MERIMETSO

Phishing / Social Engineering

Service Description Introduction

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Many recent high profile attacks have been leveraged using phishing techniques. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.

Other examples:

- Spear phishing is an example of targeting a department or individual.
- Whaling targets high profile professionals (i.e. CEO, CIO, Managing Directors etc.)

Our Approach

Engagement Structure

Below we outline a specific exercise which involves the sending of a phishing email in order to persuade recipients to divulge their username and password(s). It is essential that as few people as possible, including members of the IT Department, are aware that the exercise is being conducted. Obviously for professional reasons and since the success of the exercise is based on the fact that the target(s) must be unaware that they are a target, and must not be suspicious of the approach, we have limited the amount of detail we give here regarding our exact techniques. This test may be designed to examine the responsiveness of the IT department or any other responsible body to identify that an attack is underway and take the necessary actions to stop it.
Environment and people vulnerabilities can be a larger threat than network and IT vulnerabilities.

The Approach

We use various techniques, but they generally involve sending an email to nominated personnel. The email asks them to take certain actions which will result in them giving sensitive information like usernames and passwords. This information is then received by us, while the user is re-directed somewhere that looks genuine, in order to minimise suspicion. Social Engineering attacks will test the ability of employees to:
·Recognise and detect a possible security attack.

- To take appropriate action in the event of such an attack.
- To understand the necessity for keeping confidential information, including login details, secure.

Knowledge of the conducting of this exercise should be confidential

Methodology

Example Scenario

Passive reconnaissance against the target sites using open source information gathering techniques will be carried out, so the Our tester can get an understanding of the company structure, employees, and the company online profile. The most common phishing attack is spoofing the organisation website. We will register a domain similar to the organisation website, for example “www.organisation.co.uk”. The domain name would include the “www” without the full stop in order to trick the user into thinking the “www.” prefix is present. Once the domain is registered, Our will start work on duplicating the website layout and inserting a login form which would capture any data input and record it to a discretely placed file. The visits to the page will be captured. Via open source intelligence, using LinkedIn for example, the tester will identify an appropriate (usually someone in the IT support department or Senior Management) company employee. An email will then be created to be sent from said employee to the list of email addresses the client has supplied.

Client Employee Sample

A list of up to 30 names and email addresses will be given to us by the main Point of Contact. Our testing consultants will use their skills to carry out a discovery exercise on the company and its employees, in order to find a further 15 names and email addresses to target. These are usually representative across the different departments and disciplines. This exercise uses open source information available online only.

Output

A partially obfuscated list of gathered usernames and passwords presented within current data protection guidelines. An analysis of when phishing emails were opened, how long it took a target to click a link or open an attachment etc. At the end of the exercise, a comprehensive report will be produced. This will detail the approach, what was found and suggested resolutions. This report can be used in support of compliance requirements

Deliverables

In-depth report, broken down into 3 main parts:

1. Management Summary
2. Technical Overview
3. Detailed Technical Findings

Highlighting the vulnerabilities:

1. Type of RISK
2. The EFFECT of that RISK
3. Recommendations on how to address and mitigate vulnerabilities
4. Estimate of effort required to remediate any vulnerabilities identified

Project Management

Project Management resource will be assigned throughout the engagement but will not be allocated full time.

Key roles and responsibilities:

- Run engagement kick off workshop.
- Run engagement closure.
- Maintain and communicate engagement risks and issues log.
- Weekly status meetings and engagement tracker.

Prerequisites

The following pre-requisites are required from the client

- Email addresses of the targeted personnel
- Point of contact details

Deliverable Acceptance Criteria

Merimetso may present interim deliverables to the customer for review throughout the engagement. Should Merimetso present an interim deliverable, the customer will review, and either accept, or document specific corrective items in writing within three (3) business days. In the absence of any comments, deliverables produced by Merimetso will be deemed accepted after three (3) business days.

