**Task 1 - OSINT**

**מגישים:**

דוד סיידון

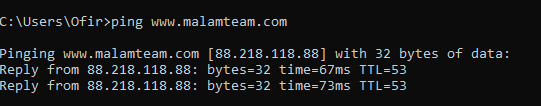
אופיר גן

**Section 1** - Information Gathering:

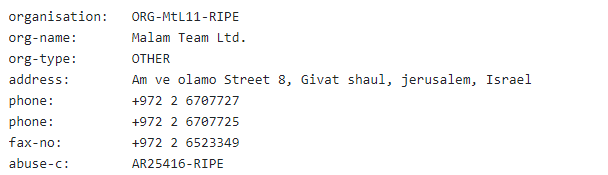
In this exercise, we collected information on MalamTeam.

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding** | **Source** | **Reconnaissance** | **ID** |
| We found the IP of MalamTeam Website | Ping Command | Passive | 1 |
| We found info about MalamTeam Website/Domain/Phone.. | WhoIs Command | Passive | 2 |
| We found Physical location, Phone, Email, net Worth | Look In The Web | Passive | 3 |
| We can seek a job interview in MalamTeam job section site and by that we can get a valid information from the interviewer | Malam job interview | Semi-Passive | 4 |
| Conferences Event Dates, Clients | Malam Team Site | Semi-Passive | 5 |
| Applications Used by the company | Maltego | Passive | 6 |
| Current Employees | LinkedIn | Semi-Passive | 7 |

