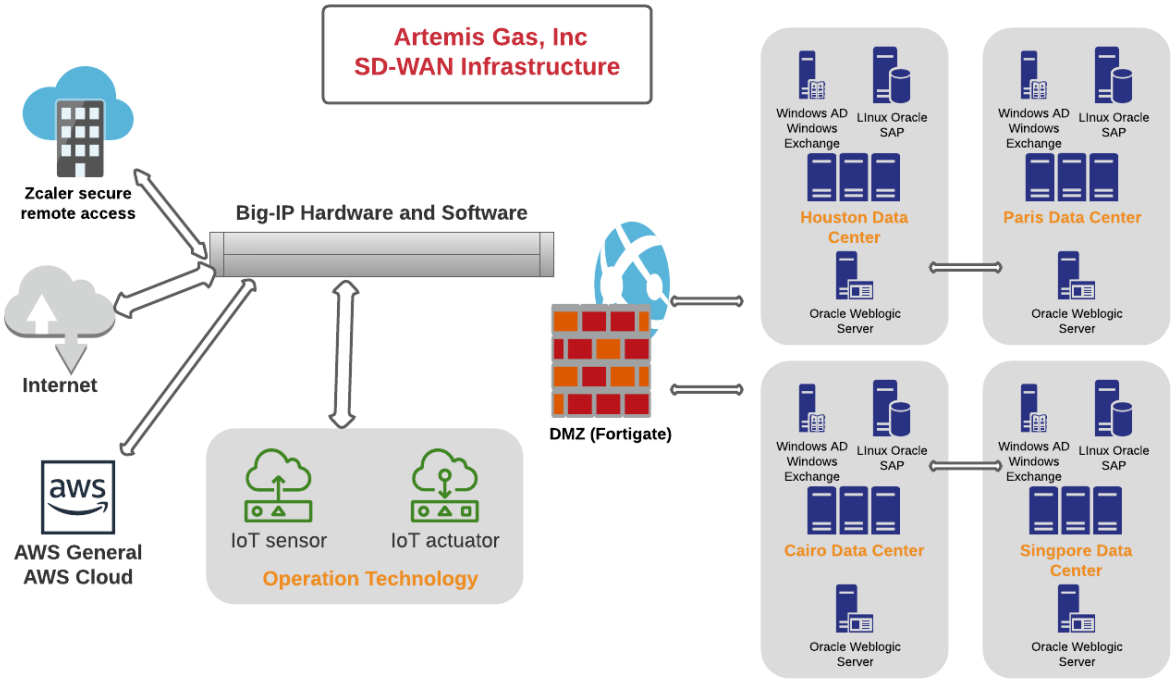
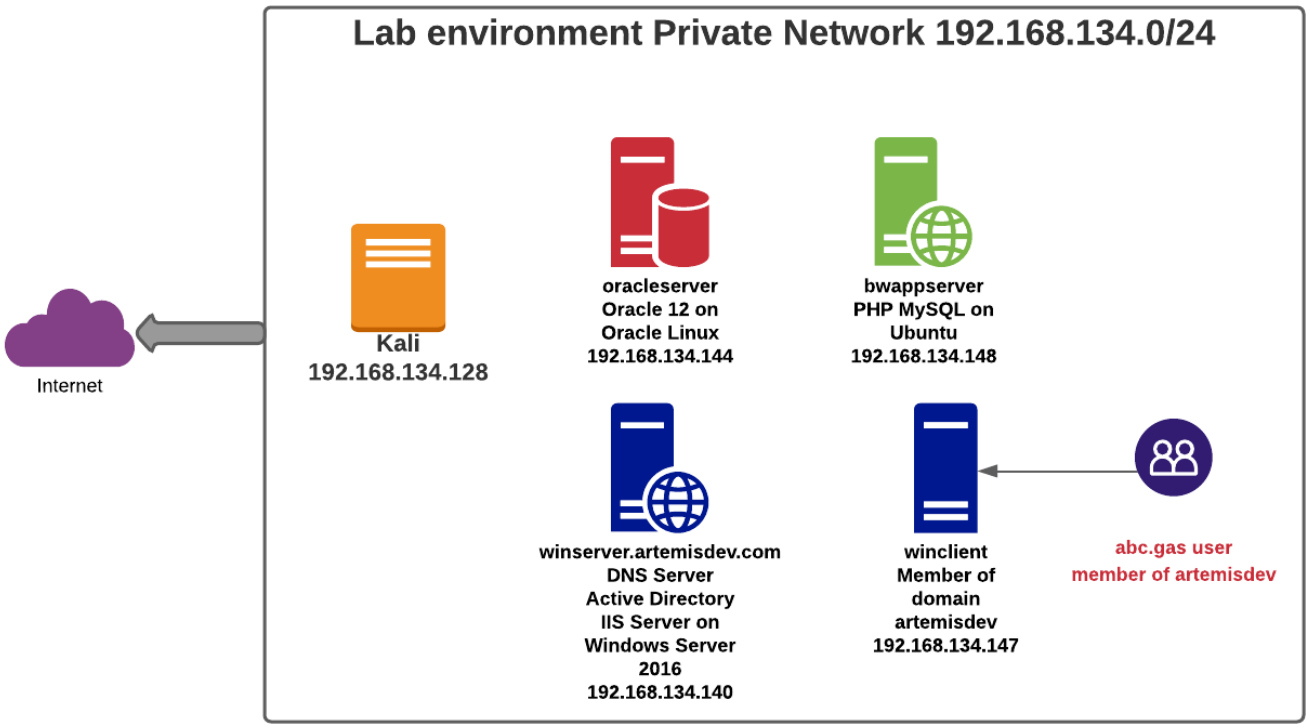
As cybersecurity analyst lead of **Pappas Security Firm**, I will oversee the penetration test performed for Artemis Gas Inc. by the pentester. The management group at Artemis has given the pen tester a vast amount of information on its company, thus this will be a white box penetration test. Senior management at Artemis gave the following information to use in the penetration test:

