



Hacking 310

Lesson 3: Non-Invasive Reconnaissance

Learning Objectives

After completing this lesson, students will be able to:

1. Conduct a Google Search of an organization for exposed files and/or information.
2. Conduct a Whois lookup of a domain and understand the results.
3. Conduct an extended sub-domain search and identify additional targets.
4. Use the basic functions of Maltego to create a case.

Exposed Files and/or Information

Open source recon tools:

- Google Hacking Database (GHDB) aka Google Dorking aka Google Search Parameters
- Whois.net / GoDaddy Domain Search
- Pentest-Tools.com
- SearchDiggity from Bishop Fox
- FOCA / Evil FOCA from ElevenPaths

Challenge: Google Hacking

Navigate to the Google Hacking Database and identify a Google Dork that would be helpful in discovering information that a company may not want to be discovered. Copy and paste that Google Dork into chat with an explanation of what it finds and why it's bad.

How could an organization use these Google Dorks to help defend their internet presence?

What is a Whois Lookup?

Whois standard:

- Public Domain Entities
- Private Domain Registrars

Whols: uw.edu

Domain Name: UW.EDU

uw-noc@uw.edu

Registrant:

University of Washington
4545 15th Ave NE
Suite 400
Seattle, WA 98105-4527
UNITED STATES

Name Servers:

HANNA.CAC.WASHINGTON.EDU
MARGE.CAC.WASHINGTON.EDU
HOLLY.S.UW.EDU 173.250.227.69,
2607:4000:301:1::69

Administrative Contact:

UW Network Operations Center
University of Washington
4545 15th Avenue NE
Box 354840 UW-IT NOC
Seattle, WA 98105-4527
UNITED STATES
(206) 221-6000
uw-noc@uw.edu

Domain record activated: 05-Mar-1999

Domain record last updated: 14-Jul-2015

Domain expires: 31-Jul-2018

Technical Contact:

UW Network Operations Center
University of Washington
4545 15th Avenue NE
Box 354840 UW-IT NOC
Seattle, WA 98105-4527
UNITED STATES
(206) 221-6000

Whols: scarletsecurity.com

Domain Name: scarletsecurity.com
Registry Domain ID: 1835877116_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: <http://www.gandi.net>
Updated Date: 2017-10-15T00:29:16Z
Creation Date: 2013-11-18T07:01:23Z
Registrar Registration Expiration Date: 2018-11-18T07:01:23Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller: Amazon Registrar, Inc.
Domain Status: clientTransferProhibited
<http://www.icann.org/epp#clientTransferProhibited>
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Contact
Registrant Organization: Scarlet Security LLC
Registrant Street: Obfuscated whois Gandi-63-65 boulevard Massena
Registrant City: Obfuscated whois Gandi-Paris
Registrant State/Province: Paris
Registrant Postal Code: 75013
Registrant Country: FR
Registrant Phone: +33.170377666
Registrant Phone Ext:
Registrant Fax: +33.143730576
Registrant Fax Ext:
Registrant Email: 144c878b0b3b33d3a52a454f7d6d1f4e-4346891@contact.gandi.net
Registry Admin ID:
Admin Name: Domain Contact
Admin Organization: Scarlet Security LLC

Admin Street: Obfuscated whois Gandi-63-65 boulevard Massena
Admin City: Obfuscated whois Gandi-Paris
Admin State/Province: Paris
Admin Postal Code: 75013
Admin Country: FR
Admin Phone: +33.170377666
Admin Phone Ext:
Admin Fax: +33.143730576
Admin Fax Ext:
Admin Email: 144c878b0b3b33d3a52a454f7d6d1f4e-4346891@contact.gandi.net
Registry Tech ID:
Tech Name: Domain Contact
Tech Organization: Scarlet Security LLC
Tech Street: Obfuscated whois Gandi-63-65 boulevard Massena
Tech City: Obfuscated whois Gandi-Paris
Tech State/Province: Paris
Tech Postal Code: 75013
Tech Country: FR
Tech Phone: +33.170377666
Tech Phone Ext:
Tech Fax: +33.143730576
Tech Fax Ext:
Tech Email: 144c878b0b3b33d3a52a454f7d6d1f4e-4346891@contact.gandi.net
Name Server: NS-616.AWSDNS-13.NET
Name Server: NS-1619.AWSDNS-10.CO.UK
Name Server: NS-418.AWSDNS-52.COM
Name Server: NS-1172.AWSDNS-18.ORG
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: Unsigned

Sub-Domain Search: uw.edu

The screenshot shows the Pentest-Tools website interface. The browser address bar displays the URL `https://pentest-tools.com/information-gathering/find-subdomains-of-domain?run`. The page title is "Find Subdomains Result". A green checkmark and the text "uw.edu" indicate a successful search. Below this, a section titled "Found 141 subdomains" lists the results in a table. The table has five columns: Subdomain, IP address, Netname (whois), Country (whois), and Actions. The Actions column contains a "Scan with" button for each subdomain. The subdomains listed are: www.pce.uw.edu, brite.uw.edu, careers.uw.edu, www.hepatitisc.uw.edu, guides.lib.uw.edu, www.apsafe.uw.edu, www.brite.uw.edu, bioe.uw.edu, collaborate.uw.edu, ciso.uw.edu, privacy.uw.edu, www.hiv.uw.edu, www.std.uw.edu, hepatitisc.uw.edu, hr.uw.edu, webservices.uw.edu, comotion.uw.edu, sip.uw.edu, sites.uw.edu, canvas.uw.edu, cms.uw.edu, hsnewsbeat.uw.edu, and food.uw.edu.

Subdomain	IP address	Netname (whois)	Country (whois)	Actions
www.pce.uw.edu	13.91.47.132	?	?	Scan with
brite.uw.edu	23.236.62.147	?	?	Scan with
careers.uw.edu	34.199.156.30	?	?	Scan with
www.hepatitisc.uw.edu	34.209.6.190	?	?	Scan with
guides.lib.uw.edu	34.235.92.7	?	?	Scan with
www.apsafe.uw.edu	34.242.133.7	?	?	Scan with
www.brite.uw.edu	34.242.133.7	?	?	Scan with
bioe.uw.edu	35.163.14.75	?	?	Scan with
collaborate.uw.edu	37.60.253.109	?	?	Scan with
ciso.uw.edu	52.11.136.112	?	?	Scan with
privacy.uw.edu	52.11.136.112	?	?	Scan with
www.hiv.uw.edu	52.27.72.204	?	?	Scan with
www.std.uw.edu	52.32.11.61	?	?	Scan with
hepatitisc.uw.edu	52.42.244.164	?	?	Scan with
hr.uw.edu	52.52.1.88	?	?	Scan with
webservices.uw.edu	52.87.111.201	?	?	Scan with
comotion.uw.edu	52.88.145.91	?	?	Scan with
sip.uw.edu	52.112.192.203	?	?	Scan with
sites.uw.edu	52.202.201.6	?	?	Scan with
canvas.uw.edu	52.205.171.159	?	?	Scan with
cms.uw.edu	54.67.36.205	?	?	Scan with
hsnewsbeat.uw.edu	54.84.55.102	?	?	Scan with
food.uw.edu	69.91.245.18	?	?	Scan with

Maltego

Introduction to Maltego:

- Maltego Transforms
- Maltego Automated Machines

User Guide: <https://docs.paterva.com/en/user-guide/>