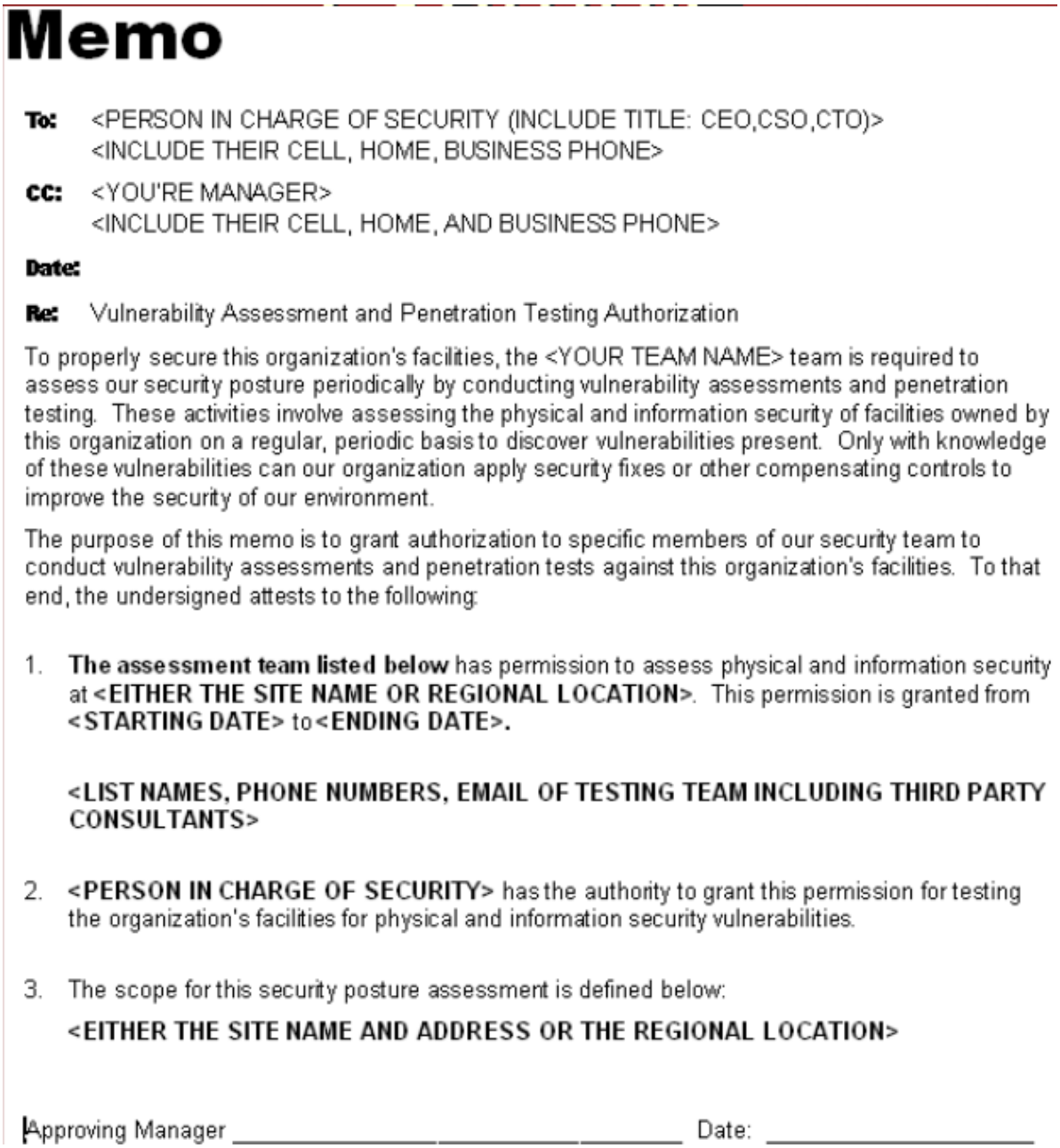
Physical Penetration Testing Toolkit

pentestlab.blog/category/social-engineering/page/2

January 27, 2013



Memo

To: <PERSON IN CHARGE OF SECURITY (INCLUDE TITLE: CEO,CSO,CTO)>
<INCLUDE THEIR CELL, HOME, BUSINESS PHONE>

CC: <YOU'RE MANAGER>
<INCLUDE THEIR CELL, HOME, AND BUSINESS PHONE>

Date:

Re: Vulnerability Assessment and Penetration Testing Authorization

To properly secure this organization's facilities, the <YOUR TEAM NAME> team is required to assess our security posture periodically by conducting vulnerability assessments and penetration testing. These activities involve assessing the physical and information security of facilities owned by this organization on a regular, periodic basis to discover vulnerabilities present. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our security team to conduct vulnerability assessments and penetration tests against this organization's facilities. To that end, the undersigned attests to the following:

