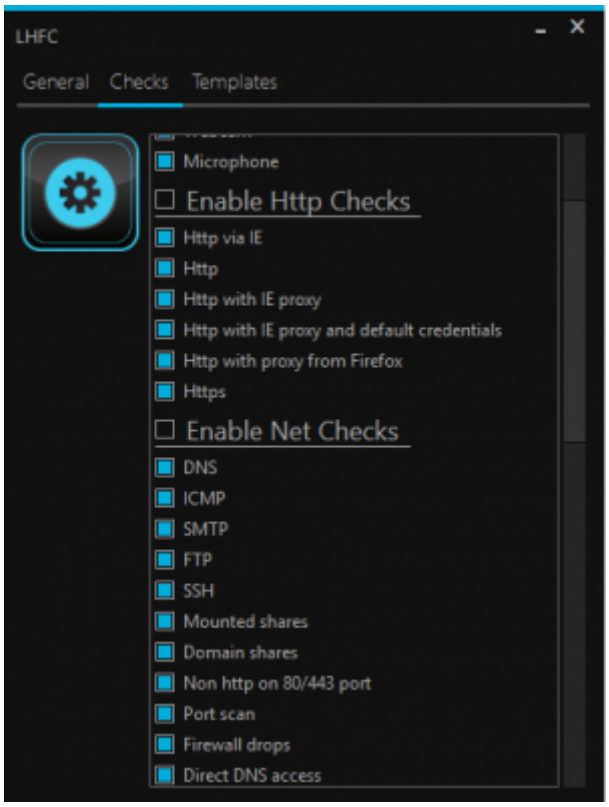
Technical tests without involving employees

LUCY offers the possibility to carry out technical tests without the involvement of employees. These are tests of the infrastructure (network, Windows client etc.).

LHFC - Malware testing Simulation

You have invested time, effort, and money in defenses. However, employees may still execute a malicious file. How do you know your defenses will work? To reduce the risk from malware coming into your environment, you need safe and effective ways to test your systems. This is where LUCY's Malware Simulation Toolkit (LHFC) comes in place. LHFC is an advanced malware simulation suite capable of emulating various threat simulations equivalent to many of the tools employed by hackers. More info about this test can be found here.



