Background Info

Not only does the popular perimeter-based approach to security provide little risk reduction today; it is, in fact, contributing to the increased attack surface criminals are using to launch potentially devastating attacks. In general, the perimeter-based approach assumes two types of agents: insiders and outsiders. The outsiders are considered to be untrusted while the insiders are assumed to be extremely trustworthy. This type of approach promotes the development of architectures where networks are clearly broken into delineated “trusted” zones and “untrusted” zones. The obvious flaw with the perimeter approach is that all the insiders — that is the employees of a business — are assumed to be fully trustworthy.

With LUCY, we are now able to expose how the emerging breed of attackers are able to leverage application and browser flaws to launch “inside-out” attacks, allowing them to assume the role of the trusted insider; a type of attack used in the "1 Billion Dollar Heist" (see page 9 https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf). Traversing the corporate firewall to attack an internal application may seem like an impossible task, but attackers have the advantage of knowing that most corporate firewalls make an exception to web traffic (http & https). Although an attacker cannot force HTTP content through the firewall, the attacker can execute code that he/she controls behind an organization's perimeter if an employee "invites" it in. This invitation might come in a phishing mail, asking the victim to download and execute some file. Once executed, the browser of the client can be hijacked and used to establish an open communications channel to the attacker. You can imagine it like this: the Malware tells the victim's browser to connect back to a webserver that belongs to the attacker. But instead of displaying a website, the attacker makes sure that the connection to that website stays open - invisible to the user. Having control over the website, the attacker is now able to send back commands to that victim in that already established web connection. This is called interactive sessions. Using this feature with LUCY, we can now simulate such attacks. But who needs such advanced hacker techniques? Well, for example, security companies performing penetration tests with their clients. But also any organization, who wants to test, if such hidden communication channels are possible within their infrastructure. Since LUCY is simulating the attack from A-Z (creating the Malware simulation, creating the website, sending the email with the Malware sample, establishing the reverse http channels, etc.) you don’t need to have in-depth IT security skills anymore to verify the exposure against such attacks.

About the Tool

The tool is called "ConsoleInteractive" in LUCY. It allows you to establish a reverse HTTP/HTTPS channel to LUCY and execute commands within the admin web GUI. Those commands are pulled from the LUCY Malware simulation and are then executed. The results then are visible in the admin GUI: once the file has been executed, you can see the session in “Sessions”.

Differences to MSF

LUCY is mainly a tool that simulates social hacks with a big variety in attack templates. Those predefined attack templates can be combined with actual malware simulations, which makes LUCY among many other attack toolkits unique.

