**HACK LIKE A PRO**

How to Use Maltego to Do Network Reconnaissance

BY OCCUPYTHEWEB

11/11/2014 1:56 AM

RECON

MALTEGO

Welcome back, my greenhorn hackers!

Before we attempt to exploit any target, it is wise to do proper [reconnaissance](#). Without doing reconnaissance, you will likely be wasting your time and energy as well as risking your freedom. In previous guides, I have demonstrated multiple ways to perform reconnaissance including passive recon with [Netcraft](#), active recon with [Nmap](#) or [hping3](#), recon by exploiting [DNS](#) or [SNMP](#), and [many others](#).

In this tutorial, we will be using an active tool called [Maltego](#), developed by [Paterva](#), that can do many of these tasks with one simple scan. There is a community edition built into our [Kali Linux](#) that allows us 12 scans without purchasing Maltego. It is capable of a significant amount of information gathering about a prospective target in a single sweep of the domain.

Using Maltego in Kali to Recon a Target Network

Maltego is capable of gathering information about either a network or an individual; here we will focus on the former and leave individual information gathering for another time. We will be looking at gathering info on all the subdomains, the IP address range, the WHOIS info, all of the email addresses, and the relationship between the target domain and others.

Step 1

Open Maltego & Register

Let's start by firing up Kali and then opening Maltego. Maltego can be found in numerous places in Kali, but the easiest way to get to it is to go to Applications -> Kali Linux -> Top 10 Security Tools. Then, among the Top 10, you will find Maltego at number 5, as shown in the screenshot below.



When you open Maltego, you will need to wait a brief moment for it to startup. After it finishes loading, you will be greeted by a screen asking you to register Maltego.

