Social Engineering

Case Study and Preventative Measures

Case Study

- Whurley was hired by a resort group in Las Vegas to perform a security audit
- He spent a week surveying the Strip in order to research the culture
- The audit was performed two weeks premature in order to ensure that the manager of the resort did not inform the employees of the audit
- The goal of the audit was to try to get into every protected area of the casino, document his presence and try to penetrate as many security systems as he could. He also wanted to access the financial systems and the visitor information.

Case Study (contd)

- The night before the penetration test he heard about a special the casino offered on their fitness club
- He went to the club and spoke to a lady called Lenore
- Lenore was the financial auditor of the casino
- Whurley observed her non verbal cues and attempted to create a common ground for communication
- Lenore accepted to go for dinner with Whurley

Case Study (contd)

- During dinner with Lenore he told her that he was also interested in become a financial auditor
- Lenore provided information about her job and even provided details about what her job entails and who her employer is
- The next day Whurley attempted to access the casino and carried along a wireless gateway and an antenna

Case Study (contd)

- Standing outside the casino Whurley noticed two security guards talking
- The conversation ended and Whurley started walking along the street
- He let the security guard pass him and only then asked attempt to start a conversation with the guard
- If you approach someone from behind, people are generally less defensive than if approached from the front

Case Study (contd)

- Whilst talking to the guard, Whurley noticed the guard had a name badge which said Charlie
- Also another guard called Charlie by his nickname Cheesy
- After this he went to the employee entrance of the casino which was guarded by another security guard
- He asked the guard at the entrance if he has seen Cheesy

Case Study (contd)

- Whurley mentioned that Cheesy owes him $20 which Whurley needed for lunch now
- The guard asked why Whurley needed money for lunch (as employees get free lunch)
- Whurley said that he needed the cash to take out a lady friend
- The guard then mentioned that Cheesy is gone for the rest of the week and Whurley responded shockingly

Case Study (contd)

- This guard then felt compassion for Whurley
- He gave Whurley $40, because he said that $20 is not enough to treat a lady
- He also attempted to give Whurley “fatherly” advice
- The guard then let Whurley in without ever asking for the name badge
- Just as Whurley walked in the guard yelled and asked for the badge, on which Whurley responded that it is in his bag.
- The guard just accepted this information as true

Case Study (contd)

- Walking inside the building Whurley did not really know where to go
- He was wearing clothes which resemble a junior executive position
- Most of the other people in the building were wearing staffer clothes and thus didn't question him
- Whurley found a room which was a camera room. It contained many screens and vcr’s

Case Study (contd)

- Whurley walked into the room and immediately said to the guys in a commanding voice “Focus on the girl on 23.” before anyone could challenge him
- Whurley stood there for 15 minutes just examining the cameras
- Whurley then said that he is Walter from internal audit and he just got hired onto Dan Moore’s staff
- He picked up the name Dan Moore in one of the conversations with Lenore (The girl from the previous night)

Case Study (contd)

- The people in the camera room then helped “Walter” to find the executive offices as he pretended that because he is new he does not know where they are
- Walking towards the executive offices he found a small break room
- He walked into the break room to find a lady called Megan
- He spoke to her about his new job and when she realised that he was from internal audit she gave him some items which needed to go there

Case Study (contd)

- Included in these items were a few name badges, internal memos and papers which belonged to the internal audit office
- Whurley now acquired a name badge. He flipped it around so that the picture was not visible though
- Whurley then walked out to find another office which was empty
- In this office was two network ports which he could not determine if they were working by just looking at them

Case Study (contd)

- Whurley then went back to Megan and told her that he forgot to tell her that he must add a “network security monitor” to her machine
- He then went to sit at her desk and gracefully asked for her password which she just provided
- Whurley then showed her the wireless access point from his bag and said that he must add this
- She responded by saying that she doesn’t understand the geeky stuff and he must just go ahead while she goes to the bathroom

Case Study (contd)

- While she was out he plugged in the wireless access point into the machine and also used a flash drive to copy data from her machine
- He then asked her, when she returned, where the Network Operation Centre is and proceeded there
- Arriving at the NOC he realised his badge doesn't allow him in and he tried knocking on the door
- A guy opens the door and Whurley spins the story that he is from internal audit
- The guy who opened the door then decided to clarify this information with this boss (Richard)

Case Study (contd)

- Richard then asked Whurley an array of questions
- He then said that he is going to call Internal Audit to verify the information
- Whurley was thus busted for being a fraud
- Whurley then thinking on his feat admitted defeat to Richard and said he was doing a security audit and gave Richard a business card which reflected his name as Whurley and that he was from a security audit firm
- He then tells Richard about his findings so far and insists that Richard calls the person who hired Whurley to confirm his indentity