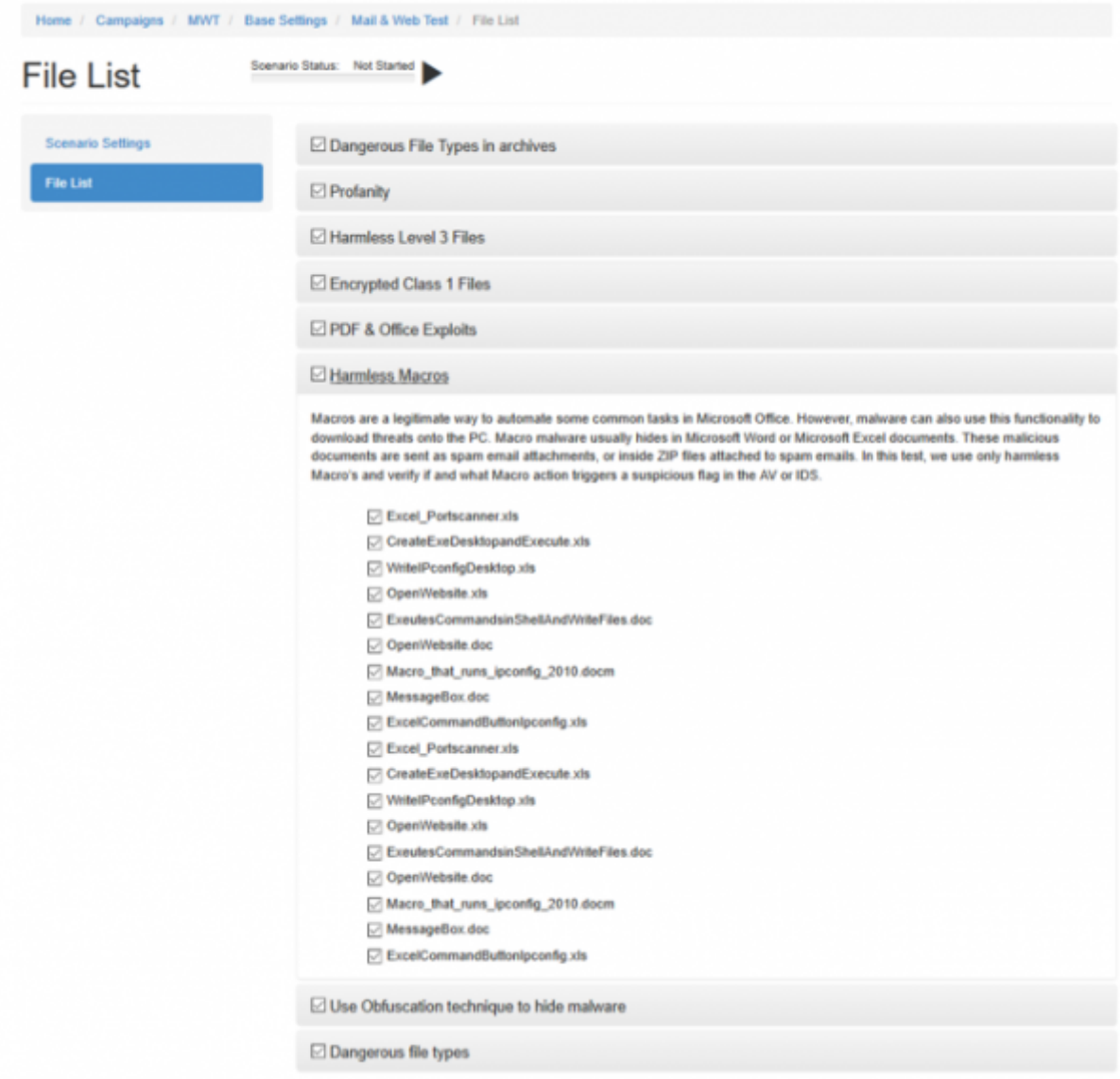


Main Questions answered by this tool:

- Does your AV detect known Malware downloads?
- What happens if an employee falls for a real attack?
- Is your SIEM able to trigger activities from this tool?
- Is Malware able to modify System Settings?
- Is Malware able to communicate to external servers?
- Can Malware access sensitive data on the local host or your intranet?

Mail and Webfilter Test

The Email and Internet malware protection test checks whether the implemented security measures are sufficient to defend against an unstructured or structured malware attack via the e-mail infrastructure or internet infrastructure. With our software you can check which file types could potentially enter the company and which are blocked by the security infrastructure. LUCY works with a wide range of file types that can be brought to the end system via e-mail or on a website for download. You can thus see whether potential malicious code, such as Java files, backdoors, scripts, embedded Office Objects are detected and blocked by the filter infrastructure. Based on these results, you can then carry out targeted phishing campaigns. More info about this test can be found here.



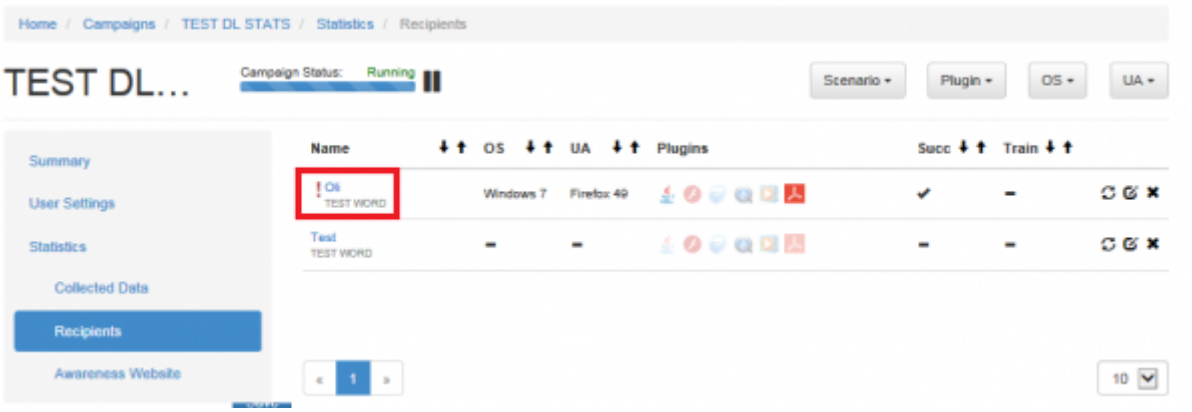
Main Questions answered by this test:

- How can malware potentially enter your network?
- What type of file types can be send as attachments to the end user?
- What type of file types can be downloaded from a website by the user?
- Does your internet and mail protection software detect potential malware?
- Does your internet and mail protection software detect obfuscated malware?

