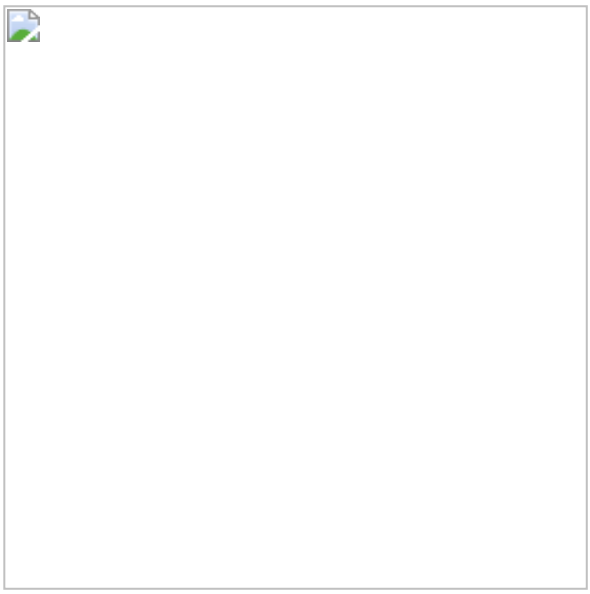
Dumpster Diving

pentestlab.blog/category/social-engineering

March 28, 2013



Dumpster diving is a method of obtaining information about a company just by examining their trash.This technique was very popular especially back in the 90's where many old school hackers like Kevin Mitnick had managed to hack major companies just by discovering critical information through their garbage.This proves that companies and organizations must take into their consideration how they manage and destroy their trash in order to mitigate this threat.

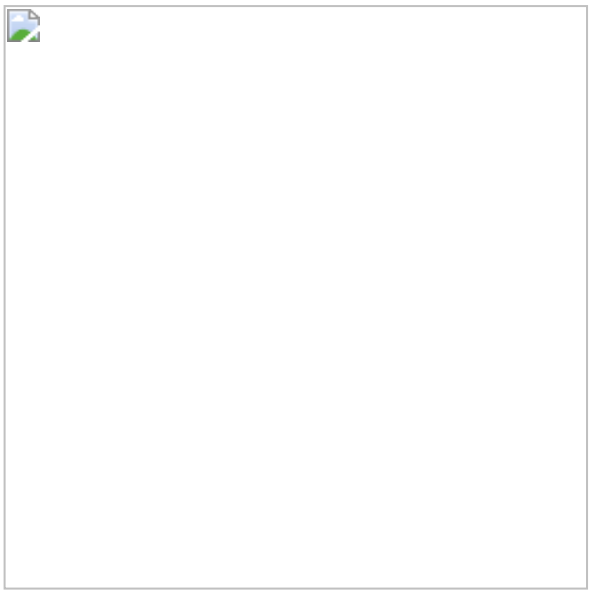
In nowadays dumpster diving can be a part of physical penetration test.The information that the penetration tester should collect will help him to construct his attack scenario.In this article we will examine what a penetration tester should look for when he is performing a dumpster diving for his engagement.

Employee Information

Documents that contain information about employee's names,departments etc are very important as they can be used during the physical penetration test as information which is valid.Knowing already information from inside will allow you to establish more easily the trust as you will appear as someone valid.