Case Study (contd)

- This gamble paid of greatly, because Richard then assumed Whurley was legitimate and didn't verify his identity
- Whurley just continued telling Richard about all the flaws he found
- It was close to lunchtime and Richard invited Whurley to have lunch with him
- Walking to lunch Whurley again insists that Richard verifies his identity on which Richard responds "You've got a card, I know who you are"

Case Study (contd)

- Whurleys newly acquired “friend” then had lunch
- Richard was the director of IT, and is responsible for computer security
- Richard was then sharing all kinds of privileged information with Whurley, but has never taken the basic step of verifying his identity
- After lunch Richard took Whurley into the NOC and introduced him to Larry
- Richard told Larry that Whurley is trustworthy and told Larry all about the audit

Case Study (contd)

- Larry then accepted this information and told Whurley lots of sensitive information
- Whurley then told Larry about the access point he left in Megan's office and that he needs to go get it
- He told Larry that he now needs a badge to get back into Megan's office
- Larry was reluctant to give a badge and Whurley said he should ask Richard if it is okay.
- Larry then phone Richard who said Whurley can get a badge of an employee who has been fired earlier the week and was not yet deactivated

Case Study (contd)

- Larry and Whurley then spoke about the network layout and what security measures were in place
- Larry's wife then called who sounded angry
- Whurley then told Larry to put his wife on hold and told Larry that he should sort out this issue with the wife and Whurley will help himself to a badge
- So Whurley helped himself to two or more badges
- Whurley then left Larry for 20 minutes and proceeded back to Megan's office

Case Study (contd)

- Whurley knew that badge access was controlled by a computer system
- He now wanted to gain access to this computer
- He didn't know where this system was and decided he is better of asking someone
- He decided to ask the security guard at the employee entrance, because he was the most helpful so far
- The guar d then pointed him in the right direction

Case Study (contd)

- Whurley located this system in a small networking room
- The machine was on the floor with a list of ID badges already open
- The machine had no screen saver or a password
- In Whurley's view, this is typical. "People have an 'out of sight out of mind' mentality"
- Whurley then gave his new badge all area access
- He then swopped some employees names on the cards in order to muddy the audit logs

Case Study (contd)

- Whurley then went to collect the access point from Megan's office
- He went back to Larry's office who just finished on the phone
- He asked Larry to explain the network topology in detail
- Larry was reluctant and Whurley quickly said sorry "How is things with your wife?"
- After Larry explained this he told Whurley all about the network topology

Case Study (contd)

- Whurley then told Larry he needs to do a network audit and Larry gave him access to his machine
- Whurley then took out his machine and showed it to Larry
- Because Whurley had top of the range IT equipment any real geek would love to see “new gadgets” so Larry let Whurley plug this into the network
- Whurley then proceeded to compromise many machines on the network and burn some information to DVD’s which was never questioned

Case Study (contd)

- After gathering tons of sensitive information Whurley decided to really push his luck
- He decided to ask all the people he spoke to, to take a picture of them with Whurley in the photo
- This proved to be amazingly simple as everyone agreed
- He then left the casino and provided all the evidence to the internal audit officer who was shocked to see what Whurley was capable of doing

Countermeasures

- Developing clear, concise security protocols that are enforced consistently throughout the organization
- Developing security awareness training
- Developing simple rules defining what information is sensitive

Countermeasures (contd)

- Developing a simple rule that says that whenever a requestor is asking for a restricted action (that is, an action that involves interaction with computer-related equipment where the consequences are not known), the requestor's identity must be verified according to company policy
- Developing a data classification policy

Countermeasures (contd)

- Testing employees on ways to resist social engineering attacks
- Testing your employee's susceptibility to social engineering attacks by conducting a security assessment

Guidelines for Training

- Raise awareness that social engineers will almost certainly attack their company at some point, perhaps repeatedly
- Use role-playing to demonstrate personal vulnerability to social engineering techniques, and to train employees in methods to resist them
- Aim to establish a sense in the trainees that they will feel foolish if manipulated by a social engineering attack after the training

Designing programs for countering social engineering

- Develop procedures for employee actions when a social engineering attack is recognized or suspect
- Develop simple guidelines for employees, defining what information the company considers sensitive
- Modify organization politeness norms – It's okay to say "NO"!

Designing programs for countering social engineering (contd)

- Developing procedures to verify identity and authorization
- Get top management to buy-in: Inform employees that they will NEVER be asked by management to circumvent any security protocol. And no employee will get into trouble for following security protocols, even if directed by a manager to violate them

References

- Kevin D. Mitnick, William L. Simon, The art of Intrusion, John Wiley and Son, 2005