- Artemis supplies gas to 40 countries with 30,000 employees and over 1.7 million customers. They own and operate over 1,000 miles of industrial gas pipelines in the US. It's infrastructure consists of Operation Technology (OT) and Information Technology (IT).
- The OT consists of Internet of Things (IoT) sensors and actuators, Programmable Logic Controllers (PLCs), Human Machine Interface (HMI) and Supervisory control and data acquisition (SCADA).
- Big-IP, Software-defined wide area network (SD-WAN), and some Multiprotocol label switching (MPLS) links are used to connect to the internet and within the company intranet. The demilitarized zone (DMZ) into the four data centers mainly use Fortigate firewalls. Each data center consists of Windows Active Directory, Exchange Server, Oracle and SAP on Linux and Oracle Weblogic Server.
- For a remote access solution, Zcaler is used.
- For a cloud solution, Amazon Web Services (AWS) is used.
- The target (Artemis) IP ranges.
- The key contacts at Artemis who will be notified of the pen test.

In addition, the pentester has determined the time and duration of the penetration test.
The infrastructure for Artemis is shown in the diagram below:



A test lab was set up to allow the penetration tester to perform a structured walkthrough without affecting the production servers. The lab is shown is in the diagram below:



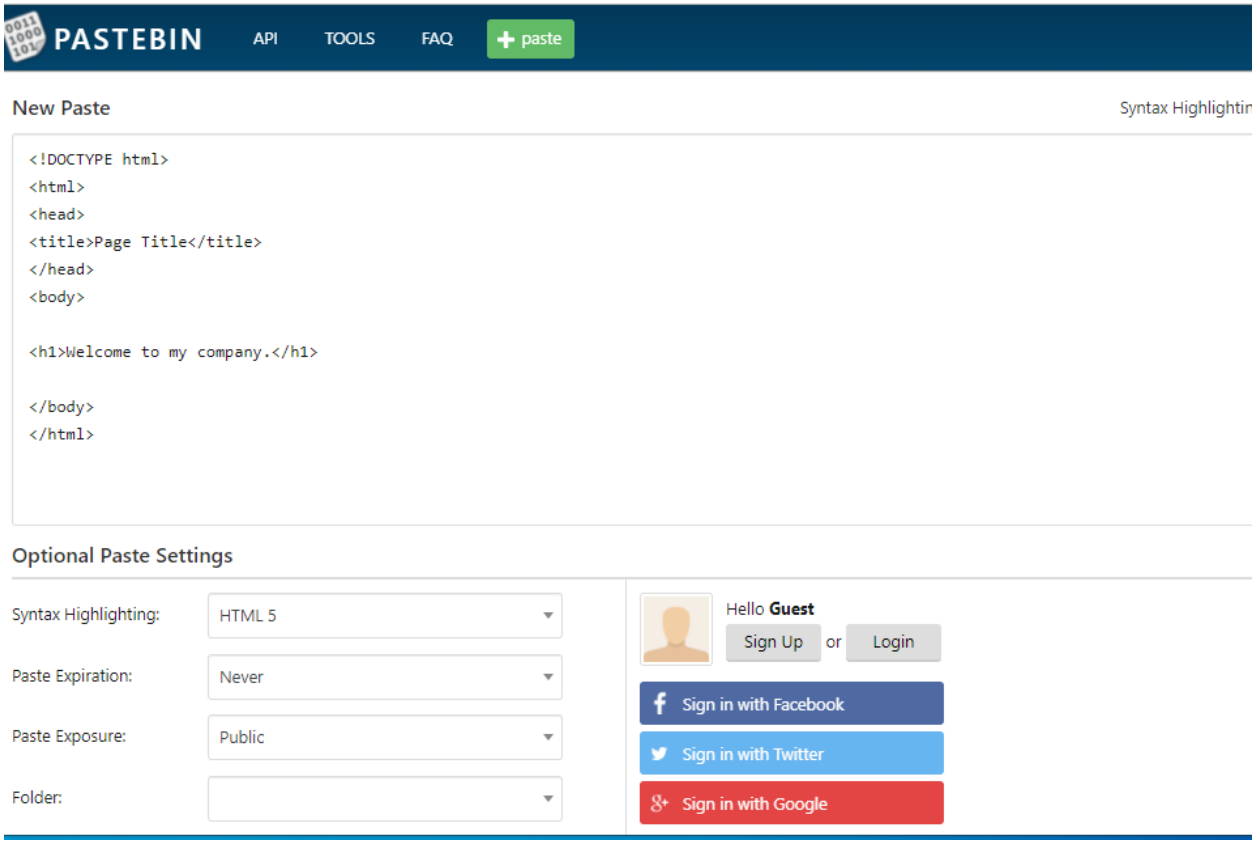
The penetration test will be performed in the following five phases:

- Phase 1: Perform Reconnaissance
- Phase 2: Identify Targets and Run Scans
- Phase 3: Identify Vulnerabilities
- Phase 4: Threat Assessment
- Phase 5: Reporting

In phase 1 ,performing reconnaissance, the pentester will use 15 tools from the OSINT framework to build a strong profile of Artemis which will consist of usernames, email addresses, phone numbers and resumes of employees and customers. The tools that will be used to collect this information will be as follows:

- **Tool 1:** When online services are compromised, it is likely that it will appear on “paste” sites like https://pastebin.com . Pastebin sites allow anonymous users and are hosted on the deep web where they are viewable in a regular internet browser, but the content is not indexed by Google and other traditional search engines. Since sharing is among anonymous users, **Pastebin** allows these users to share plain text like company code and Personal Identifiable Information (PII) such as names, addresses, social security

numbers, and credit card numbers of employees and customers. An example is shown below where the user is anonymous and code is made public:

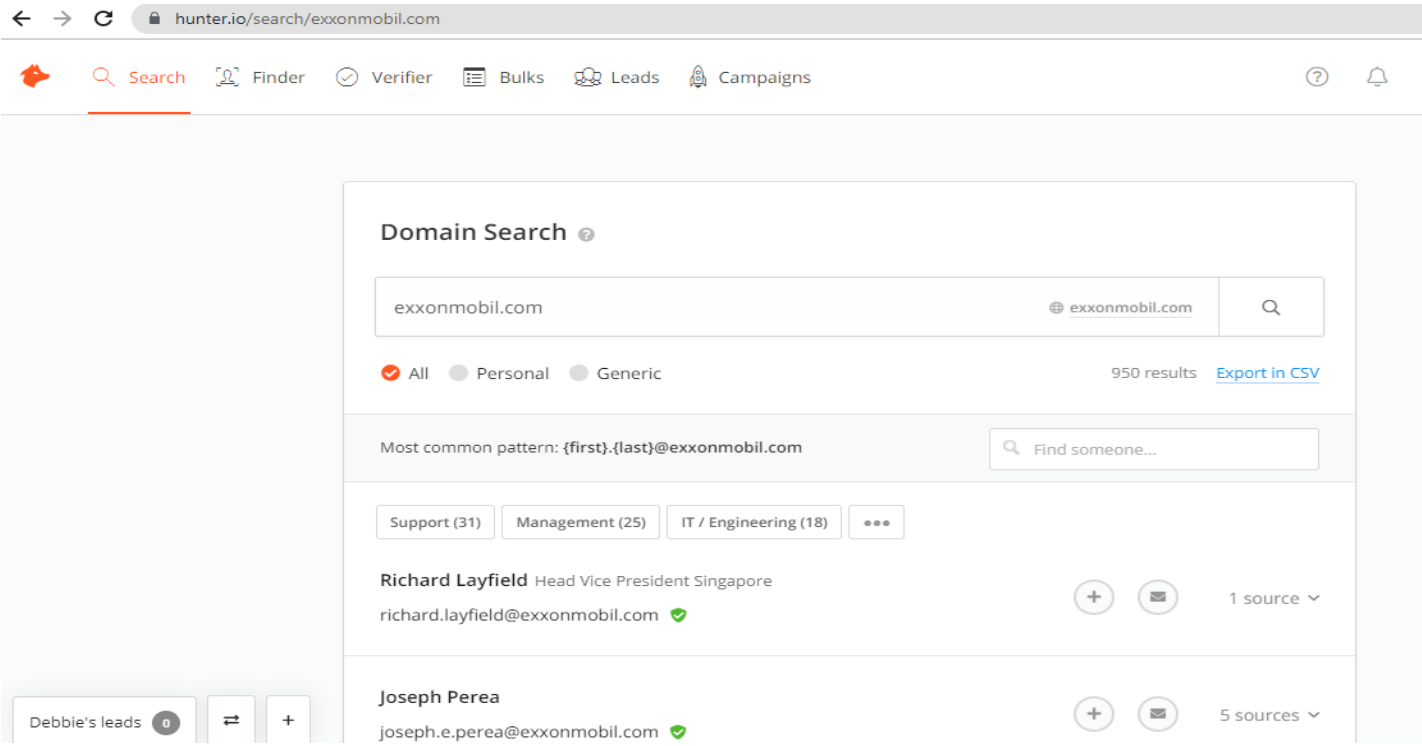