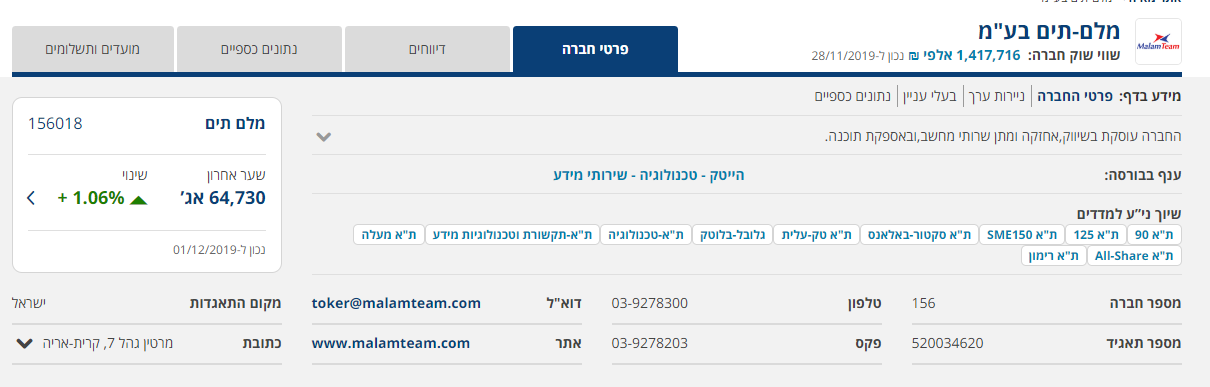
**1. Ping**

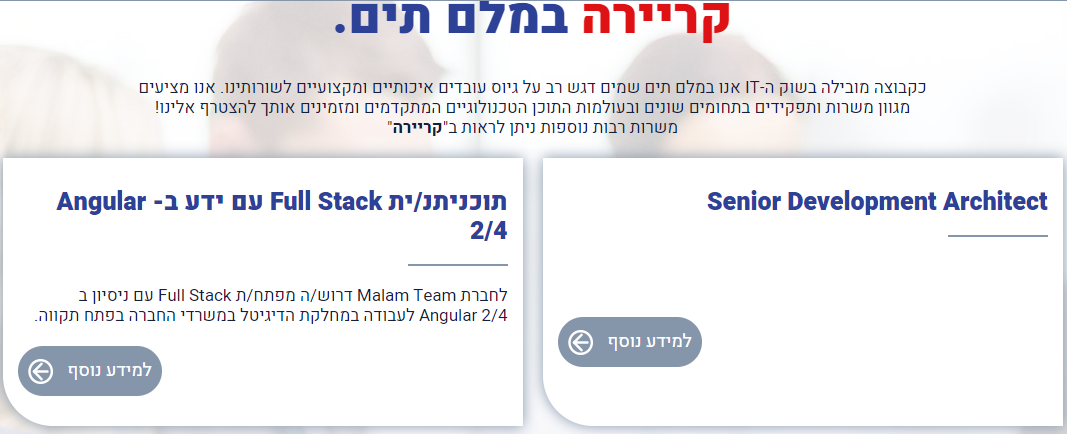
****

**2. WhoIs**

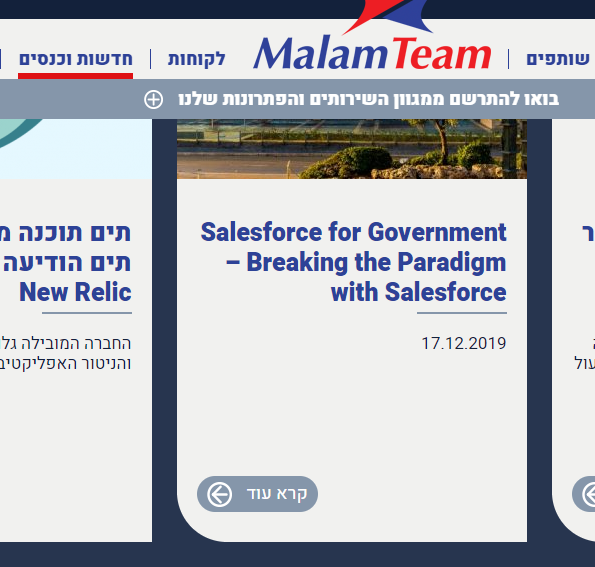
****

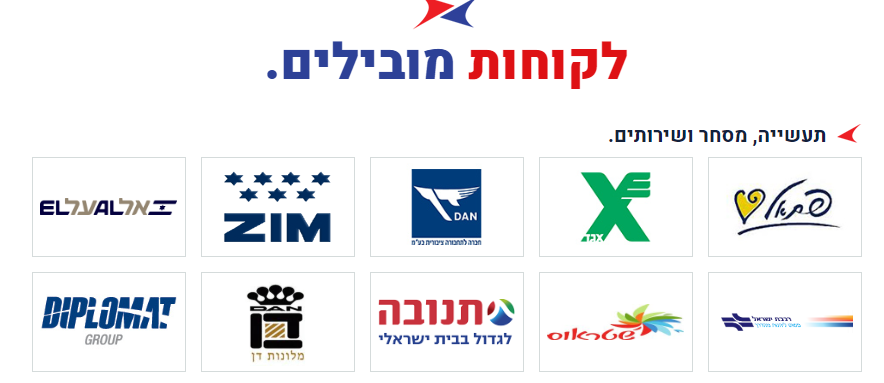
**3. Web Search:**

****

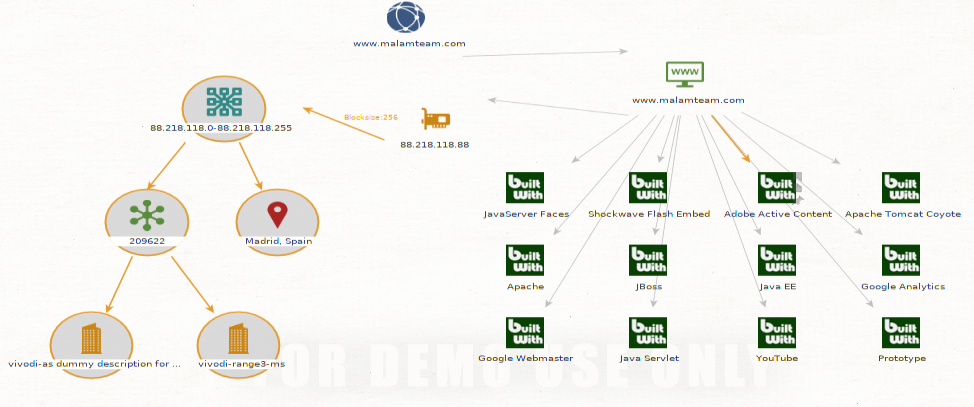
**4. Open Job Positions**

**3. Malam Website:**

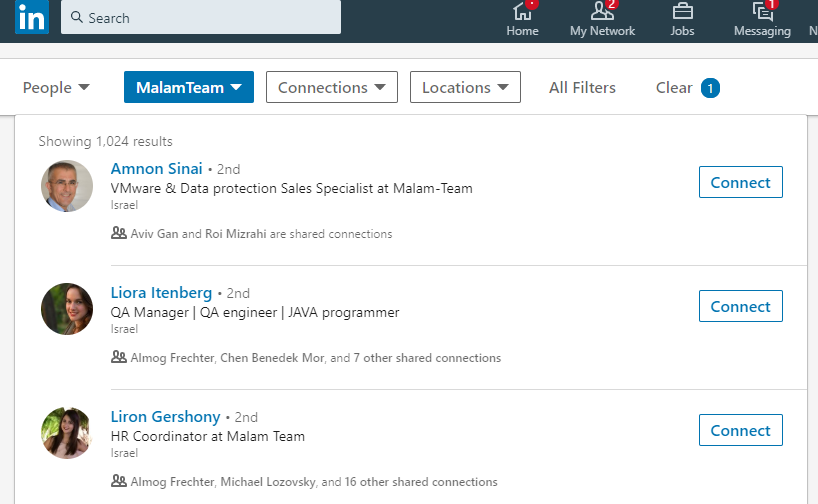
****

****

**6. Maltego**

****

**7. LinkedIn**

****

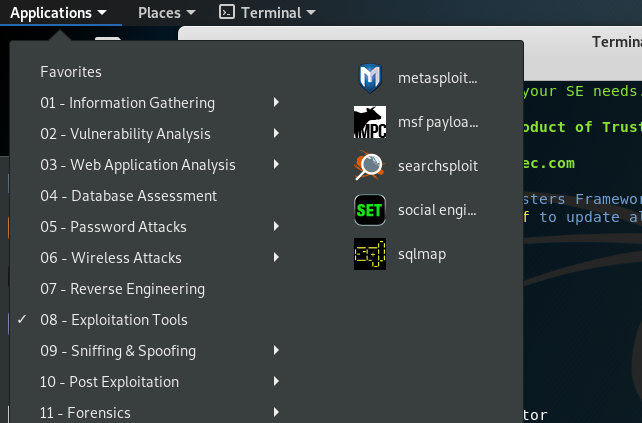
**Section 2** - Social engineering:

We succeed hacking to Facebook accounts with Kali Linux tool thought cloning.

