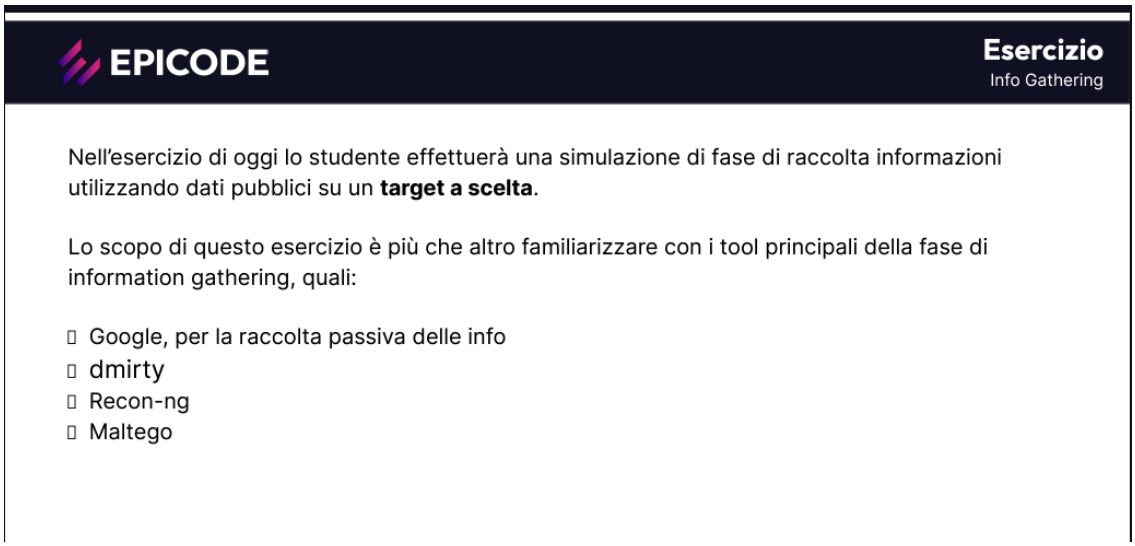
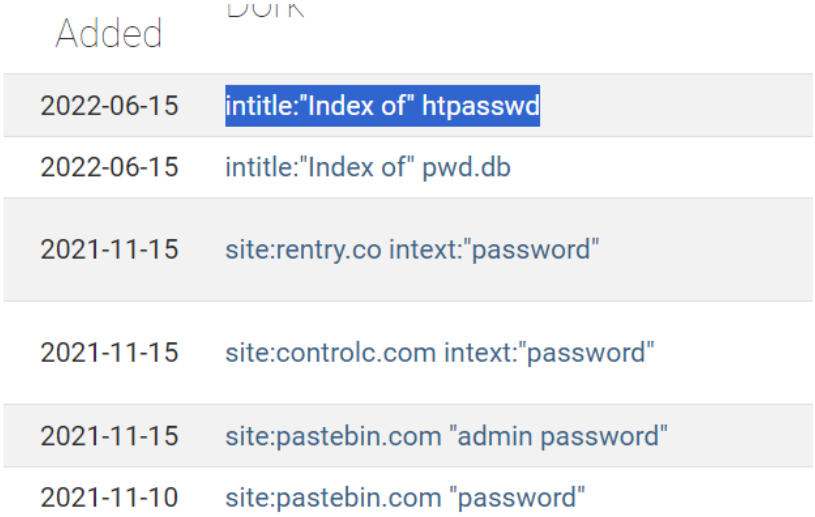
ESERCITAZIONE WEEK 10 DAY 3



1. **Google Hacking DB**

Per allenamento sono state anaizzate le seguenti dork:



2. **Dmirty**

Comando	Risultati
dmitry -i epicode.com	Deepmagic Information Gathering Tool "There be some deep magic going on" HostIP:35.207.141.200 HostName:epicode.com Gathered Inet-whois information for 35.207.141.200 --- inetnum: 32.0.0.0 - 36.255.91.255 netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK descr: IPv4 address block not managed by the RIPE NCC

	remarks: ---------- remarks: remarks: For registration information, remarks: you can consult the following sources: remarks: remarks: IANA remarks: http://www.iana.org/assignments/ipv4-address-space remarks: http://www.iana.org/assignments/iana-ipv4-special-registry remarks: http://www.iana.org/assignments/ipv4-recovered-address-space remarks: remarks: AFRINIC (Africa) remarks: http://www.afrinic.net/ whois.afrinic.net remarks: remarks: APNIC (Asia Pacific) remarks: http://www.apnic.net/ whois.apnic.net remarks: remarks: ARIN (Northern America) remarks: http://www.arin.net/ whois.arin.net remarks: remarks: LACNIC (Latin America and the Carribean) remarks: http://www.lacnic.net/ whois.lacnic.net remarks: remarks: ---------- country: EU # Country is really world wide admin-c: IANA1-RIPE tech-c: IANA1-RIPE status: ALLOCATED UNSPECIFIED mnt-by: RIPE-NCC-HM-MNT created: 2019-04-16T15:48:11Z last-modified: 2019-04-16T15:48:11Z source: RIPE role: Internet Assigned Numbers Authority address: see http://www.iana.org. admin-c: IANA1-RIPE tech-c: IANA1-RIPE nic-hdl: IANA1-RIPE remarks: For more information on IANA services remarks: go to IANA web site at http://www.iana.org. mnt-by: RIPE-NCC-MNT created: 1970-01-01T00:00:00Z last-modified: 2001-09-22T09:31:27Z source: RIPE # Filtered % This query was served by the RIPE Database Query Service version 1.109.1 (ABERDEEN) All scans completed, exiting

dmitry -w epicode.com	Deepmagic Information Gathering Tool "There be some deep magic going on" HostIP:35.207.141.200 HostName:epicode.com Gathered Inic-whois information for epicode.com --- Domain Name: EPICODE.COM Registry Domain ID: 26700881_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.godaddy.com Registrar URL: http://www.godaddy.com Updated Date: 2023-05-13T05:04:09Z Creation Date: 2000-05-09T18:57:38Z Registry Expiry Date: 2031-05-09T18:57:38Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: 480-624-2505 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Name Server: NS-1492.AWSDNS-58.ORG Name Server: NS-1580.AWSDNS-05.CO.UK Name Server: NS-198.AWSDNS-24.COM Name Server: NS-953.AWSDNS-55.NET DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of whois database: 2024-01-13T14:08:48Z <<< For more information on Whois status codes, please visit https://icann.org/epp NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration. TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or

	modify existing registrations; the Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time. The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars. All scans completed, exiting

dmitry -e epicode.com	Deepmagic Information Gathering Tool "There be some deep magic going on" HostIP:35.207.141.200 HostName:epicode.com Gathered E-Mail information for epicode.com --- Searching Google.com:80... Searching Altavista.com:80... Found 0 E-Mail(s) for host epicode.com, Searched 0 pages containing 0 results All scans completed, exiting
dmitry -s epicode.com	Deepmagic Information Gathering Tool "There be some deep magic going on" HostIP:35.207.141.200 HostName:epicode.com Gathered Subdomain information for epicode.com --- Searching Google.com:80... Searching Altavista.com:80... Found 0 possible subdomain(s) for host epicode.com, Searched 0 pages containing 0 results All scans completed, exiting
dmitry -n epicode.com	Deepmagic Information Gathering Tool "There be some deep magic going on" HostIP:35.207.141.200 HostName:epicode.com Gathered Netcraft information for epicode.com --- Retrieving Netcraft.com information for epicode.com Netcraft.com Information gathered All scans completed, exiting