1. **The assessment team listed below** has permission to assess physical and information security at **<EITHER THE SITE NAME OR REGIONAL LOCATION>**. This permission is granted from **<STARTING DATE>** to **<ENDING DATE>.**

   <LIST NAMES, PHONE NUMBERS, EMAIL OF TESTING TEAM INCLUDING THIRD PARTY CONSULTANTS>

2. **<PERSON IN CHARGE OF SECURITY>** has the authority to grant this permission for testing the organization's facilities for physical and information security vulnerabilities.

3. The scope for this security posture assessment is defined below:

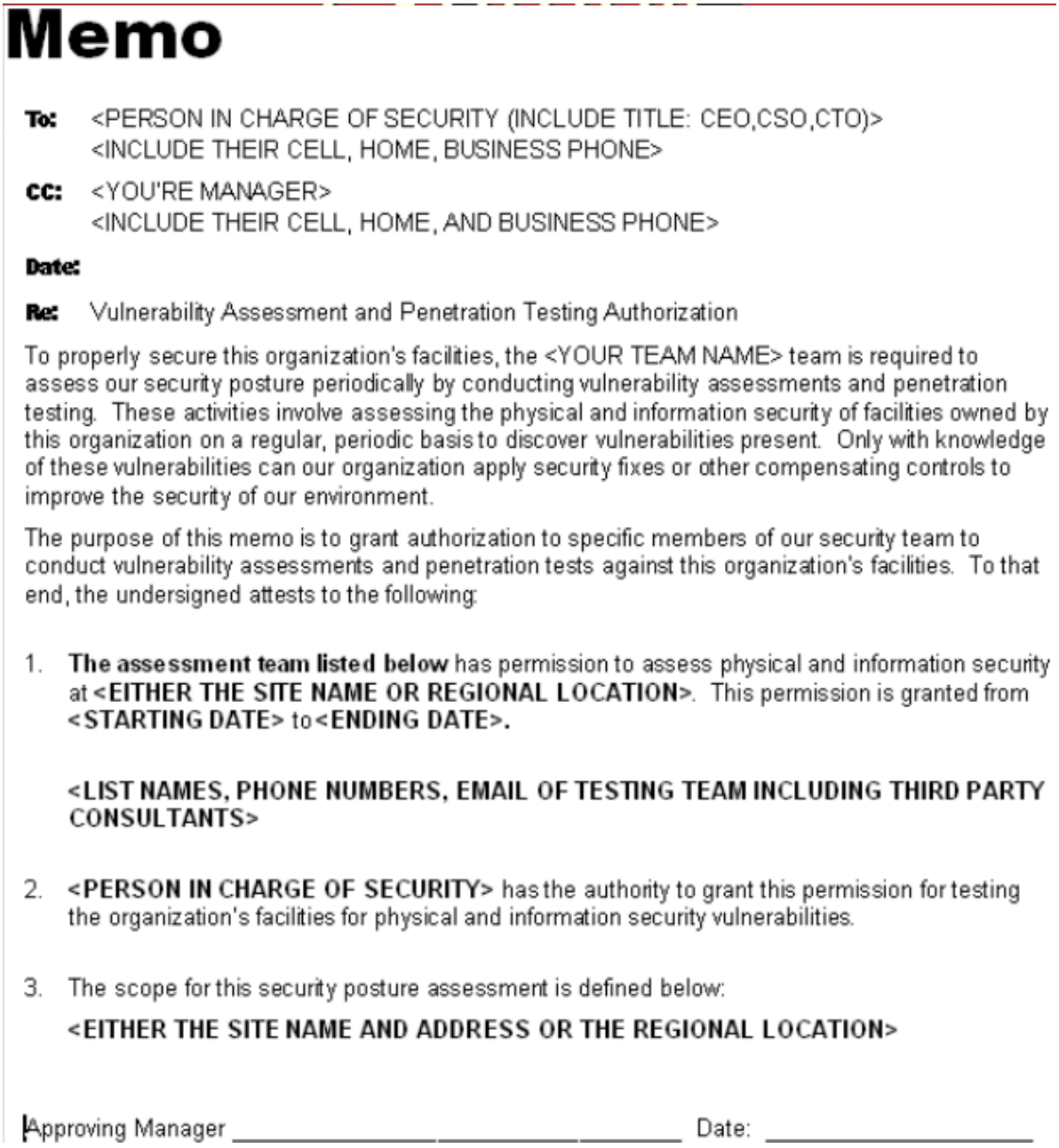
   <EITHER THE SITE NAME AND ADDRESS OR THE REGIONAL LOCATION>

Approving Manager _____ Date: _____

Most penetration testing companies provide and physical penetration testing as part of their services.Some of them are taking this service more seriously than others as they are spending part of their budget to obtain specialized costumes and equipment that can be used in physical penetration tests.In this article we will examine some of the equipment that is necessary to have if we are going to conduct a physical penetration test.