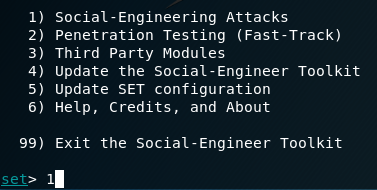
Note: Gmail has double authentication (one page leads to another), therefore the Gmail cloning was didn’t work correctly.

The hacking was by these following steps:

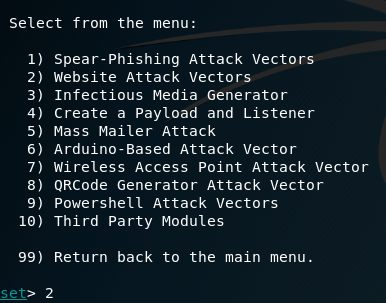
1.We used tool called setoolkit.



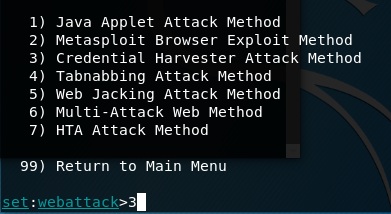
2. We proceeded to Social-Engineering attacks for the attacking option.



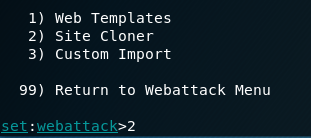
3. We then go to website attack vector.



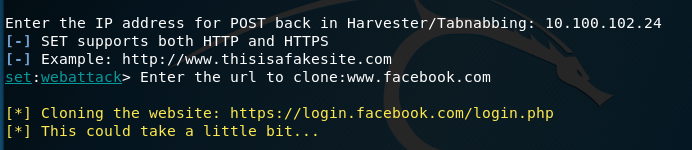
3. We choose the credential harvester attack method.