- **Tool 2: LinkedInt** is an open source tool generated by running a python script located on github at https://github.com/vysecurity/LinkedInt . When the script is run, the user inputs the domain name and keywords of the Artemis company. The script will then generate a html and csv file with photos, email addresses, job titles and locations. The input below shows the output when exxonmobil.com was used as the domain name.

  The input used (gm.com was replaced with exxonmobil.com):

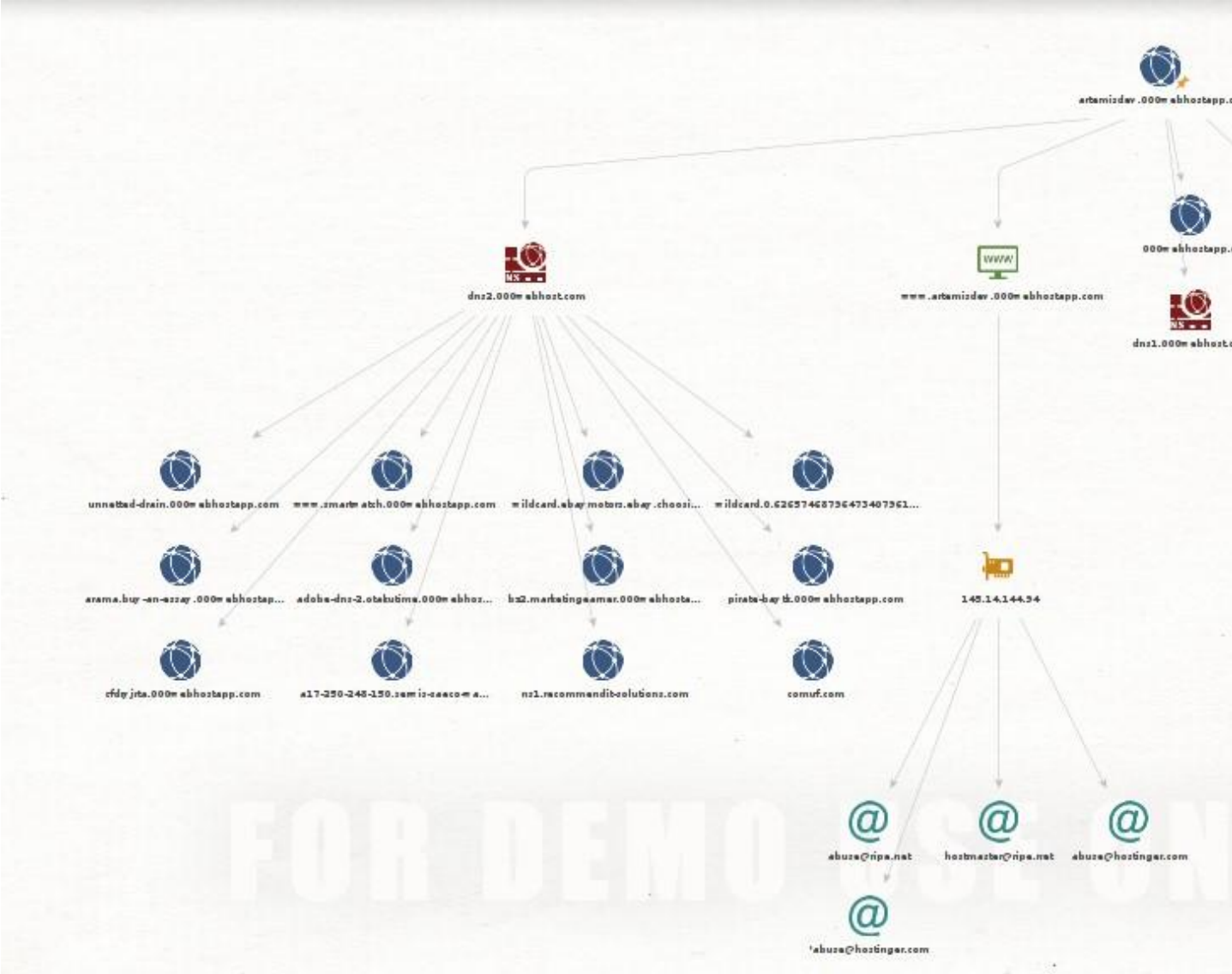
```
Providing you with Linkedin Intelligence
Author: Vincent Yiu (@vysec, @vysecurity)
Original version by @DisK0nn3cT
[*] Enter search Keywords (use quotes for more precise results)
"General Motors"

[*] Enter filename for output (exclude file extension)
generalmotors

[*] Filter by Company? (Y/N):
Y

[*] Specify a Company ID (Provide ID or leave blank to automate):


[*] Enter e-mail domain suffix (eg. contoso.com):
gm.com

[*] Select a prefix for e-mail generation (auto,full,firstlast,firstmlast,flast,first.last,fmlast):
auto

[*] Automatically using Hunter IO to determine best Prefix
[!] {first}.{last}
[+] Found first.last prefix
```