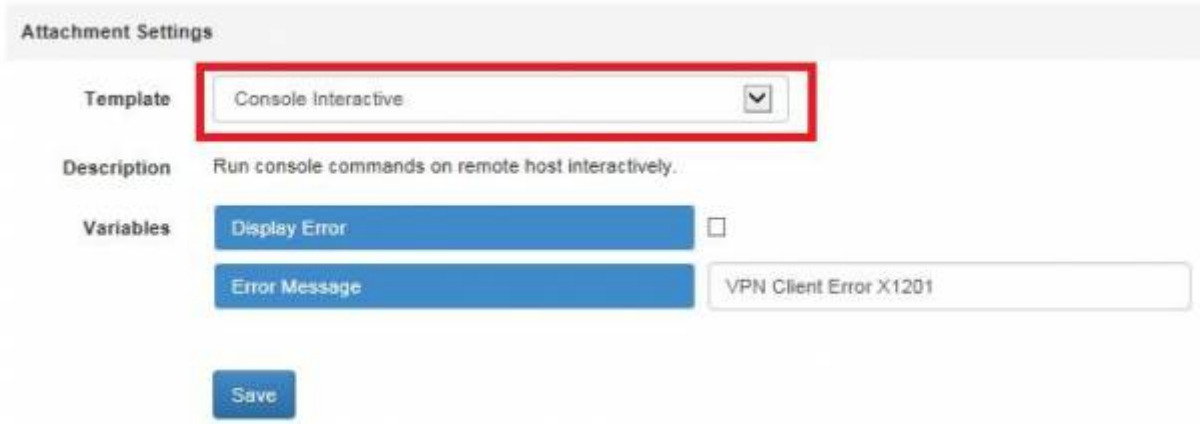
Security Concerns

The Tool only runs in the memory (called “file” in Process View). After the termination, the session cannot be established again. You can click on the IP and start executing commands in the Windows shell. The output should appear after a few seconds automatically. Also, this Tool only works with Windows 7/8/10 in combination with Internet Explorer, Firefox, Microsoft Edge and Chrome.

Configuration

To be able to perform an interactive attack, the user needs to download and execute the file that LUCY creates during the campaign. On the user's side, the file requires no installation (it runs as a portable executable) and needs only standard Windows user rights.

You can either choose to send the attachment via Email (use the network activity report) or create a download page (e.g. select the VPN Download scenario). The specific Malware Simulation Settings can then be edited either within the landing page template or the email template. To perform an attack with the interactive shell, please select "Console Interactive" as the tool.