3. <u>Recon-ng</u>

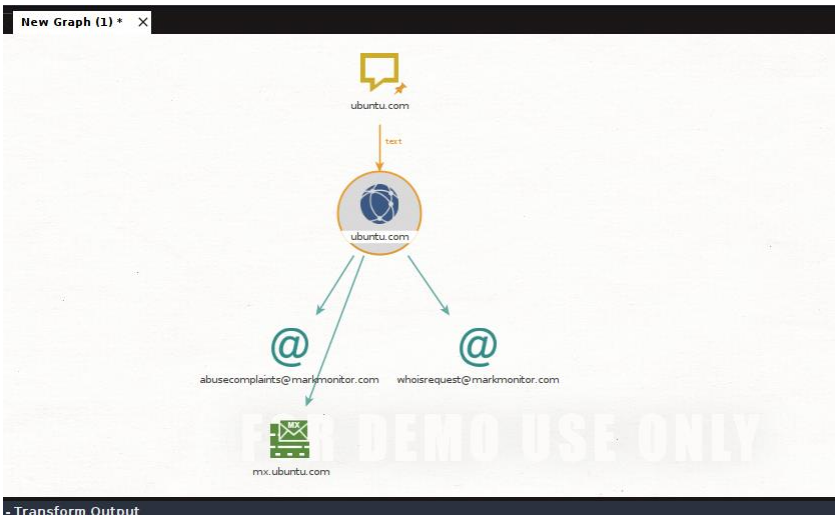
Comando	Risultati
Modules load recon/domains-contacts/whois_pocs options set source google.com run	GOOGLE.COM --- [*] URL: http://whois.arin.net/rest/pocs;domain=google.com [*] URL: http://whois.arin.net/rest/poc/CREEK14-ARIN [*] Country: United States [*] Email: alexcreek@google.com [*] First_Name: Alex [*] Last_Name: Creek [*] Middle_Name: None [*] Notes: None

	[*] Phone: None [*] Region: Reston, VA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/ABA104-ARIN [*] Country: United States [*] Email: ari@google.com [*] First_Name: Ari [*] Last_Name: Barkan [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Mountain View, CA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/ABA105-ARIN [*] Country: United States [*] Email: ari@google.com [*] First_Name: Ari [*] Last_Name: Barkan [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Mountain View, CA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/ZG39-ARIN [*] Country: United States [*] Email: arin-contact@google.com [*] First_Name: None [*] Last_Name: Google LLC [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Mountain View, CA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/ALS11-ARIN [*] Country: Switzerland [*] Email: arturolev@google.com [*] First_Name: Arturo [*] Last_Name: Servin [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Zurich [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/BROWN545-ARIN [*] Country: United States [*] Email: brownlow@google.com [*] First_Name: Tom [*] Last_Name: Brownlow [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: San Francisco, CA

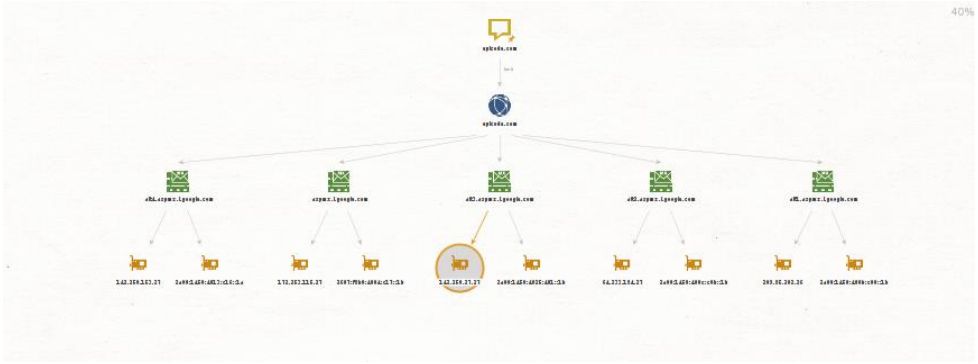
	[*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/CJC43-ARIN [*] Country: United States [*] Email: cjac@google.com [*] First_Name: Carl [*] Last_Name: Collier [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Seattle, WA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/CJC44-ARIN [*] Country: United States [*] Email: cjac@google.com [*] First_Name: Carl [*] Last_Name: Collier [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Seattle, WA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/SCHWA252-ARIN [*] Country: United States [*] Email: daveschwartz@google.com [*] First_Name: Dave [*] Last_Name: Schwartz [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Mountain View, CA [*] Title: Whois contact [*] ---------- [*] URL: http://whois.arin.net/rest/poc/SCHWA253-ARIN [*] Country: United States [*] Email: daveschwartz@google.com [*] First_Name: Dave [*] Last_Name: Schwartz [*] Middle_Name: None [*] Notes: None [*] Phone: None [*] Region: Mountain View, CA [*] Title: Whois contact [*] ---------- [*] URL:http://whois.arin.net/rest/poc/SCHWA254-ARIN ^C ------- SUMMARY ------- [*] 10 total (0 new) contacts found. [recon-ng][default][whois_pocs] >