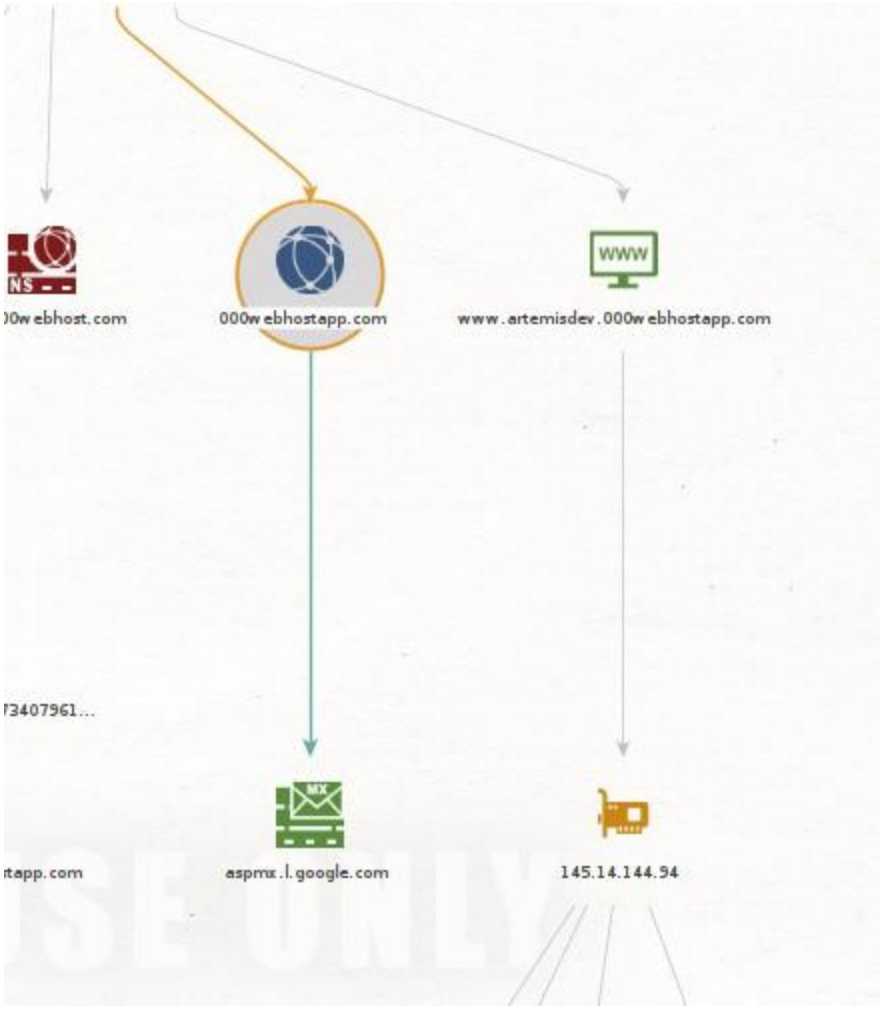
Tool 3: Hunter.io will primarily search for all email addresses associated with any domain. The example below is used with **exxonmobil.com** as the domain.



The results of the domain name search resulted in the email address of the Head Vice President in Singapore. This can be used in a whaling attack.

Tool 4: Using Maltego, we were able to extract the IP address of our server in our lab. The lab was set up with a Windows Server 2016 hosting a website http://winserver.artemisdev.com which gets redirected to a website https://artemisdev.000webhostapp.com . Besides Internet Information Services, Winserver (the windows server hostname) in the lab is also configured with Active Directory and DNS server. The diagrams below show that Maltego discovered that winserver.artemisdev.com is a webserver with the IP address of **145.14.144.94**, two DNS server named **dns1 and dns2**, and a **DNS 'mail exchange'** server coming from a mail server connecting to **google.com**.