Get Of Jail Free Card

This is usually a signed letter from the client which states that the penetration tester is authorized to perform the test and the client is aware.This type of letter will work as a proof in case that things go bad and you will get caught by the security personnel or the police authorities.So the letter must include the contact details of the people that they are aware that a test is performed (preferably people in higher level positions) and must be reachable during the test.This letter should never be forgotten by the penetration tester and it is a good practice to have at least 2 original copies in case that one is lost accidentally or is destroyed.



Memo

To: <PERSON IN CHARGE OF SECURITY (INCLUDE TITLE: CEO,CSO,CTO)>
<INCLUDE THEIR CELL, HOME, BUSINESS PHONE>

CC: <YOU'RE MANAGER>
<INCLUDE THEIR CELL, HOME, AND BUSINESS PHONE>

Date:

Re: Vulnerability Assessment and Penetration Testing Authorization

To properly secure this organization's facilities, the <YOUR TEAM NAME> team is required to assess our security posture periodically by conducting vulnerability assessments and penetration testing. These activities involve assessing the physical and information security of facilities owned by this organization on a regular, periodic basis to discover vulnerabilities present. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment.

The purpose of this memo is to grant authorization to specific members of our security team to conduct vulnerability assessments and penetration tests against this organization's facilities. To that end, the undersigned attests to the following:

1. **The assessment team listed below** has permission to assess physical and information security at **<EITHER THE SITE NAME OR REGIONAL LOCATION>**. This permission is granted from **<STARTING DATE>** to **<ENDING DATE>.**

   <LIST NAMES, PHONE NUMBERS, EMAIL OF TESTING TEAM INCLUDING THIRD PARTY CONSULTANTS>

2. **<PERSON IN CHARGE OF SECURITY>** has the authority to grant this permission for testing the organization's facilities for physical and information security vulnerabilities.

3. The scope for this security posture assessment is defined below:

   <EITHER THE SITE NAME AND ADDRESS OR THE REGIONAL LOCATION>

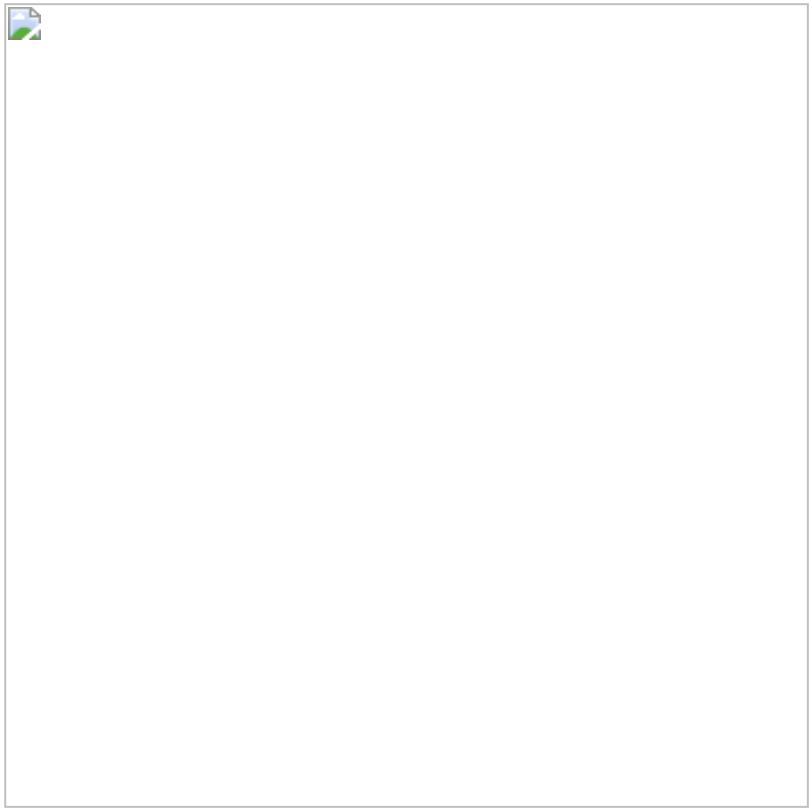
Approving Manager _____ Date: _____

Get Out Of Jail Template

Cameras

Cameras are important equipment because you can take photos of client documents,facilities and the areas that you have managed to gain access.These photos can be used as evidence in the penetration testing report afterwards.Of course cameras

of mobiles phones can be used as well but it is recommended a proper digital camera with large amount of memory.



