Modulo 3 esercitazione 5 – Russo Alessio

Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali:

- Google, per la raccolta passiva delle info
- dmirty
- Recon-ng
- Maltego

1: si possono trovare una serie di informazioni per il si

Per il quale è possibile accedere a file di audit e altro

Effettuando una scansione preliminare attraverso dmitry è gia possibile ottenere una serie di info interessanti. Salvo il file facendo:

dmitry -o nomefile.txt target

è possible quindi avere già una seerie di info di seguito

HostIP [redacted]
HostName [redacted]
Gathered Inet-whois information fo [redacted]
inetnum: [redacted]
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
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: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
remarks: http://www.arin.net/ whois.arin.net
remarks: LACNIC (Latin America and the Carribean)
remarks: http://www.lacnic.net/ whois.lacnic.net
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: 2023-08-14T14:48:20Z
last-modified: 2023-08-14T14:48:20Z
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 (BUSA)

Gathered Inic-whois information for jvvkukatpally.com

Domain Name: [redacted]
Registry Domain ID: [redacted]
Registrar WHOIS Server: whois.wildwestdomains.com
Registrar URL: http://www.wildwestdomains.com
Updated Date: 2023-08-20T20:30:25Z

Creation Date: 2016-08-19T09:12:43Z
Registry Expiry Date: 2024-08-19T09:12:43Z
Registrar: Wild West Domains, LLC
Registrar IANA ID: [redacted]
Registrar Abuse Contact Email: [redacted]
Registrar Abuse Contact Phon[redacted]
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 [redacted]
Name Server: NS66.[redacted]
DNSSEC: unsigned
URL of the ICANN Whois Inaccura [redacted]
>>> Last update of whois database:

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Gathered Netcraft information fo [redacted]

Retrieving Netcraft.com information for [redacted]
Netcraft.com Information gathered

Gathered Subdomain information for [redacted]

Searching [redacted]
HostName [redacted]
HostI [redacted]
Searching Altavista.com:80...
Found 1 possible subdomain(s) for host [redacted], Searched 0 pages containing 0 results

Gathered E-Mail information for [redacted]

Searching Google.com:80...
Searching Altavista.com:
Found 0 E-Mail(s) for host [redacted] Searched 0 pages containing 0 results

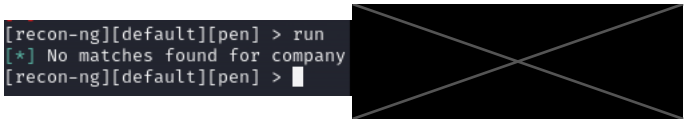
E una serie di porte con stato open

```
 Port           State

21/tcp          open
53/tcp          open
80/tcp          open
110/tcp         open
143/tcp         open

Portscan Finished: Scanned 150 ports, 143 ports were in state closed
```

Proseguiamo con l'utilizzo di alcuni tool di recon-ng

Per avviare recon in terminale digito: "recon-ng"
Per visualizzare i vari moduli disponibili: "marketplace search"
Per visualizzare info sul modulo: "marketplace info path modulo"
Per caricare il modulo scelto: "modules load path modulo"
Per settare il modulo: "option set SOURCE host.com"
Per visualizzare l'input selezionato: input
Per avviare il modulo: "run"

Primo modulo scelto: recon/companies-contacts/pen – no results.

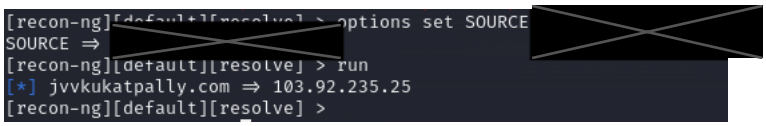


Secondo Modulo selezionato: recon/companies-domains/pen – no results

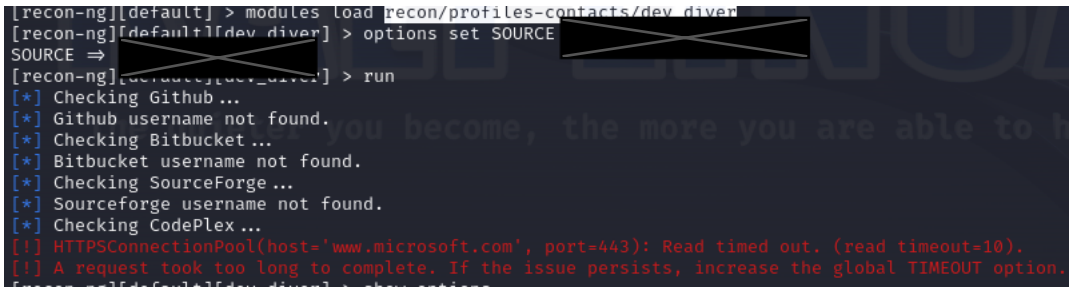
Terzo modulo selezionato: recon/domains-contacts/whois_pocs – no results

Quarto modulo selezionato: recon/domains-hosts/google_site_web – CAPTCHA triggered.

Quinto modulo selezionato: recon/hosts-hosts/resolve



Sesto modulo Selezionato: recon/profiles-contacts/dev_diver – TIMEOUT



Maltego il quale ha rilevato denne informazioni come la localizzazione, due indirizzi IP che cpomunicano sulla porta 25, non trovate vulnerabilità CVE, trovato numero di telefono.