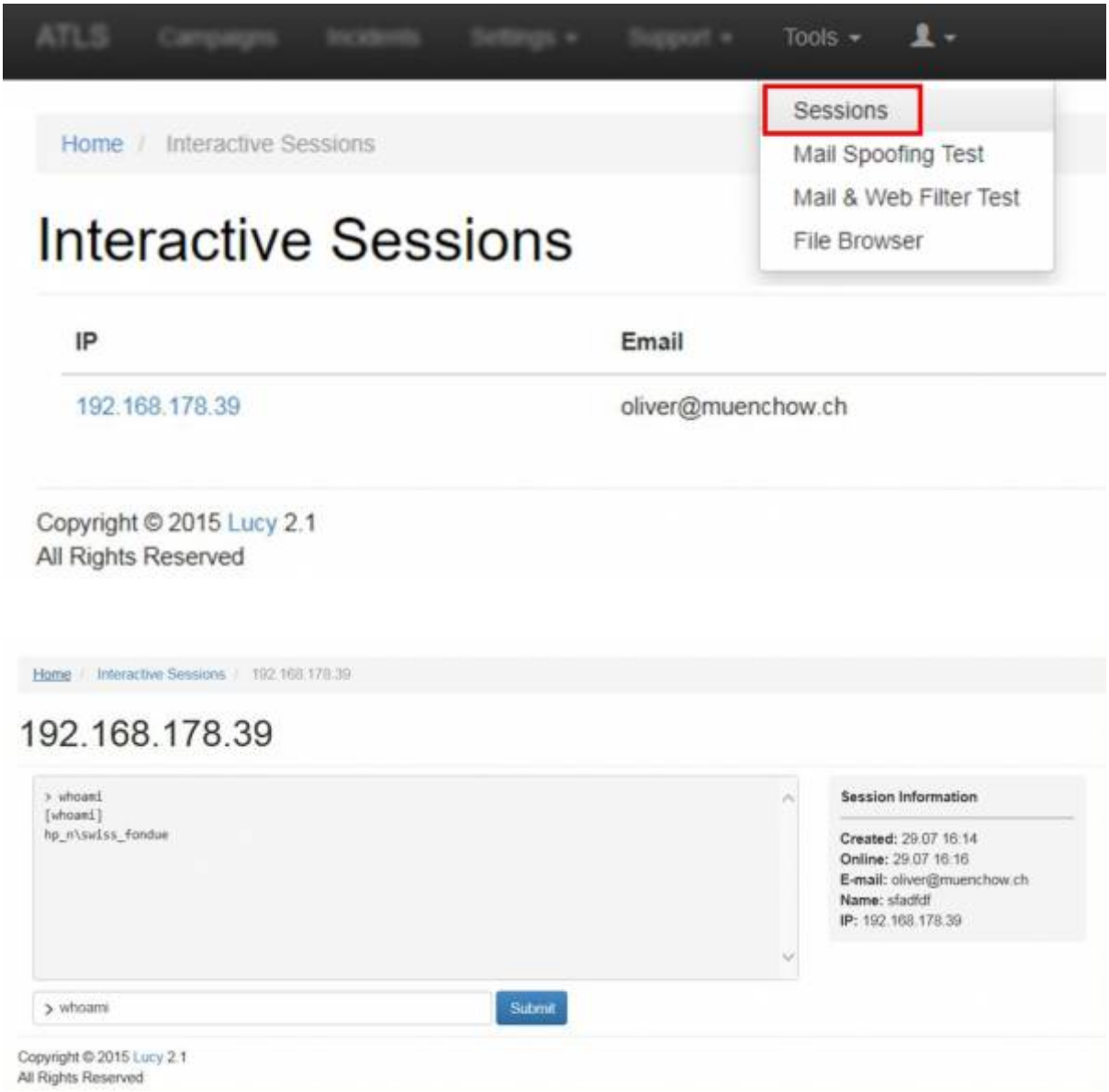


If you only want the executable to be provided as a download link and not an email attachment, simply select the "Console Interactive" in the web landing page as a file template. If you want the file also to be sent via email, select the "Console Interactive" in the email settings as a file template.

If you don't choose to select to show a custom error upon execution, then the file runs silently in the memory. Otherwise, a popup will appear when the user executes the file.

Where to type in your commands?

All interactive sessions can be configured in the Top Navigation Menu under "Interactive Sessions". You will have the ability to select the user first, and then start your interactive session.



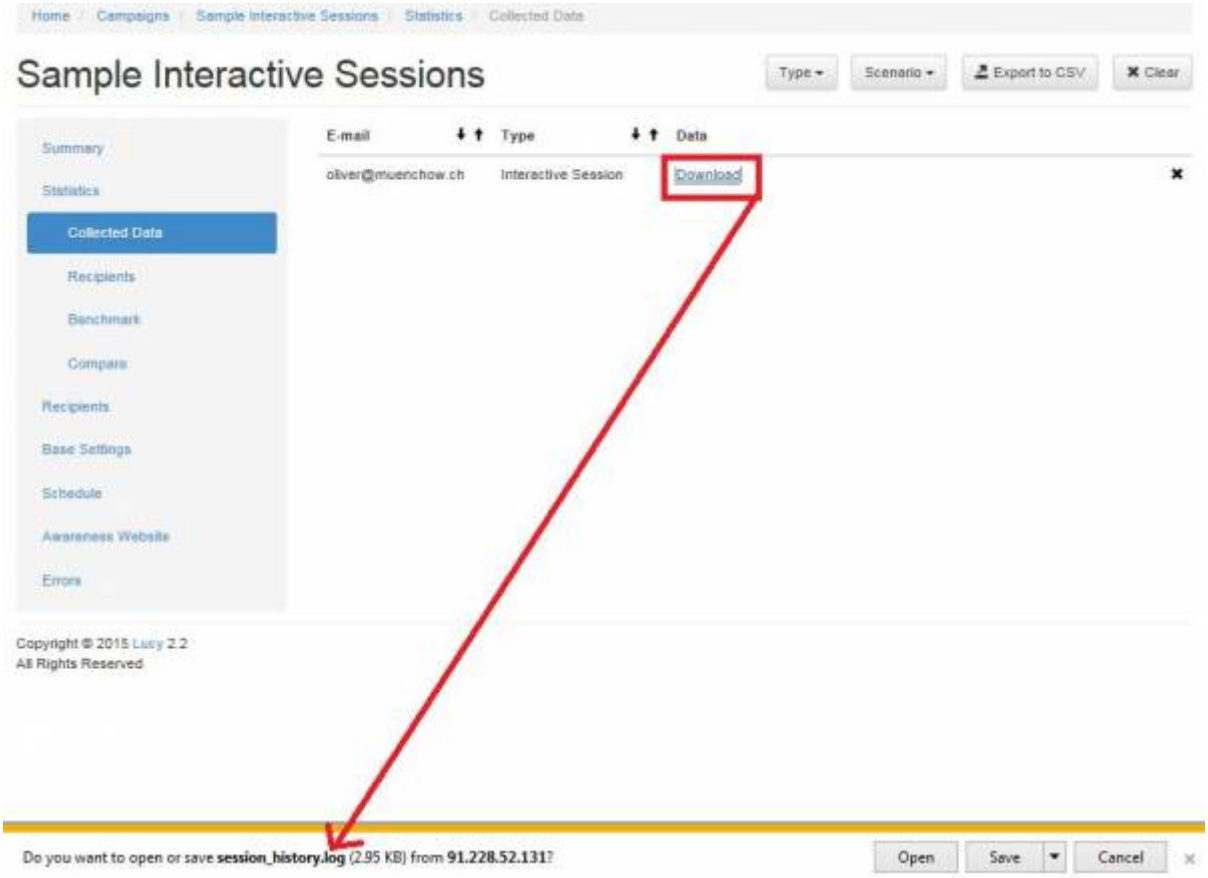
What commands are supported?