Limitations & Exclusions

- This engagement covers only the activities detailed in this document. Additional Merimetso offerings may be purchased as add-ons, otherwise additional consulting work not contained in this engagement is deemed out of scope.
- Working time is defined as Monday to Friday (excluding local bank/statutory holidays), 9am-5pm, with a 60-minute break for lunch.
- Merimetso is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities.
- Only third-party software and infrastructure identified during the pre-sales phase will be in scope for the engagement. There will be no change of scope where third-party software or infrastructure has been changed by the customer during the course of the engagement, or this will incur additional cost.

Customer Responsibilities

1. The customer must provide appropriate resources during the engagement from commencement date.
2. The customer must provide Merimetso representatives with information and resources to ensure Merimetso is able to successfully execute the engagement. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing resources, and attendance in planning, execution, or training meetings.
3. Customer will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review.
4. Customer must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third parties customer vendors, suppliers, and consultants.
5. If the consultant should travel to a customer location for the delivery of this engagement, there will be additional travel and expense costs. These travel and expense costs can be paid for prior to the engagement, or at actuals, at engagement completion.
6. The customer shall provide at least seventy-two (72) hours' notice for the cancellation or postponement of any work already scheduled as part of the engagement. In such scenario of a cancellation or postponement Merimetso reserves the right at its sole discretion to charge the customer for additional resources at Merimetso's then current daily rate for the delay period.
7. Customer must have a right to use the software and licenses. This requires that the customer must have purchased, or have converted, the appropriate license rights to the target environment.
8. Hardware requirements are the responsibility of the customer, and it is the customer's responsibility to ensure the hardware requirements are met prior to the engagement.

Merimetso may subcontract all or a portion of the services and/or have the services performed by one of its affiliates.

Note: The services described in this Service Description are subject to the terms and conditions by Merimetso Terms

Our Senior Testing Team

Dr Andrew Blyth - Founder and Director of R&D

Dr Blyth received his PhD in Computer Science in 1995 from Newcastle University, UK. Dr Blyth held the position of Professor of Computer Forensics at the University of South Wales, UK, throughout his illustrious career. Co-authored a textbook on Information Assurance, supervised 15 successful PhD candidates, created several BSc and MSc Computer Forensics and Cybersecurity Programmes. He was instrumental in the University of South Wales being the first University in the UK to behave an MSc in Computer Forensics accredited by the UK Government's National Technical Authority (GCHQ/NCSC).

He was the Cybersecurity Technical Lead at the UK Ministry of Defence's (MOD), Defence Science and Technology Laboratory (DSTL). During that time, he created and ran the Computer Network Defence Technical Demonstrator programme and defined various other research programmes within DSTL. He has over 50 peer-review publications and managed millions of dollars of research funding.

Campbell Murray - Founder and COO

Campbell is an established global leader in the field of information security. With over 25 years of experience ranging from offensive security assessments and security engineering in a vast range of environments providing Campbell with rare detail and insight into the field of cybersecurity. Campbell established himself as a penetration testing consultant in 2000. A firm believer in knowledge transfer, Campbell was a founding director of the TigerScheme in 2007 and the Cyber Scheme in 2013.

The Cyber Scheme is the recognised course used by NCSC to affirm CHECK status on any penetration tester who wishes to work on Government infrastructure in the UK. Campbell is now the chair of the technical panel for the Cyber Scheme and is one of only a handful of GCHQ appointed CHECK Team Leader assessors.

David Mound - Founder and CTO

David is a highly experienced Cyber Security Researcher with a demonstrated history of working in the Computer & Network Security industry and threat intelligence. Skilled in Penetration Testing, Reverse Engineering, Computer Forensics, Red Teaming and Threat Intelligence, he has worked with numerous global agencies within the 5 Eyes community, including GCHQ and the NSA delivering, advising on Red Team methods and engagements to assess Blue Team capabilities.

David's current speciality and focus are cloud-based technologies, and he holds multiple cloud certifications such as AWS Certified Security Specialist. David is an ex-Naval officer and is currently a member of the Army Reserves, where he coordinates threat hunting and assists network defence within the UK MOD and Gov estates. David brings his extensive technical capability to design the innovation to the Merimetso Cyber Technical Training platform.