Camera

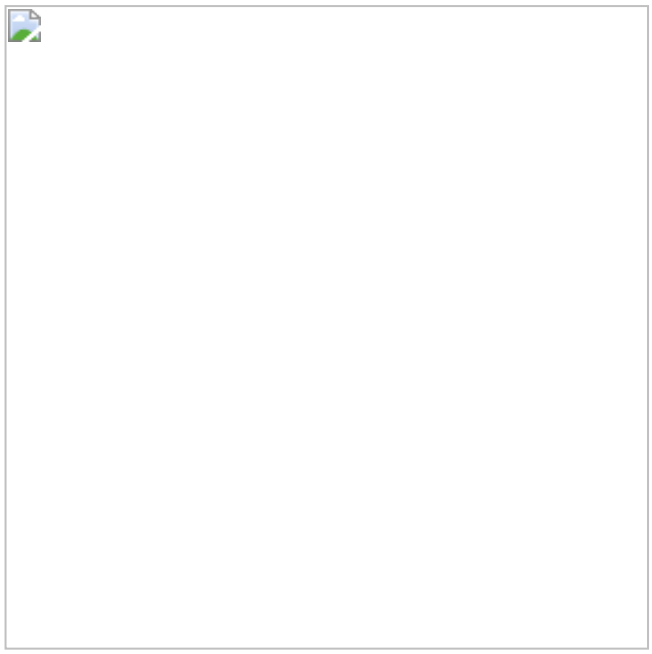
Binoculars

Binoculars are useful in cases that you want to observe the security guards from long distance or you want to perform shoulder surfing attacks against the employees of your client.For portability reasons and for not raising any alerts it is advised to buy binoculars that can fit into your pocket.

Portable Binoculars

Laptops

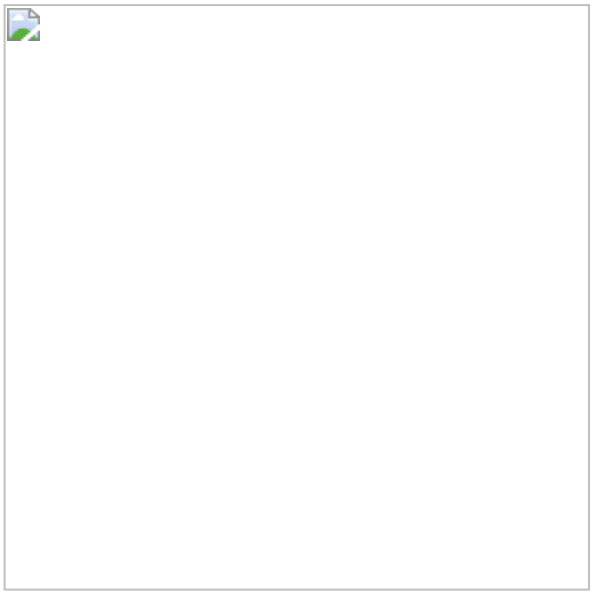
In a physical penetration test someone will assume that a laptop is not needed because all you have to do is to physical penetrate.Wrong!In case that you want to construct a scenario where you will disguise as an employee of the company a laptop is a critical component.Additionally you can have a case where the client will require from you to manage to attach into the internal network.



Laptop

GPS

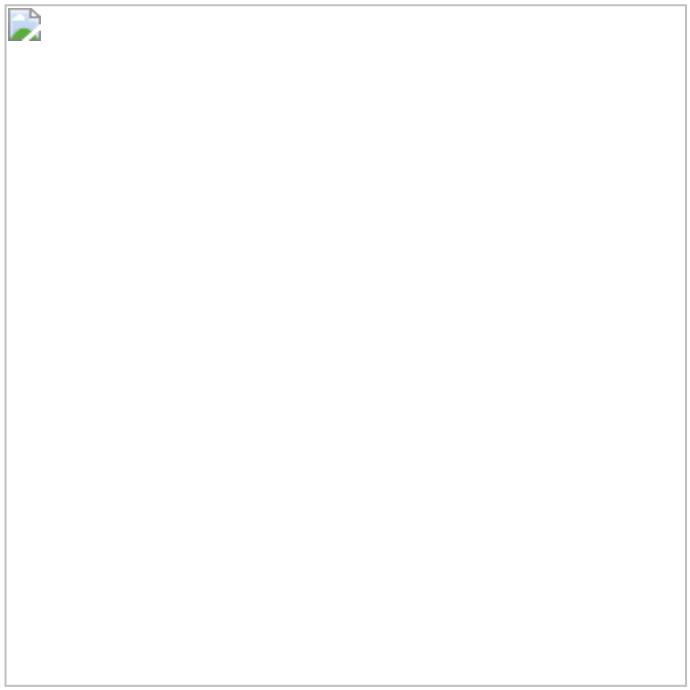
A GPS device can help you in many ways.First of all you can have an idea of the location that you are going to attack by observing satellite photos before the test.Alternatively you can use Google maps for that but the GPS has the advantage that you can carry it with you during the test and you can mark locations that you want to explore or to avoid.Also it is vital for your support team to know exactly where are you.Before you buy a GPS make sure that the device can export the route that you took in order to include it into the report.