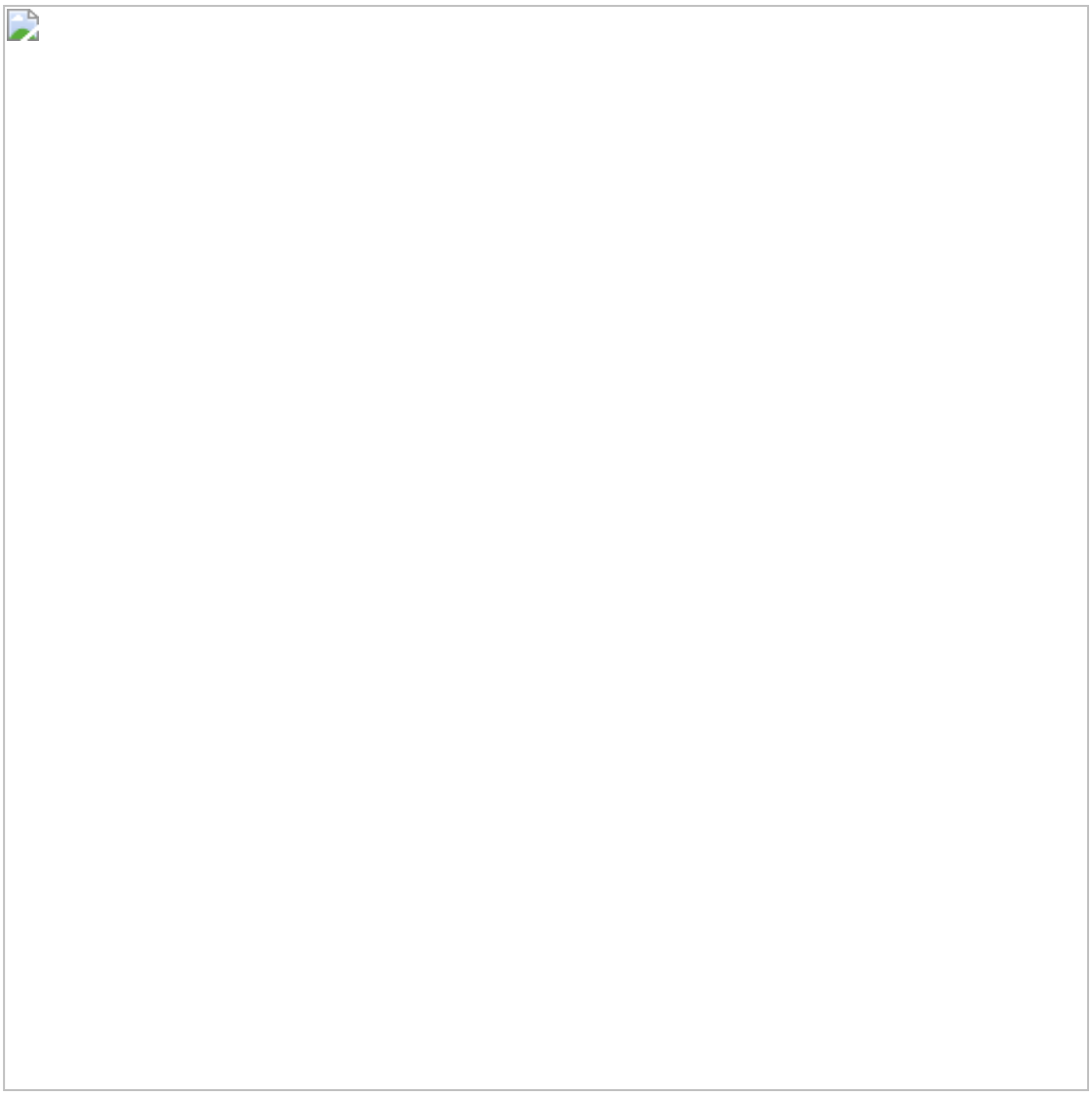
Emails

Obviously you can find corporate emails and from other sources like Linkedin,official website etc. but also papers containing some email address is always a good finding as you will be able to discover internal information and also the structure of the emails accounts inside the company.