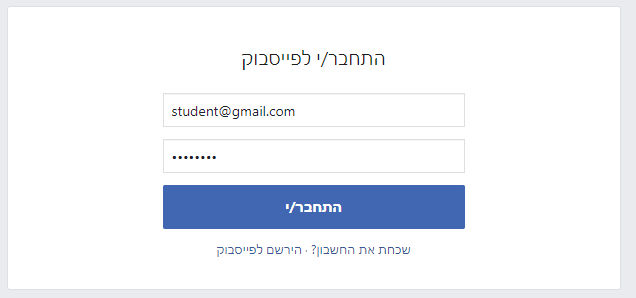
4. Now we select the Site Cloner option.



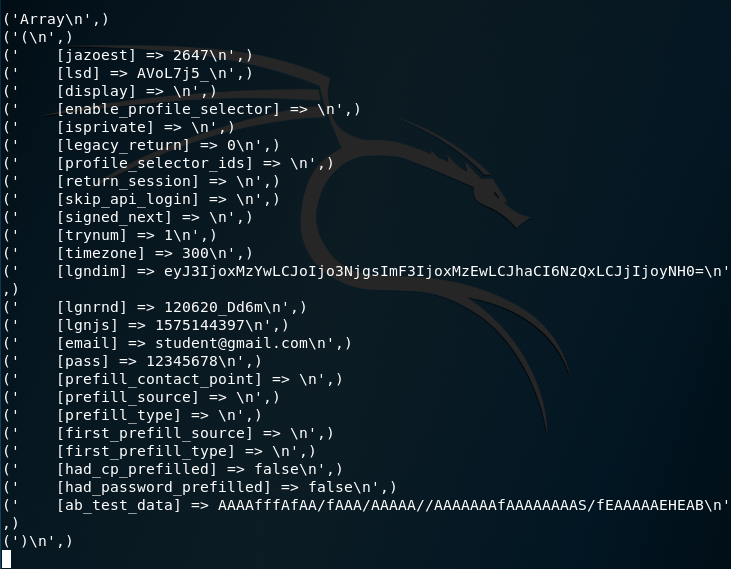
5. We enter the IP address of the machine we want to hack and the site we want to clone.



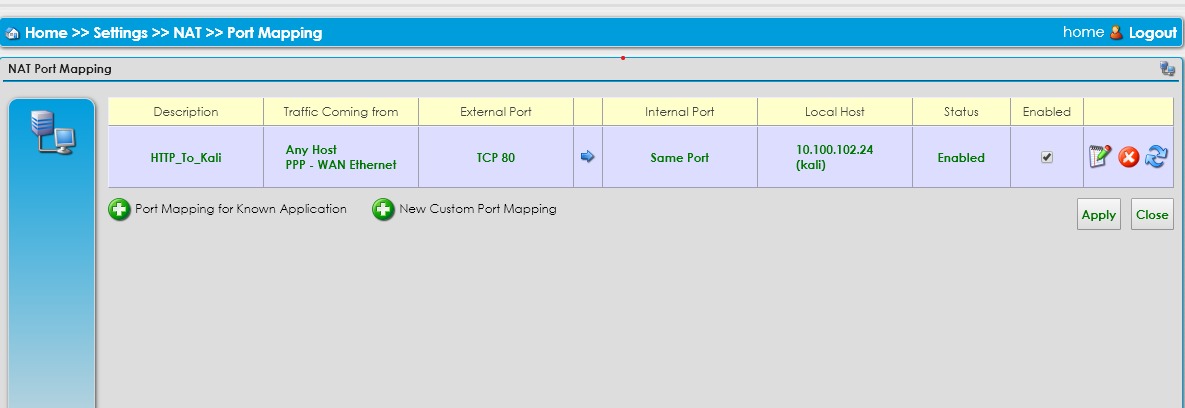
6. The victim enters his user name and password to the fake Facebook login site.



