees and to maximize the repeatability, reliability and reportability of the tests. As part of the validation of the methodologies, we orchestrated over 30 physical penetration tests where groups of students obtained marked laptops from unaware employees at the premises of two universities. A schematic overview of our steps in the methodology is presented in Figure.

Setup

After the management decides to run a physical penetration test, the security officer initializes the test by defining the target, scope and the rules of engagement. The target of a physical penetration test is either the tester to leave objects (that should represent bombs or recording devices) in a restricted location or to take assets from a restricted location. If the scenario is a terrorist attack, where the terrorists plants a bomb, then the focus is only reaching the location. If the scenario is stealing an asset, then it is important to show that the tester can reach the location, take the asset and leave the company undetected. If the scenario is to put recording devices, the tester has to show that they can reach the location multiple times, to place the device and to collect the recorded material. From these goals, taking an asset is more challenging, because if the tester takes only a

Actors

During the penetration tests we identified 6 actors.

- *Security officer*. The officer is responsible for the security in the company and represents the management. The security officer knows where the sensitive assets are and has a clear picture which attack scenarios the management would allow and which are of too greater risk.
- *Coordinator*. The coordinator is usually a contractor responsible for the penetration tests and the behavior of the penetration tester. The coordinator with the help of the security officer orchestrates the whole penetration test.
- *Penetration tester*. This is a security professional who attempts to gain possession of the asset or leave objects without being detected or caught.
- *Contact person*. The security officer is usually having an overview of the test, but there is a person who provides logistic support in the organization and a person to be contacted in case of an emergency.
- *Custodian*. This is an employee responsible for the asset. The custodian should not be aware of the penetration test until the closing stage of the penetration test.
- *Employee*. This actor represents is the rest of the people in the company who have none of the roles above. The employees should also not be aware of the penetration test.

copy of the asset, the test is not realistic, and if the tester takes the original asset, she might cause production loss or service disturbance of the company. In addition, the custodian to whom the asset belongs is affected by these tests. The scope and the rules of engagement are defined similarly as with digital penetration tests.

The security officer hires a coordinator and assigns her contact people from the company to help with the test. The office also provides the coordinator with marked assets similar to the asset for which the security is measured. The penetration testers sign the rules of engagement before the start of the execution stage and get a *get out of jail* card in case they get caught.

The contact people should select a number of custodians based on specific roles the employees have in the company, or a specific characteristic. The custodians should not know the real purpose of the test; otherwise they would not react realistically. There should be a cover story which explains why the custodian is given the asset. The contact people give the marked assets to the custodians and get a signed informed consent. If the asset can store data, the document must clearly state that the custodian should not store any sensitive nor private data in the asset.

In the penetration tests we orchestrated, the asset was a laptop. The cover story was that we are performing a usability study on the laptops, and wanted to know if the employees find them useful in performing their tasks. In some of the penetration tests we chose the custodians based on which department they work for and their role in the department. In most of the tests, however, we chose the custodians randomly from the employee database.

Before the penetration test starts, the coordinator should distribute a list of penetration testers to the security officer, and a list of asset locations to the penetration tester.

Execution

When the execution stage begins, the penetration testers scout the area, obtain as much information as possible about the target asset and the custodian and propose attack scenarios. The coordinator and later the security officer should agree with these scenarios before the tester starts executing them. The coordinator checks whether the proposed attacks are within the scope of the test and follow the rules of engagement. The approved scenarios are then sent to the security officer for a second round of screening. The security officer has a more in-depth knowledge of the company thus she can judge the risk associated with each scenario on a more global perspective.

Figure 1. *Steps in a physical penetration test where the goal is to obtain a marked asset from an unaware employee within the premises of the company*

The penetration testers then begin with the execution of the approved scenarios (Figure 2). Although the scenarios should be as specific as possible and contain termination conditions, they should also leave space for improvisation. Along the course of the attack, the tester might be faced with unforeseen opportunities or difficulties, and must be able to make decisions on the spot.

If a penetration tester is caught or the tester gains possession of the asset, they immediately informs the contact person and the coordinator. Then the contact person inspects the location and informs the security officer. If the tester gains possession of the asset without the knowledge of the custodian, the contact person needs to reach the custodian before the custodian reaches the office and explain to the custodian that the test is terminated. The tester should also leave a note stating that the asset has been taken as part of a test together with contact details from the coordinator and the security officer. The security officer obtains surveillance videos from the CCTV and access logs and gives them to the coordinator to be included in the report.

Closure

After the execution of the penetration test, the testers should provide a report of the failed and successful attempts. In the closing stage, the coordinator collects the marked assets from the contact people and then debriefs the security officer and the custodians.