- **Tool 5:** Fast Google Dorks Scan is available on github. The script named FGDS.sh is run against a website. For example, for the website in our lab the command would be:

  -> ./FGDS.sh artemisdev.000webhostapp.com

  This script collects all possible Google dorks search combinations to find the information about the specific website such as admin panels, file types and path traversal. The running script is shown in the diagram below:

```
Checking Login Page:
[*] Checking ADMIN        [-] No results
[*] Checking LOGIN        [-] No results
[*] Checking ADMINLOGIN          [-] No results
[*] Checking CPLOGIN      [-] No results
[*] Checking WEBLOGIN     [-] No results
[*] Checking QUICKLOGIN          [-] No results
[*] Checking WP-ADMIN     [-] No results
[*] Checking WP-LOGIN     [-] No results
[*] Checking PORTAL       [-] No results
[*] Checking USERPORTAL          [-] No results
[*] Checking LOGINPANEL          [-] No results
[*] Checking REMOTE       [-] No results
[*] Checking DASHBOARD    [-] No results
[*] Checking AUTH         [-] No results
[*] Checking EXCHANGE     [-] No results
[*] Checking FORGOTPASSWORD      [-] No results
[*] Checking TEST         [-] No results

Checking specific files:
[*] Checking DOC          [-] No results
[*] Checking DOCX         [-] No results
[*] Checking XLS          [-] No results
[*] Checking XLSX         [-] No results
[*] Checking PPT          [-] No results
[*] Checking PPTX
```

Tool 6: **Metagoofil** is installed by default on Kali Linux. It is used to extract files from a website. In the **artemisdev.com** domain, files with extensions pdf, doc, xls, ppt, odp, ods, docx, dxls, and pptx can be discovered by Metagoofil. These files can contain usernames which can be used for brute-force password attacks and diagrams of the company's infrastructure. In addition, this tool can extract "paths" of documents where you can get shared resource and server names.The diagram below shows the GUI interface of metagoofil:

Metagoofil results

Results for: 000webhostapp.com

0%	0%	0%	0%
0	0	0	0
Usernames	Software	Emails	Paths/Servers

User names found:

E-mails found:

0 results

Servers and paths found:

0 results

Files analyzed:

Tool 7: Recon-ng is a reconnaissance tool with an interactive console. The hackertarget module is used for the Artemis company to gather some subdomains. The source in this example is artemisdev.com which can be seen by the input command. When the show hosts command is run recon-ng discovers four hosts:

Artemisdev.000webhostapp.com (this is the website that winserver.artemisdev.com is redirected to.

000.webhostapp.com (this is the top level domain to the artemisdev website)

Ns1.artemisdev.com (this is implies that domain name artimesdev.com is highly secure, next generation managed DNS service.

