Report: Passive Reconnaissance of Purdue.edu

Objective:
The objective of this report is to perform initial passive reconnaissance of the target domain **purdue.edu**. The reconnaissance focuses on gathering publicly available information, including DNS details, WHOIS data, site information, and other relevant data, using passive tools and techniques.

Tools and Techniques Used:

1. **WHOIS & DNS Information Gathering:**
    - Utilized online tools to gather DNS information, site data, and mail-related information for the target domain (purdue.edu).
    - DNS information was gathered using tools such as **dnsdumpster**.
    - Site and mail information were extracted using WHOIS queries.
2. **Recon-ng:**
    - **Recon-ng** was used for further passive reconnaissance, where various modules were employed to gather domain, host, and contact information.
3. **Discover Scripts:**
    - The **Discover Scripts** by Lee Baird were used to gather additional information on Purdue.edu, specifically focusing on passive reconnaissance.
4. **Wayback Machine:**
    - The **Wayback Machine** was utilized as a tool to retrieve historical versions of the Purdue.edu website and gather additional information regarding the domain's past.

Results

1. WHOIS & DNS & Mail Information

- **DNS Information:**
  A screenshot of the **DNSdumpster** results for **purdue.edu** is provided. The tool revealed various DNS records, such as nameservers and IP addresses associated with the domain.
- **Site Information:**
  A screenshot of the **WHOIS** query for **purdue.edu** is provided. The results include detailed information about the domain's registration, including the registrar and registration dates.
- **Mail Information:**
  The **WHOIS** query also provided mail-related information, including the email address of the domain registrar and administrative contacts.

---

2. Recon-ng Modules Execution:

- **Workspace Setup:**
  A new workspace was created within Recon-ng with the name **[First Initial][Last Name]**.
- **Company & Domain Information Added:**
  The target company **Purdue** and domain **purdue.edu** were added to Recon-ng.
- **Modules Run:**
  The following modules were executed:
  - **bing_domain_web**: Retrieved web-related information using Bing.
  - **google_site_web**: Retrieved web-related information using Google.
  - **netcraft**: Retrieved additional domain-related information via Netcraft.
  - **resolve**: Resolved hostnames to IP addresses.
  - **reverse_resolve**: Performed reverse DNS resolution on discovered IPs.
  - **pgp_search**: Searched for PGP keys related to the domain.
  - **whois_pocs**: Retrieved WHOIS Point of Contact (POC) information.
- **HTML Report Generated:**
  An HTML report was generated, summarizing the findings. The report included my name in the "Created By" section and Purdue as the "Customer."

Screenshot of the HTML report is provided.

---

3. Discover Scripts Execution:

- **Setup:**
  The **Discover Scripts** were installed on Kali Linux, and the **discover.sh** script was launched.
- **Passive Reconnaissance:**
  The domain **purdue.edu** was entered, and the script was run in passive mode.
- **Generated Report:**
  A report was generated however Firefox had trouble opening the report. So I provided a screenshot to prove that a report was created.
- ---

4. Wayback Machine:

- **Tool Overview:**
  The **Wayback Machine** was used to retrieve historical versions of the Purdue.edu website.

- **Information Collected:**
  Screenshots of historical web pages were collected to analyze changes in the site's structure and content over time.
- **Usefulness of the Tool:**
  The Wayback Machine provides insights into the historical content of a domain. For a penetration tester, this tool can be valuable in understanding the evolution of a target site, uncovering previous vulnerabilities or outdated technologies that may still be exploitable.

Conclusion:

The passive reconnaissance performed on **purdue.edu** utilized various tools such as **Recon-ng**, **dnsdumpster**, **WHOIS**, **Discover Scripts**, and the **Wayback Machine** to gather useful information without actively probing the network. This data can be instrumental in identifying potential entry points, understanding the domain's infrastructure, and gathering contact details for further engagement in penetration testing.

All results, including screenshots of the tools' outputs, have been compiled into this report.

Screenshots:

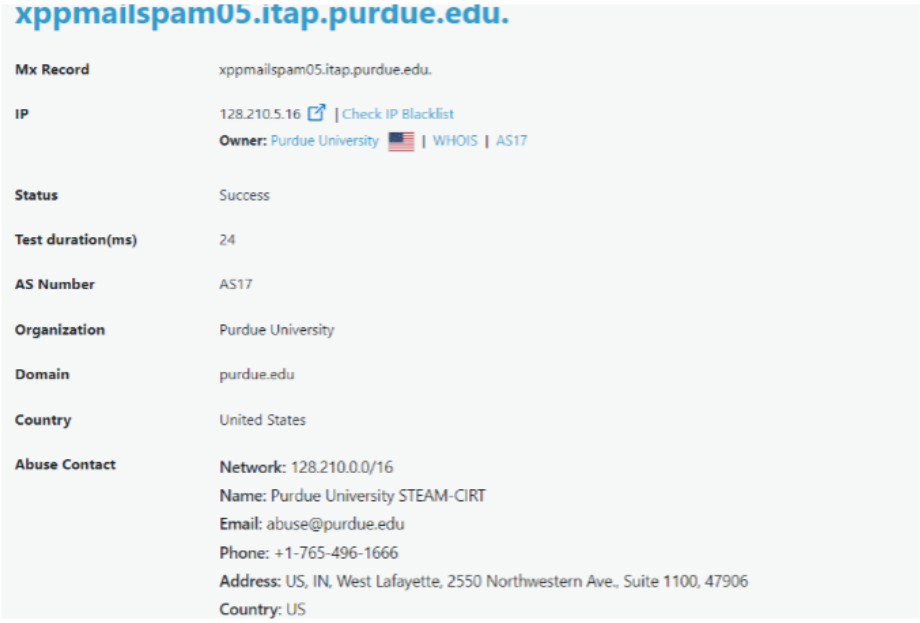
Whois: We can gather site information.

Domain Name: PURDUE.EDU
Registrant:
Purdue University
155 S. Grant Street
Young Hall
West Lafayette, IN 47907-2114
USA
Administrative Contact:
Purdue Hostmaster
Purdue University
191 North University Street
Telecommunications Building
West Lafayette, IN 47907-2068
USA
+1.7654944000
hostmaster@purdue.edu
Technical Contact:
Purdue Hostmaster
Purdue University
191 North University Street
Telecommunications Building
West Lafayette, IN 47907-2068
USA
+1.7654944000
hostmaster@purdue.edu
Name Servers:
NS1.RICE.EDU
NS3.PURDUE.EDU
PENDRAGON.CS.PURDUE.EDU
NS4.PURDUE.EDU

DNS:

DNS Servers		
ns4.purdue.edu.	128.210.224.234	PURDUE United States
harbor.ecn.purdue.edu.	128.46.154.76	PURDUE United States
ns3.purdue.edu.	128.210.224.226	PURDUE United States
pendragon.cs.purdue.edu.	128.10.2.5	PURDUE United States
ns2.rice.edu.	128.42.178.32	RICE-AS United States
ns1.rice.edu.	128.42.209.32	RICE-AS United States

Mail: Using a website like MX lookup we can see some mail server information for purdue.edu. Below is one screenshot, there is much more information that is available.



xppmailspam05.itap.purdue.edu.

Mx Record	xppmailspam05.itap.purdue.edu.
IP	128.210.5.16 | Check IP Blacklist **Owner:** Purdue University | WHOIS | AS17
Status	Success
Test duration(ms)	24
AS Number	AS17
Organization	Purdue University
Domain	purdue.edu
Country	United States
Abuse Contact	**Network:** 128.210.0.0/16 **Name:** Purdue University STEAM-CIRT **Email:** abuse@purdue.edu **Phone:** +1-765-496-1666 **Address:** US, IN, West Lafayette, 2550 Northwestern Ave., Suite 1100, 47906 **Country:** US

Recon-ng:

PURDUE

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	1
companies	1
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	218
contacts	10
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[+] Companies

[+] Hosts

[+] Contacts

Created by: Jake Simpson
Fri, Feb 09 2024 14:50:39

Discover (Proof of generation):

```
[*] Spooling output to '/tmp/networks'.
[recon-ng][purdue.edu][resolve] > db query SELECT DISTINCT netblock FROM netb
locks WHERE netblock IS NOT NULL ORDER BY netblock ASC
[*] No data returned.
[recon-ng][purdue.edu][resolve] > spool stop
[*] Spooling stopped. Output saved to '/tmp/networks'.
[recon-ng][purdue.edu][resolve] >
[recon-ng][purdue.edu][resolve] > spool start /tmp/subdomains
[*] Spooling output to '/tmp/subdomains'.
[recon-ng][purdue.edu][resolve] > db query SELECT DISTINCT host,ip_address FR
OM hosts WHERE host IS NOT NULL ORDER BY host ASC
[*] No data returned.
[recon-ng][purdue.edu][resolve] > db query SELECT DISTINCT host,ip_address FR
OM ports WHERE host IS NOT NULL ORDER BY host ASC
[*] No data returned.
[recon-ng][purdue.edu][resolve] > spool stop
[*] Spooling stopped. Output saved to '/tmp/subdomains'.
[recon-ng][purdue.edu][resolve] >
[recon-ng][purdue.edu][resolve] > exit
cat: networks: No such file or directory
cat: hosts: No such file or directory

The supporting data folder is located at /root/data/purdue.edu/

┌──(kali㉿kali)-[~/Downloads/discover-main]
└─$
```

Wayback:

This is the purdue.edu website from 2014