During the penetration tests, some of the employees might have been stressed by the penetration testers. These employees should be debriefed and it should be explained to the purpose of the test and why is it important for the company. Employees who were treated with respect and to whom the penetration tester did not cause discomfort during the interaction should

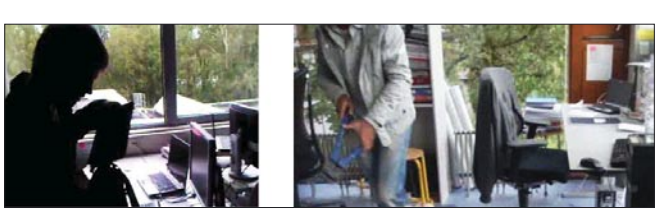

Figure 2. *Two pictures from the orchestrated penetration tests. On the left the tester used a master key to enter the room and take the marked, unlocked laptop. On the right, the testers entered the unlocked office while the custodians went for coffee and cut the Kensington lock with a bolt cutter*

not be debriefed, because the debriefing can cause more stress than the interaction with the penetration tester. The decision which employees need to be debriefed lies with the security officer. The employees that contributed to the success of the penetration tests should not be disciplined because they are only a symptom of the problem. The company should focus on improving its security policies and providing additional training for the employees to raise their security awareness.

The employees that contributed to the success of the penetration tests should not be disciplined because they are only a symptom of the problem.

While we were debriefing the custodians and the employees, we noticed that some of them felt deceived by the organization they work for. Some of the custodians were stressed from the penetration test either directly, because they were asked by the testers to violate a policy, or indirectly, by finding their asset is gone before the contact person reached them. The debriefing focused on their contribution to the tests and how the findings of the tests will help improving the security in the organization. All participants were rewarded for their participation and we took no disciplinary actions.

Closing Remarks

Physical penetration testing comes with ethical and legal implications, and cannot provide results that are as reliable and reportable as in digital penetration testing. Moreover, the physical penetration testing carries a safety risk to the employees and the testers performing the test. So, the question rises, why should we do such tests in the first place?

Physical penetration tests are not for every company and should be performed only by companies that specialize in this niche market. The main companies that order this type of penetration tests are the ones that will suffer huge consequences in money or reputation even if one attack succeeds, such as banks, laboratories that utilize intellectual property or cyber-centers. Without penetration testing these companies cannot estimate how big is their exposure to physical attacks, nor how the company culture is affecting the security awareness of the employees. This leaves the companies open to a whole range of attacks where the adversary does not restrict himself only to using a computer to obtain its target. For these companies, the legal and ethical implications of a penetration test are acceptable compared to the improved security they contribute to.

Methodologies that will improve physical penetration tests are in their infancy and are mainly developed in-house and never scrutinized by the pen-testing community. With further improvement, we believe we can eliminate the safety and ethical implications and provide usage for a greater spectrum of companies.

Further reading:

Dimkov, T. and van Cleeff, A. and Pieters, W. and Hartel, P.H. (2010) *Two methodologies for physical penetration testing using social engineering*. In:Proceedings of the Annual Computer Security Applications Conference (ACSAC), 06-10 Dec 2010, Austin, Texas, USA. pp. 399-408. ACM. ISBN 978-1-4503-0133-6

Dimkov, T. and Pieters, W. and Hartel, P.H. (2010) *Effectiveness of physical, social and digital mechanisms against laptop theft in open organizations*. In: Proceedings of the 3rd IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom 2010), 18-20 Dec 2010, Hangzhou, China. pp. 727-732. IEEE Computer Society. ISBN 978-1-4244-9779-9

TRAJCE DIMKOV

Trajce Dimkov holds a degree in Electrical Engineering, and has worked for a few years as a software developer. Currently he is a PhD researcher at the Distributed and Embedded Security Group in University of Twente, The Netherlands. His current research interests include physical penetration testing methodologies, social engineering, and formal methods for alignment of security policies.

WOLTER PIETERS

Wolter Pieters (1978) is a postdoctoral researcher in information security at the University of Twente. He studied computer science and philosophy of science, technology and society at the same university, and wrote his interdisciplinary PhD La volonté machinale: understanding the electronic voting controversy at the Radboud University Nijmegen. Afterwards he advised the Dutch Ministry of the Interior on electronic voting and electronic travel documents. Since September 2008 he works in the VISPER project at the University of Twente, concentrating on disappearing boundaries in information security. He was program chair of the 2010 CPDP workshop on Security and Privacy in Cloud Computing, and will co-organise the 2011 Dagstuhl seminar on Secure Architectures in the Cloud. He published on electronic voting, cloud computing, verification of security properties, access control, and philosophy and ethics of information security.