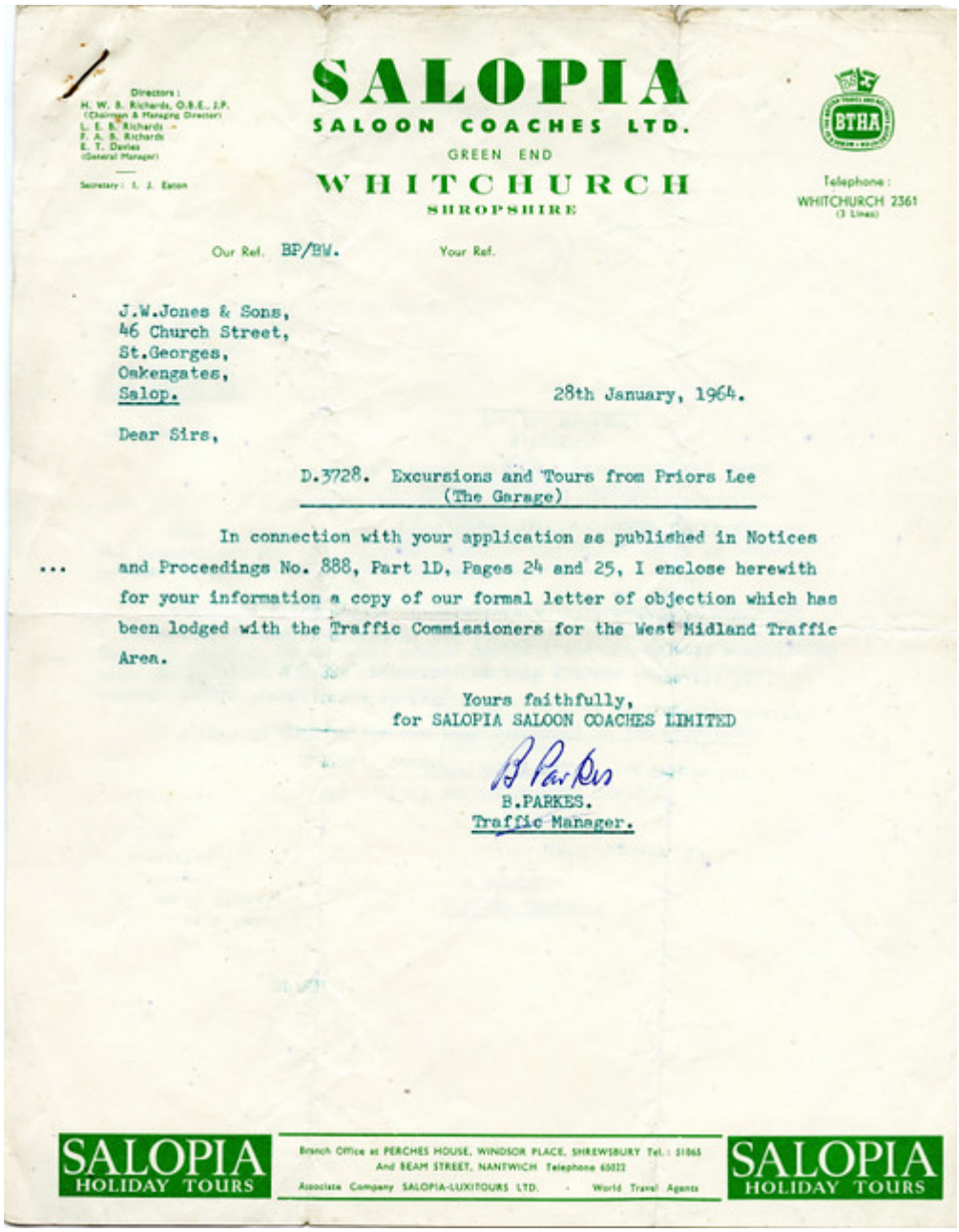
Network Diagrams

Diagrams about the internal network of the company can also be found in the trash.Network diagrams in many cases contain IP addresses,server names,network ranges and IP’s of routers which can allow the penetration tester to have a better understanding about network and which assets are important.



Headed Papers

These kind of papers can help penetration testers to create forgeries of the documents.This is essential for any social engineering engagement as you can cheat the employees to perform the action that you want.