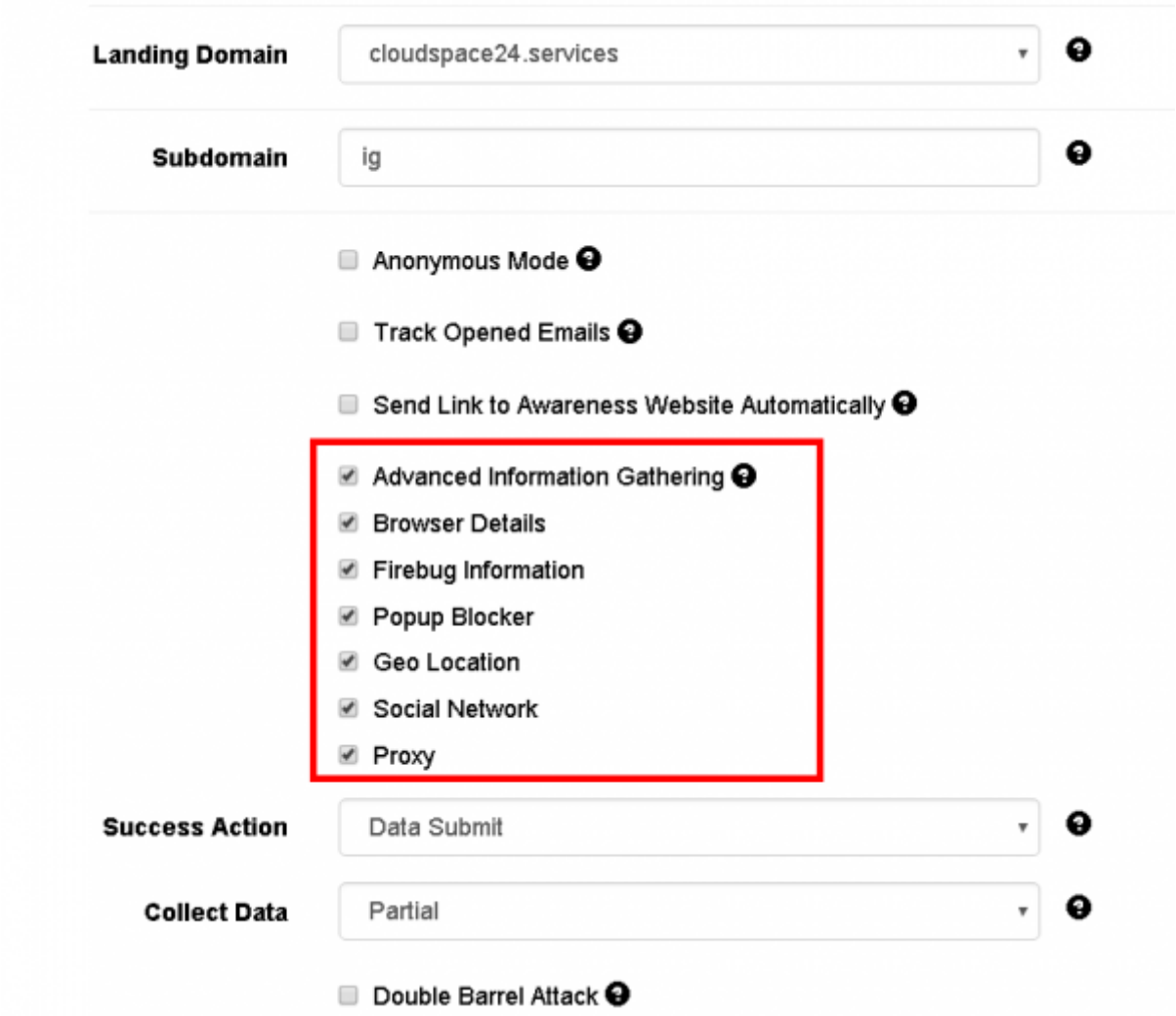
Vulnerable Browser | Vulnerable Client detection

When running a campaign, LUCY will tell you based on the user agent, if there is any vulnerability within the browser or plugins. A User Agent is a short string that web browsers and other applications send to identify themselves to web servers. A user agent string contains the following information: Mozilla/[version] ([system and browser information]) [platform] ([platform details]) [extensions]. Unfortunately, most browsers falsify part of their User-Agent header in an attempt to be compatible with more web servers. LUCY also is only enumerate major versions (like IE 11) but not minor versions which would show the actual patch status, some results might be false positives. Example: if you don't use the latest IE (e.g. IE10) we will query the CVE database and present all vulnerabilities for IE10 (http://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-9900/version_id-138705/).