The tool allows you to use a limited set of commands. Some commands in Windows are not executable, they are built into the command line (Example of command with executable: whoami). If we need to use a command which is a built-in command line, then we should call it directly. Here are a few more examples of how to run shell commands:

- dir
- cd C:\ & dir
- type C:\autoexec.bat
- dir "C:\Program Files\

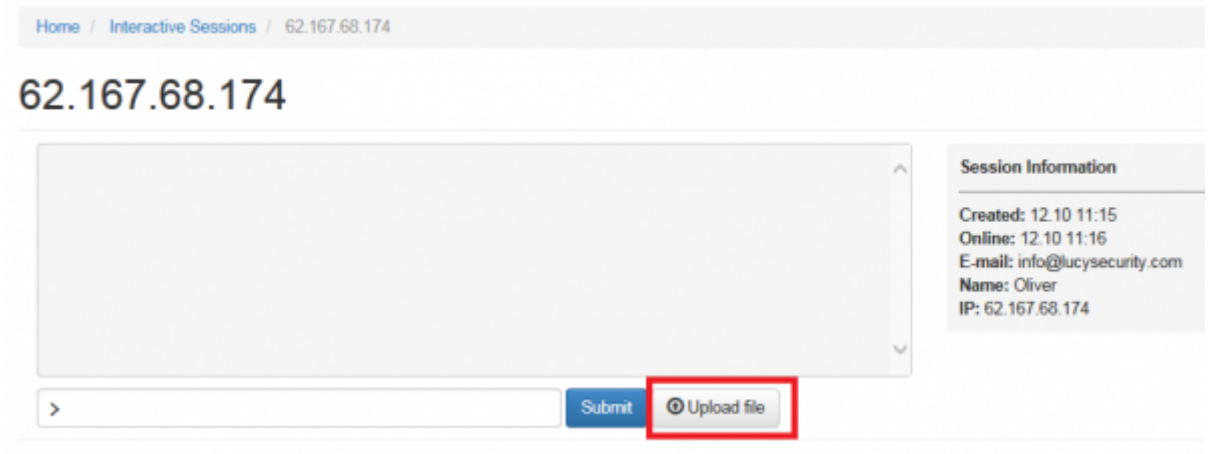
Where to download the session logs?

All raw session logs can be downloaded under Statistics/Collected data.



Can I upload my custom payload to the client?

Within a session, you can upload your own custom payload to the victim's PC. Please use the upload form field. LUCY will convert your binary file into a BASE64 string which the client will fetch and decode and then execute.



Video

Watch this video here to see the interactive shell configuration in a live example:
https://www.youtube.com/watch?v=mSA8jMXYIJU