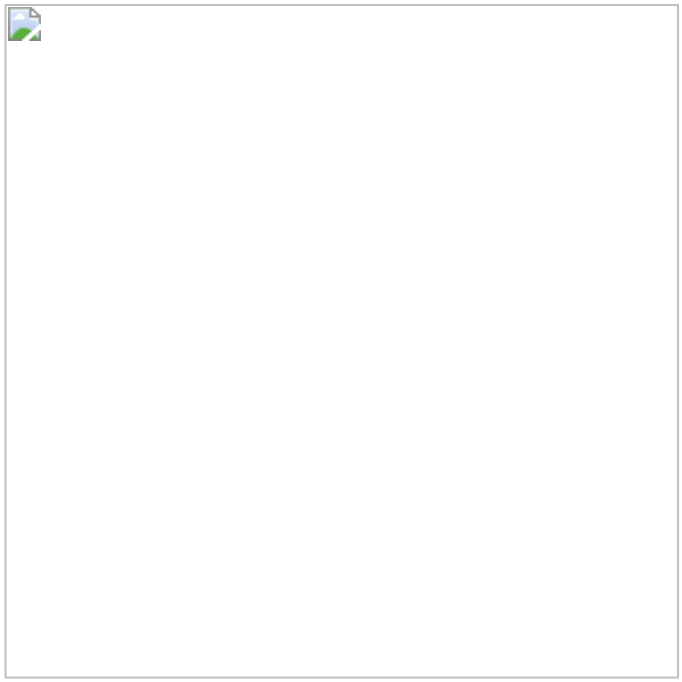
GPS Device

Lock Picking Tools

Of course in a physical penetration test you don’t expect every door to be open so it is essential to have in your bag and a set of lock picking tools.Generally lock picking tools are not very expensive so you will need to choose very carefully the best quality that it will assist your needs as you don’t want to break your client locks.



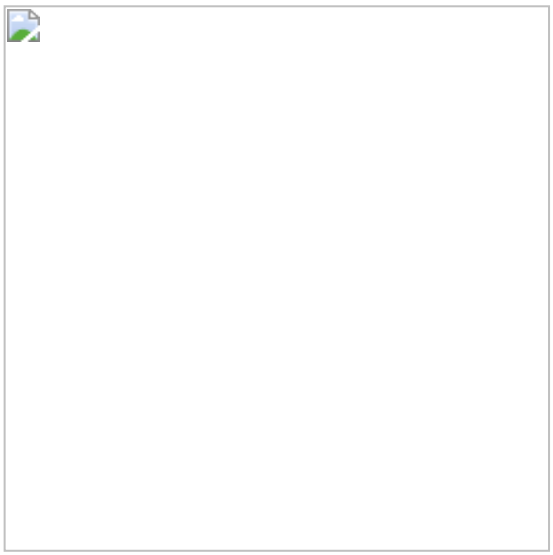
Lock Picking Tools



Snap Lock Pick Gun

USB Sticks

There are scenarios where in a physical penetration test you might require just to plant a USB stick inside the premises of the company that will contain malicious content.This will be the case when the client wants to test their employees awareness against this type of attack.You can use the social engineering toolkit in order to create the malicious USB or you can import your own files.



USB Sticks

Pwnie Express Tools

Pwnie Express is a company that specializes in constructing hardware tools that can be used in physical penetration testing engagements.Most of them are quite expensive but the effectiveness of the tools are high because they look like normal devices so when you will plug them on the network it will be difficult to be discovered by the employees or the administrators.Some of the devices that you can buy are the following:

- Pwn Plug mini
- Power Pwn
- and PwnPhone

Pwn Plug Mini

Power Pwn