4. Maltego

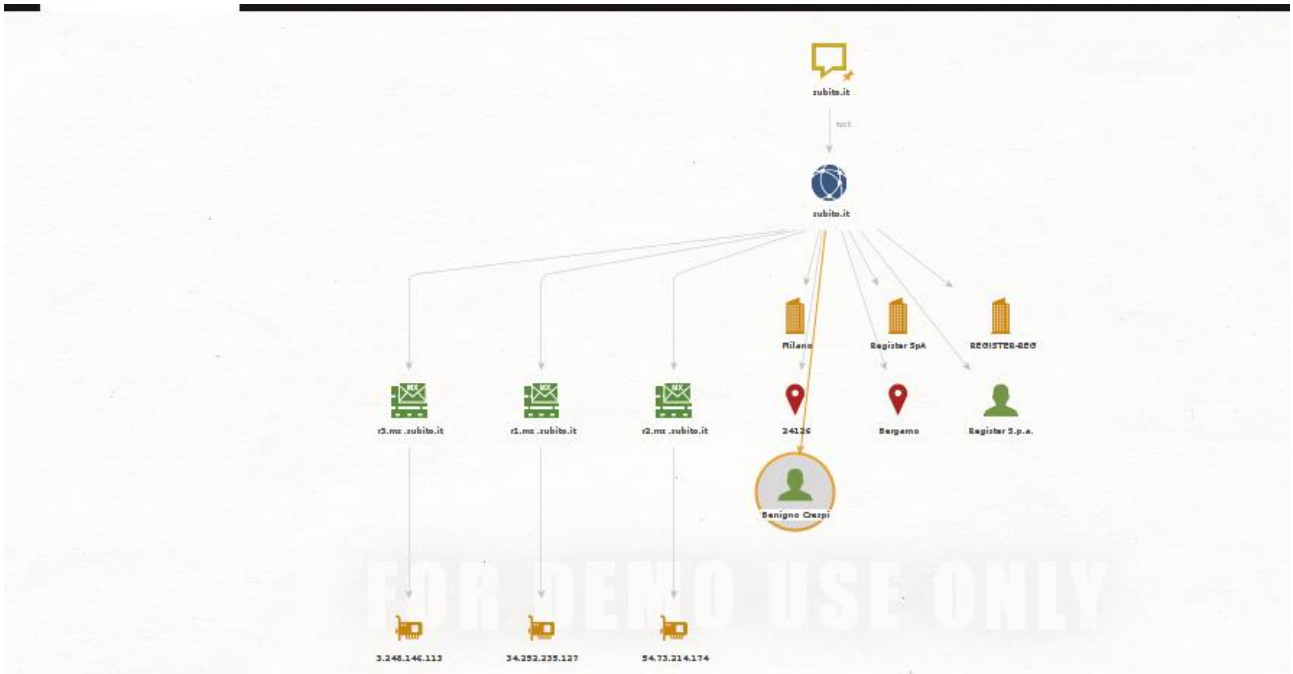
Ubuntu.com



Epicode.com



Subito.it



asroma.com