SecurusGlobal

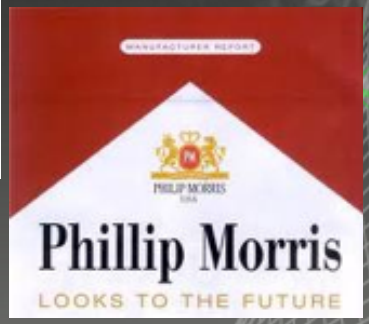

Social-Engineer.org
In Association with
DEFCON
Presents
The Social Engineering CTF
How Strong is your Schmooze?

CTF Event Background

- Social engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.
- The team at Social-Engineer.org was invited to run the Social Engineering Capture the Flag (SE-CTF) event for Defcon 18
- Contestants were assigned a target company, with each having two weeks to use passive information-gathering techniques to build a profile.
- The information was compiled into a dossier that was turned in and graded as part of the contestant's score.

SecurusGlobal

Target Companies:



Information Sources

- The contestants used many different sources for gathering data on the assigned targets.
- However, a few information sources were used by almost every contestant: Google, LinkedIn and Facebook.
- LinkedIn is a service that has not received as much popular attention, but in the context of the CTF event was far more useful than any other single information source.
- I was able to build very complete organisational chart simply by mapping relationships of employees within their target organisation.

Sources Of Information:

Pretexts Used

- Pretexting is when a social engineer develops a storyline that he or she are able to portray to the target.
- The pretext of a survey is an obvious one that justifies the contestant making a great number of questions without alarm being raised.
- The pretext of internal employees, however, is a more complex pretext to successfully accomplish. Proper execution of this approach requires a greater degree of information gathering in order to ensure that suspicion is not raised by the caller not having information that an employee would be expected to have.

The Flags

- Contestants were allowed 25 minutes to contact their assigned targets during the course of the contest.
- Flags were picked to be non-sensitive information, and each was assigned a point value based on the degree of difficulty in obtaining the information associated with the flag.
- The contestant's job was to develop a believable pretext along with a real world attack vector that would enable them to obtain as many flags as possible.
- Then they performed their attack vector live at Defcon during their 25 minute time slot.

Defcon Setup

In House IT Support?

How are Documents Disposed of?

Employee Schedules?

What Service Pack?

Version of Mail client?

Is there a Cafeteria?

Days of Months Paid?

Shipping Supplier?

Browser?

PDF Reader?

Websites Blocked?

VPN Software?

Who Supplies Food?

Open a Fake URL?

Trash Handling?

Who Does Offsite Back-Up?

PBX System?

Mail Client?

Anti-Virus Used?

ESSID Name?

Duration of Employment?

Time Deliveries Are Made?

Version of Browser?

Version of PDF Reader?

VPN In Use?

Badges for Bldg Access?

Wireless On-Site?

Employee Process?

Successfully Targeted Employees

In the course of the contest, most successful calls were directed toward call centers. This allowed for ease of contacting a potential target, letting the focus of the contestant's time to be directed toward the collection of flags.

How to Prevent Social Engineering Attacks

- Education & Awareness
- Social Engineering Audit
- Security policy
- Vet your staff
- Get your staff involved
- Don’t trust anyone until verified

Conclusion & Recommendations

- One of the primary factors in the success or failure of the contestant in the Capture the Flag event had to do with the planning of the overall attack.
- The most interesting aspect of this has to do with how quickly and easily information could be obtained from all companies in a relatively short period of time, even with the caller under pressure.
- An important aspect of what was revealed by this event was that companies are only as secure as their weakest employee.
- Social engineering is a very real and dangerous attack vector prepare and train your staff for it.