7. Now we have his information to log in to his account.



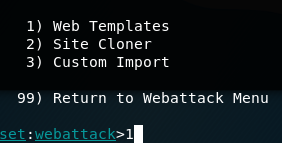
Noted that for the procedure to work behind NAT (to make our site available for everyone connected to the internet) we forwarded all packets received with destination port 80 & destination IP with our public IP to the local IP of the kali VM .

add NAT Port Mapping in the home router/switch/NAT

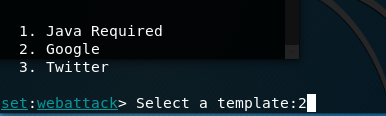
8. we have two suggestions for phishing Gmail Account:

**First Method:** Using Template

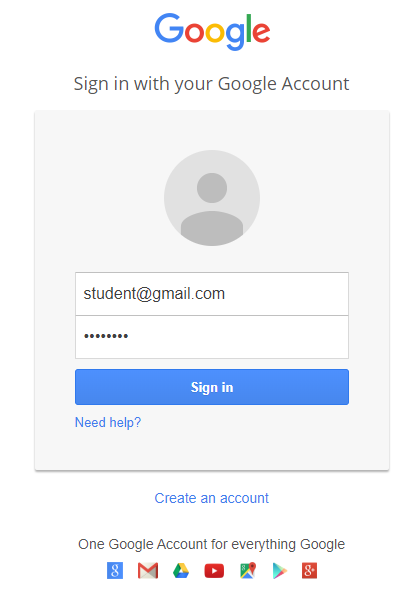
We repeat the procedure for a Gmail account hack.



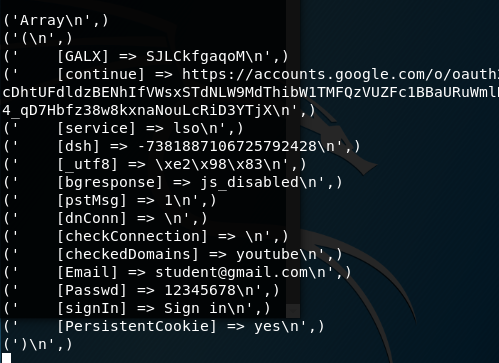
9. We choose the google option.



10. The victim enters his log in information to the fake Gmail login account

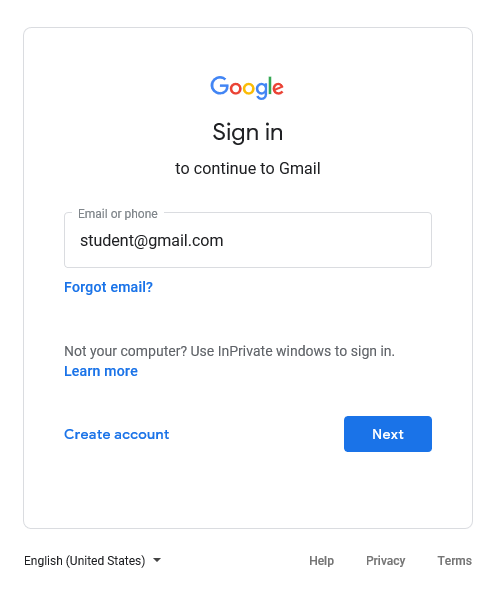
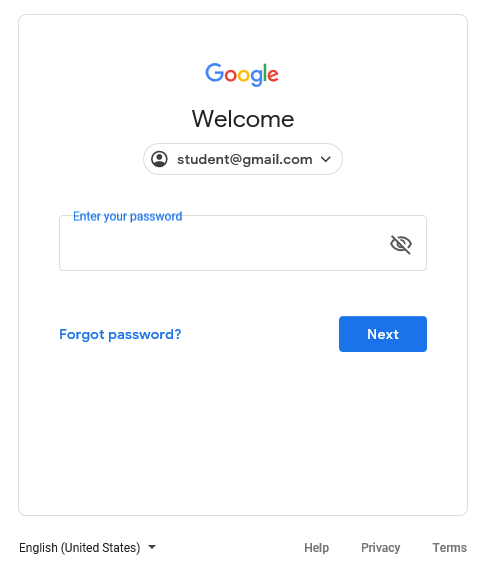


9. Now we have his Gmail log in information.



**Second Method:** use double authentication phishing,

clone the two pages of google login and redirect the victim from the first page to the second and from that to the original site.



Real Victim Gmail