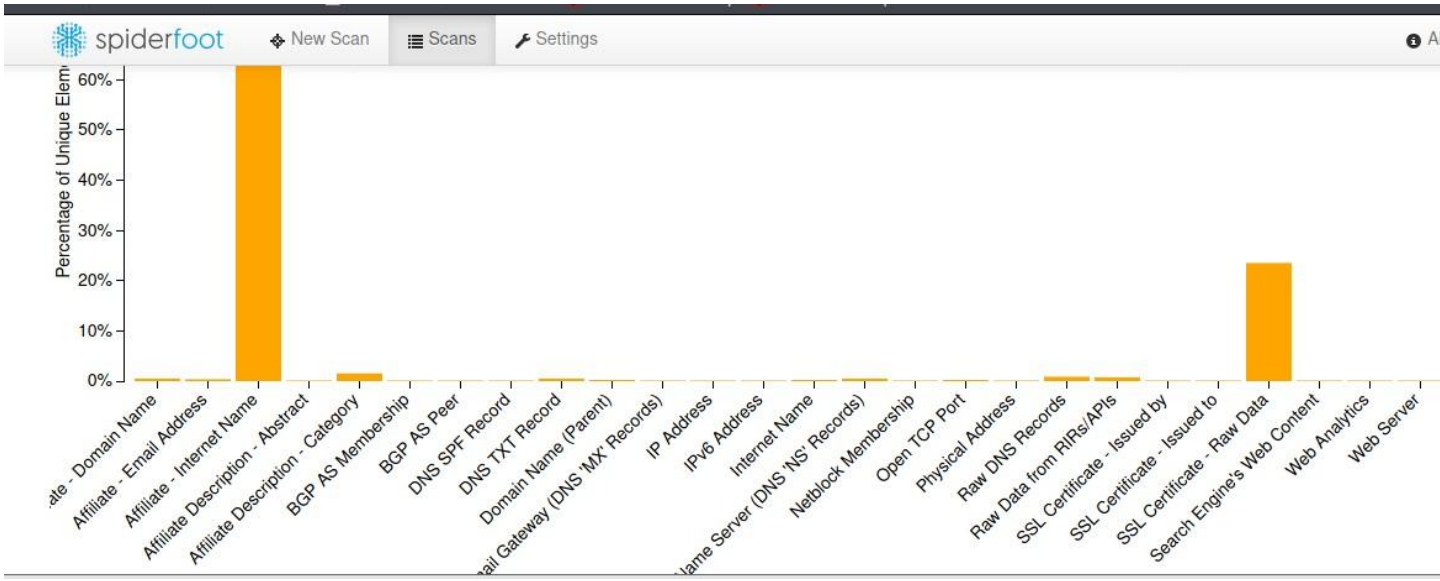
Mail.artemisdev.com (this is part of the active directory service that requests the users email address)

```
[recon-ng][default][hackertarget] > show hosts

  +-----------------------------------------------------------------------------------------------------------------------------------+
  | rowid |             host             |   ip_address   | region | country | latitude | longitude | notes | module |
  +-----------------------------------------------------------------------------------------------------------------------------------+
  | 1     | artemisdev.000webhostapp.com | 145.14.144.144 |        |         |          |           |       | hackertarget |
  | 2     | 000webhostapp.com            | 153.92.0.100   |        |         |          |           |       | hackertarget |
  | 3     | ns1.artemisdev.com           | 92.119.57.75   |        |         |          |           |       | hackertarget |
  | 4     | mail.artemisdev.com          | 92.119.57.75   |        |         |          |           |       | hackertarget |
  +-----------------------------------------------------------------------------------------------------------------------------------+

[*] 4 rows returned
[recon-ng][default][hackertarget] > input

  +----------------+
  | Module Inputs  |
  +----------------+
  | artemisdev.com |
  +----------------+
```

Tool 8: Energy companies such as Artemis are made up of Information Technology (IT) and Operation Technology (OT). The OT in Artemis contains Internet of Things (IoT) sensors and actuators. It is essential that security be addressed in IoT since these devices have many security flaws. Industrial Control Systems (ICS) are the control and IoT devices that operate or automate industrial processes. For example, to find potential vulnerabilities in the sensors for Artemis ICS, we can search using **Shodan** to find the number of sensors connected and accessible from the internet. When we try to navigate to the IP address, we can see the authentication page. By using a vulnerability scanner like Nessus we might be able to find a login vulnerability for this device. An example of Shodan is shown below. Shodan will initially discover the IP address of **http://artemisdev.000webhostapp.com** which is **145.14.144.94**. Running the command shodan host 145.14.144.94 results in the location of the server and the open ports. The 000webhostapp company is owned by Hostinger. We notice that the latest TLS version (1.3) is in place.

```
┌──(kali㉿kali)-[~]
└─$ shodan host 145.14.144.94
145.14.144.94
City:                    Hendersonville
Country:                 United States
Organization:            Hostinger International Limited
Updated:                 2021-09-25T14:55:53.964573
Number of open ports:    3

Ports:
     80/tcp
    443/tcp
        ├── SSL Versions: -SSLv2, -SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3
        ├── Diffie-Hellman Parameters:
                Bits:          2048
                Generator:     2
   8080/tcp

┌──(kali㉿kali)-[~]
└─$
```

Tool 9: Spiderfoot is used for active and passive scanning. In the Spiderfoot framework different scanning options and modules are available to set and scan the target host. Some scanning techniques it is used for are: domain footprinting, finding the phone numbers and email addresses of the target, and bitcoin addresses. A scan was run in spiderfoot of **artemisdev.000webhostapp.com**. The most data that can be seen is from the Affiliates of the Internet Name (000webhostapp.com). Given this information we can run the nmap command on the domain name or IP address to find the operating system. The diagrams below show the hostnames of the top level domain (000webhostapp.com).



spiderfoot New Scan Scans Settings

☐	acc0unts-gooogle.000webhostapp.com	000webhostapp.com	sfp_crt	2021-09
☐	accountsecuritiecheck.000webhostapp.com	000webhostapp.com	sfp_crt	2021-09
☐	acct-snap-chat.000webhostapp.com	000webhostapp.com	sfp_crt	2021-09
☐	acemnews.000webhostapp.com	000webhostapp.com	sfp_crt	2021-09
☐	aclcsm-enrollment.000webhostapp.com	000webhostapp.com	sfp_crt	2021-09
☐	acreidval.000webhostapp.com	000webhostapp.com	sfp_crt	2021-09