But that does not mean the IE is not patched. This only displays all possible vulnerabilities for this browser version. Within the campaign statistics the vulnerable clients are displayed with an exclamation mark:



Additionally to the user agent, you can also enable an advanced informagtion gaterihing script to determine, what an external webserver can find out about you. The advanced IG scripts are enabled within the campaign scenario settings:

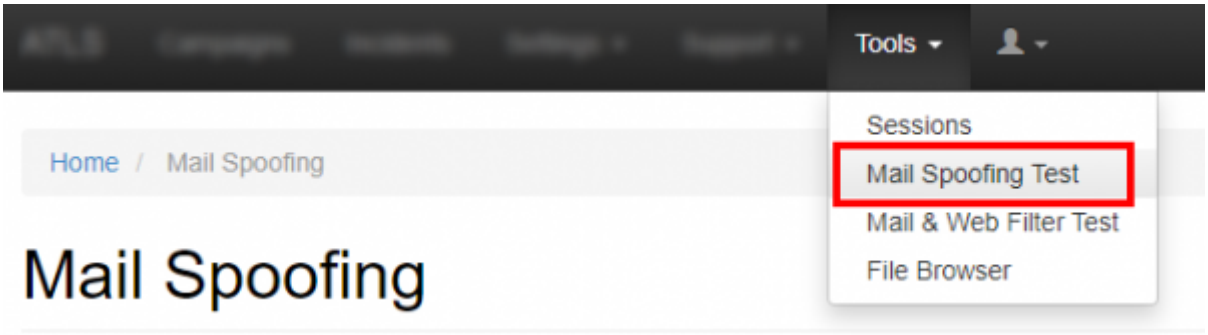


The results are under the campaign statistics (recipients):



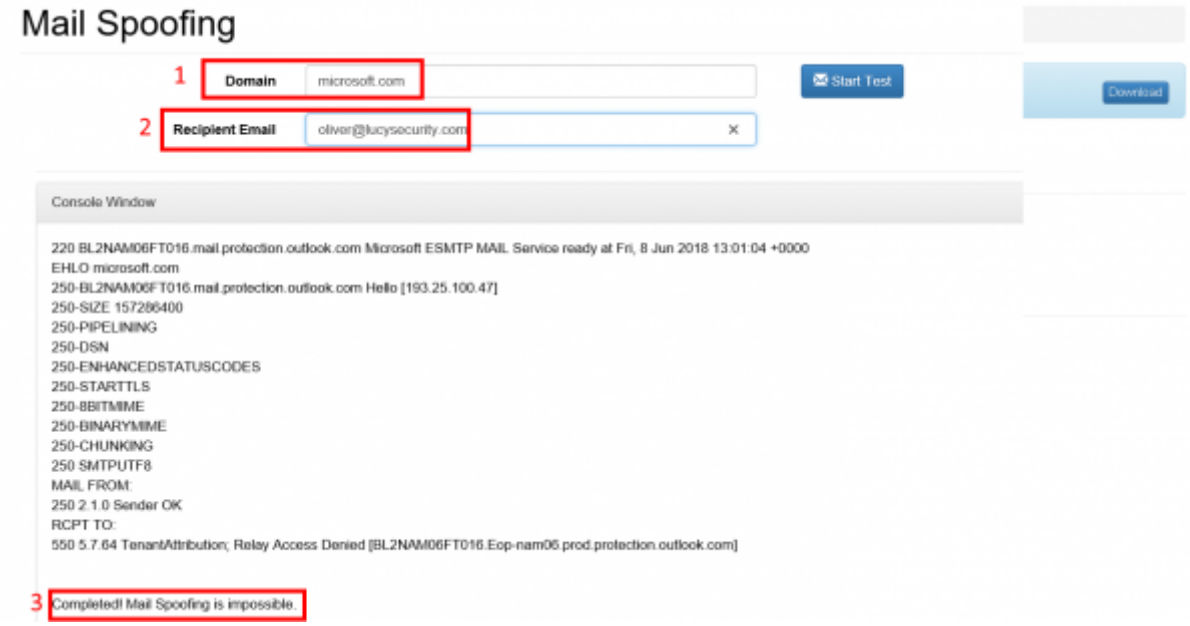
Spoofing Test

The spoofing test will verify, if an anonymous user from the internet can send a spoofed email on behalf of another domain. The test can be found under "tools":



Procedure:

1. Step 1: Enter the domain you are trying to spoof
2. Step 2: Enter a mail recipient, where the spoofed email should get sent to
3. Step 3: After a short time you will see if the pssoing test worked



From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=technical_tests_without_involving_employees&rev=1564051797

Last update: **2019/07/25 12:49**