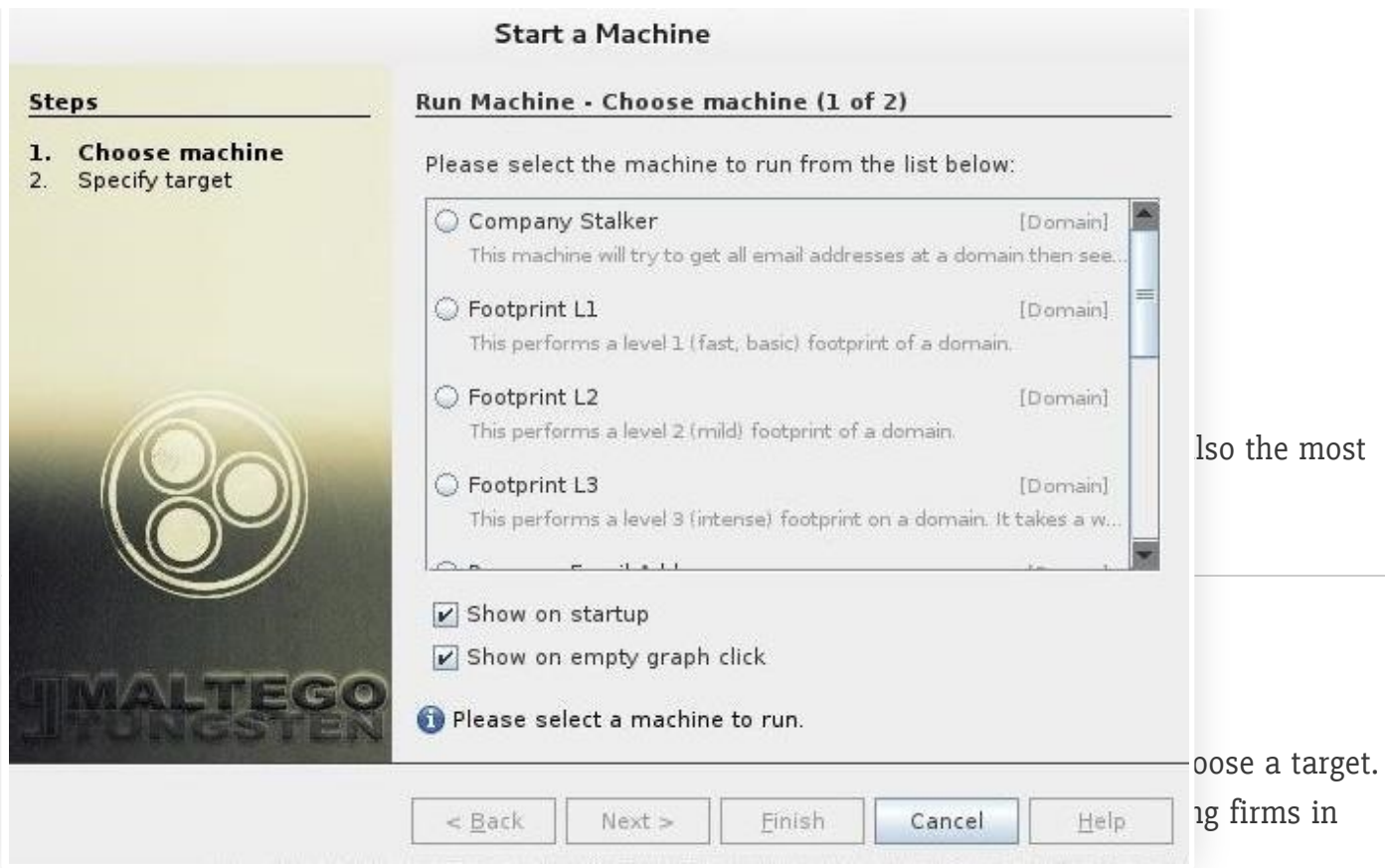


ain the next

Choose a Machine & Parameters

After successfully registering and logging into Maltego, we will have to decide what type of "machine" we want to run against our target. In Maltego's parlance, a machine is simply what type of footprinting we want to do against our target. Here, we are focusing on the network footprinting, so our choices are:

- **Company Stalker** (this gathers email information)
- **Footprint L1** (basic information gathering)
- **Footprint L2** (moderate amount of information gathering)
- **Footprint L3** (intense and the most complete information gathering)