SALOPIA
SALOON COACHES LTD.
GREEN END
WHITCHURCH
SHROPSHIRE

Directors:
H. W. B. Richards, O.B.E., J.P.
(Chairman & Managing Director)
L. E. B. Richards
F. A. B. Richards
E. T. Davies
(General Manager)

Secretary: S. J. Eaton

BTHA

Telephone:
WHITCHURCH 2361
(3 Lines)

Our Ref. BP/BW. Your Ref.

J.W.Jones & Sons,
46 Church Street,
St.Georges,
Oakengates,
Salop.

28th January, 1964.

Dear Sirs,

D.3728. Excursions and Tours from Priors Lee
(The Garage)

In connection with your application as published in Notices and Proceedings No. 888, Part 1D, Pages 24 and 25, I enclose herewith for your information a copy of our formal letter of objection which has been lodged with the Traffic Commissioners for the West Midland Traffic Area.

Yours faithfully,
for SALOPIA SALOON COACHES LIMITED

B.PARKES.
Traffic Manager.

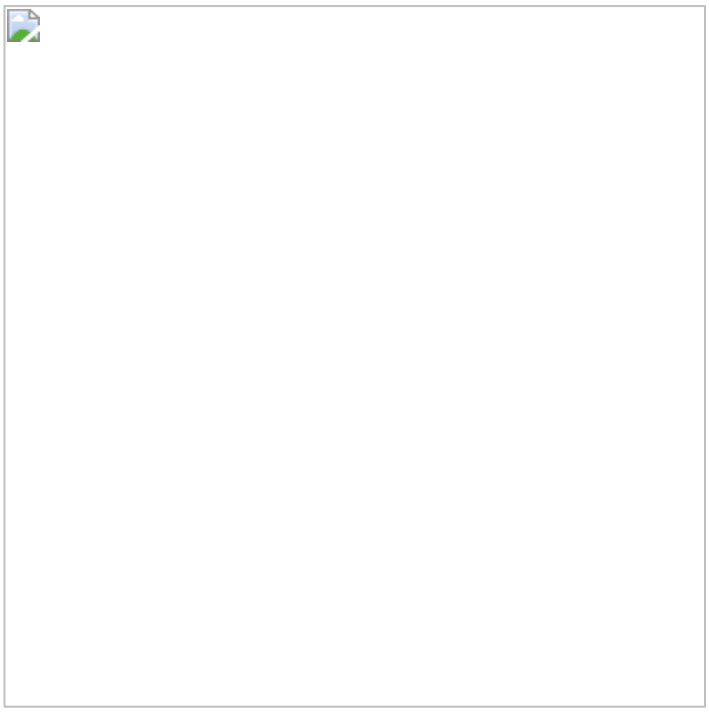
SALOPIA HOLIDAY TOURS

Branch Office at PERCHES HOUSE, WINDSOR PLACE, SHREWSBURY Tel.: 51065
And BEAM STREET, NANTWICH Telephone 65022
Associate Company SALOPIA-LUXITOURS LTD. - World Travel Agents

SALOPIA HOLIDAY TOURS

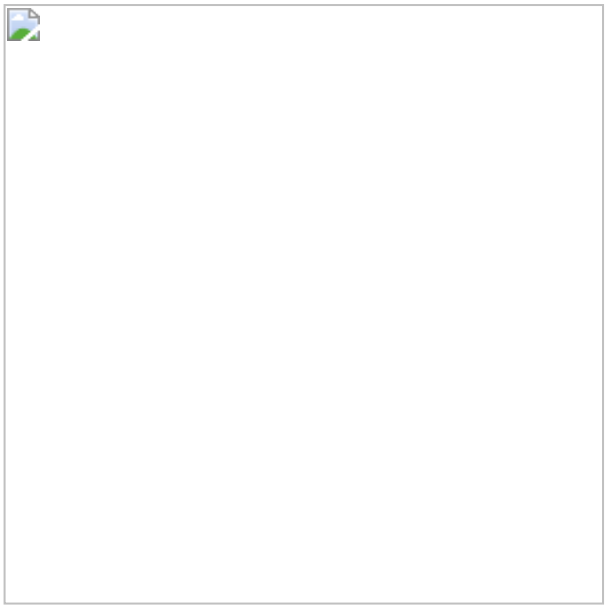
Invoices

Invoices unveil information about the company's clients and partners.This can prove very handy as the penetration tester can use this information in order to masquerade himself as an employee of the company that the target is doing business which in this scenario will give him an easy access to the target premises.