Start a Machine

Steps

1. **Choose machine**
2. **Specify target**

Run Machine - Choose machine (1 of 2)

Please select the machine to run from the list below:

- ☐ **Company Stalker** [Domain]
This machine will try to get all email addresses at a domain then see...
- ☐ **Footprint L1** [Domain]
This performs a level 1 (fast, basic) footprint of a domain.
- ☐ **Footprint L2** [Domain]
This performs a level 2 (mild) footprint of a domain.
- ☐ **Footprint L3** [Domain]
This performs a level 3 (intense) footprint on a domain. It takes a w...

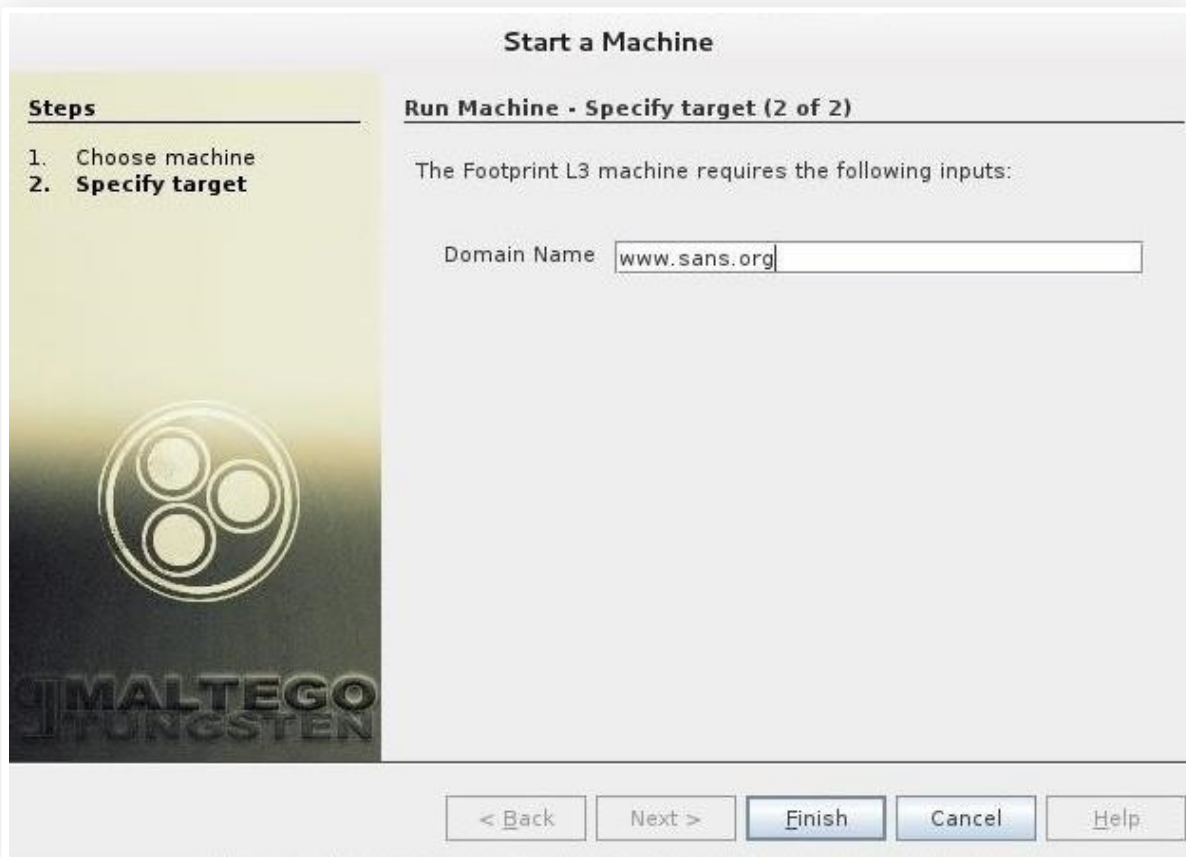
☒ Show on startup
☒ Show on empty graph click