Usernames And Passwords

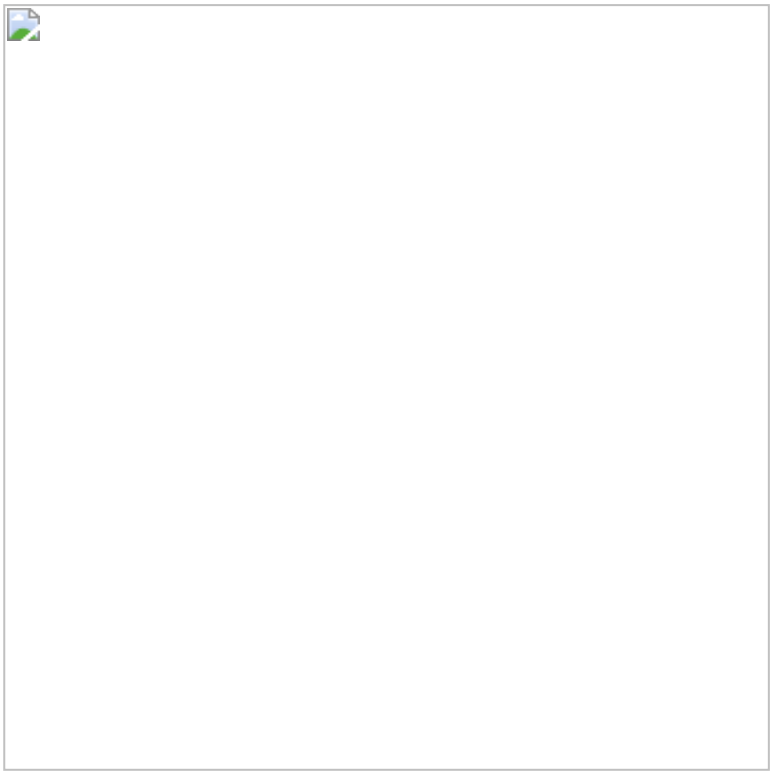
It is quite common for many company employees to keep their usernames and passwords in sticky notes.This piece of information can be often found in the garbage as administrators are enforcing passwords to be change every 2 or 3 months.Such a discovery will unveil how usernames and passwords are constructed and with a bit of luck some of them can be valid.



Electronic Media

USB sticks,CD and DVD disks even hard drives can be found in the garbage.These can be collected and analyzed later off-site.Usually nobody would bother to delete the data from a USB stick or to destroy properly a DVD disk before he throws it to the trash so

such a discovery means wealth amount of corporate information.



Handbooks,Manuals And Operating Procedures

Manuals and handbooks are often found in company's trash.This is because these documents are get updated often and the older versions are no longer needed.Usually in these documents there is plenty of information regarding internal processes and systems which can have their own role in the engagement.

Signatures

Papers that contain signatures especially from authorized people like CEO's,Head of departments and Account Managers are also important as the signature can be easily copied and used in a variety of scenarios as a valid authorization document.

Sincerely,

Kenneth D. Lewis
Chief Executive Officer and President

Shredded Paper

Even though that many companies are using shredder machines in order to destroy their documents effectively this in some occasions doesn't seem enough.This is because some shredders doesn't mix their blades when they are destroying the paper so the paper is shredded into strips.If you discover a piece of papers in strips then you can try to reconstruct the paper on your own or to use a software solution like the Unshredder.