i Please select a machine to run.

< Back Next > Finish Cancel Help

Also the most

Choose a target.
ing firms in



Start a Machine

Steps

1. **Choose machine**
2. **Specify target**

Run Machine - Specify target (2 of 2)

The Footprint L3 machine requires the following inputs:

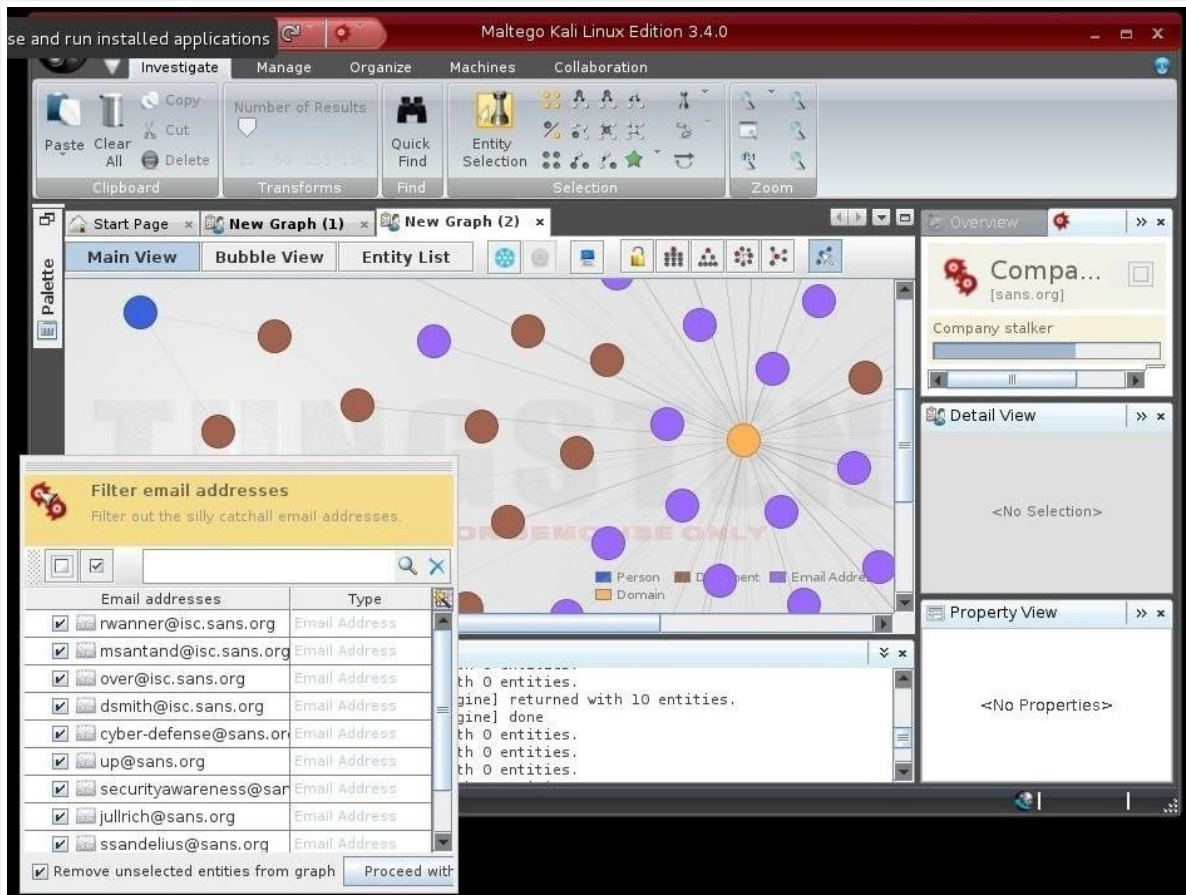
Domain Name

< Back Next > Finish Cancel Help

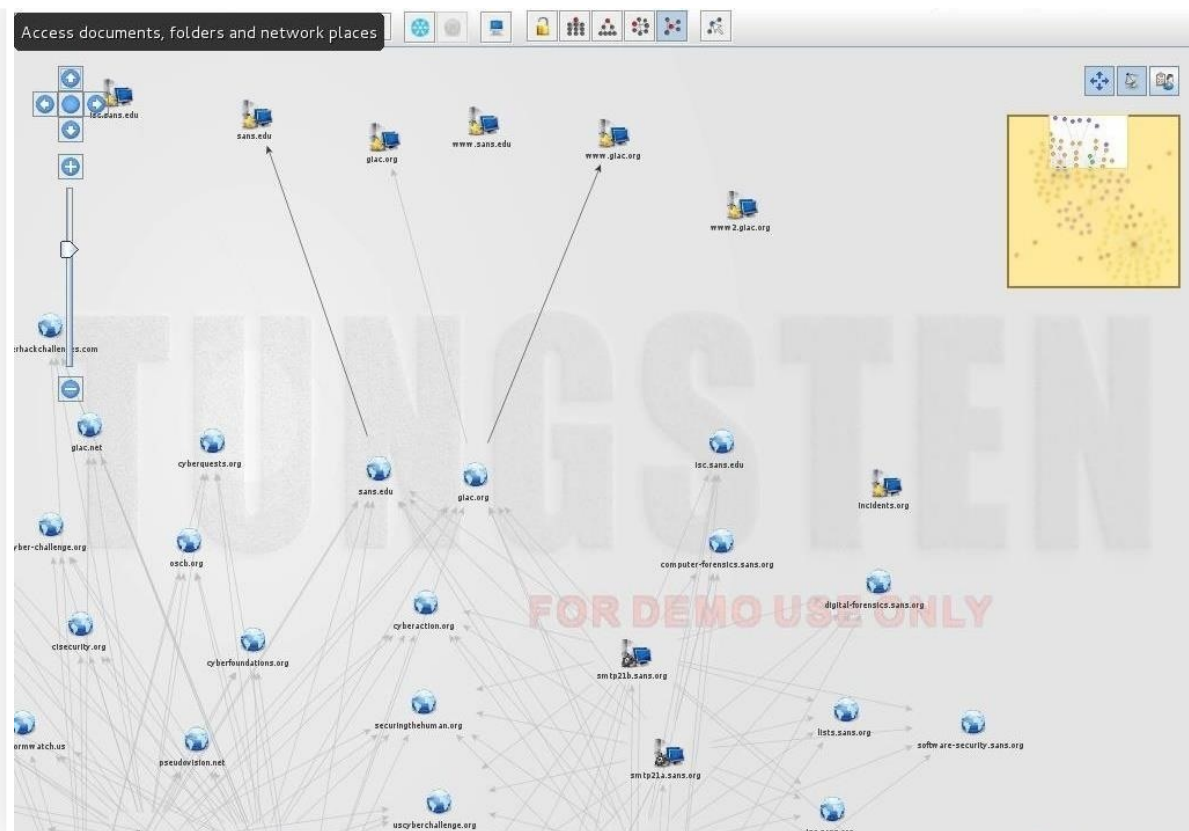
Now, click "Finish" and let Maltego do its work.

Results

Maltego will now begin to gather info on our target domain, sans.org, and display it on screen. In the screenshot below, we can see that Maltego has already collected the email addresses from the site, while it collects the nameservers and mail servers.



Finally, we can click on "Bubble View" when Maltego is done and see all of the relationships between our target and its subdomains and linked sites.



to do
of doing
ackers.

Never Miss a Hacking or Security Guide

New Null Byte in your inbox, every week.

✉ GET THE NEWSLETTER

[WonderHowTo.com](#) [About Us](#) [Privacy Policy](#) [Terms of Use](#)

Don't Miss:

New iOS 13 Features — The 200+ Best, Hidden & Most Exciting New Changes for iPhone
 13 Apple Maps Features & Changes in iOS 13 You Need to Know About
 15 Awesome 'Reminders' Features in iOS 13 That'll Make You Actually Want to Use the App
 The Best New Siri Features & Commands in iOS 13 for iPhone
 Memoji Stickers, Improved Search & More New Apple Messages Features in iOS 13 for iPhone
 20+ Features in iOS 13's Safari You Don't Want to Miss

iOS 13's Notes App Is Packing 15 Cool New Features & Changes

31 New Features for Camera & Photos in iOS 13