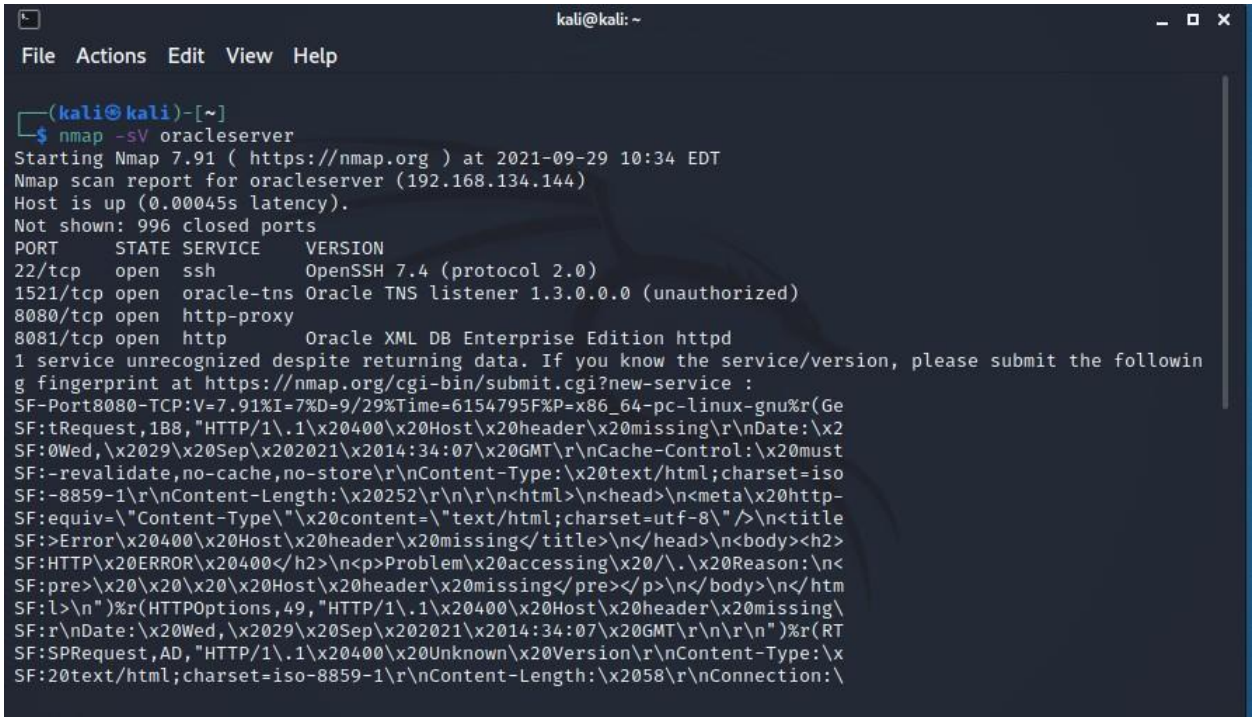
Tool 10: TheHarvester is a tool installed on Kali Linux that gathers information such as emails, sub-domains, hosts, employees names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN databases. PGP servers allow a user to search for a public key using an email address or name and download it. For the target website artemisdev.000webhostapp.com, two email addresses were found as shown below. For the Artemis company, theHarvester tool can be used to locate email addresses for phishing attacks.

```
[*] Target: artemisdev.000webhostapp.com

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 2
____________________
x22@artemisdev.000webhostapp.com
x3d@artemisdev.000webhostapp.com

[*] No hosts found.


┌──(kali㉿kali)-[~]
└─$
```

Tool 11: Artemis company uses Zcaler secure remote access to connect to the company's intranet. To find the Access Points (AP) in the Artemis company, a tool such as **aircrack-ng** can

be used. The first step is to get the wireless network card into monitor mode. This mode allows your card to see all the traffic around it. Then by using the **airodump-ng** command the BSSID (MAC address) of the AP or client will be captured. At this point, we know the number of APs Artemis has.

Tool 12: Nmap is used as a reconnaissance tool for Artemis to discover the application and services it uses and their port numbers. The command nmap -sV target is run on host winserver and host oracleserver. The following information can be obtained for Artemis using nmap:
Windows Server 2016 used as a web server, DNS server, and active directory domain controller.
The host oracleserver contains the oracle database.
Oracleserver which is not shown below will contain SAP which uses ports 32xx, 33xx and 36xx where xx is the instance number of the SAP system.
Artemis also contains Mail Exchange Server which uses mail ports such as POP3 (port 110), IMAP4 (143), SMTP (port 25), HTTP (port 80), HTTPS (443), AND LDAP (port 389).
The Oracle Weblogic Servers at Artemis use port 7001.

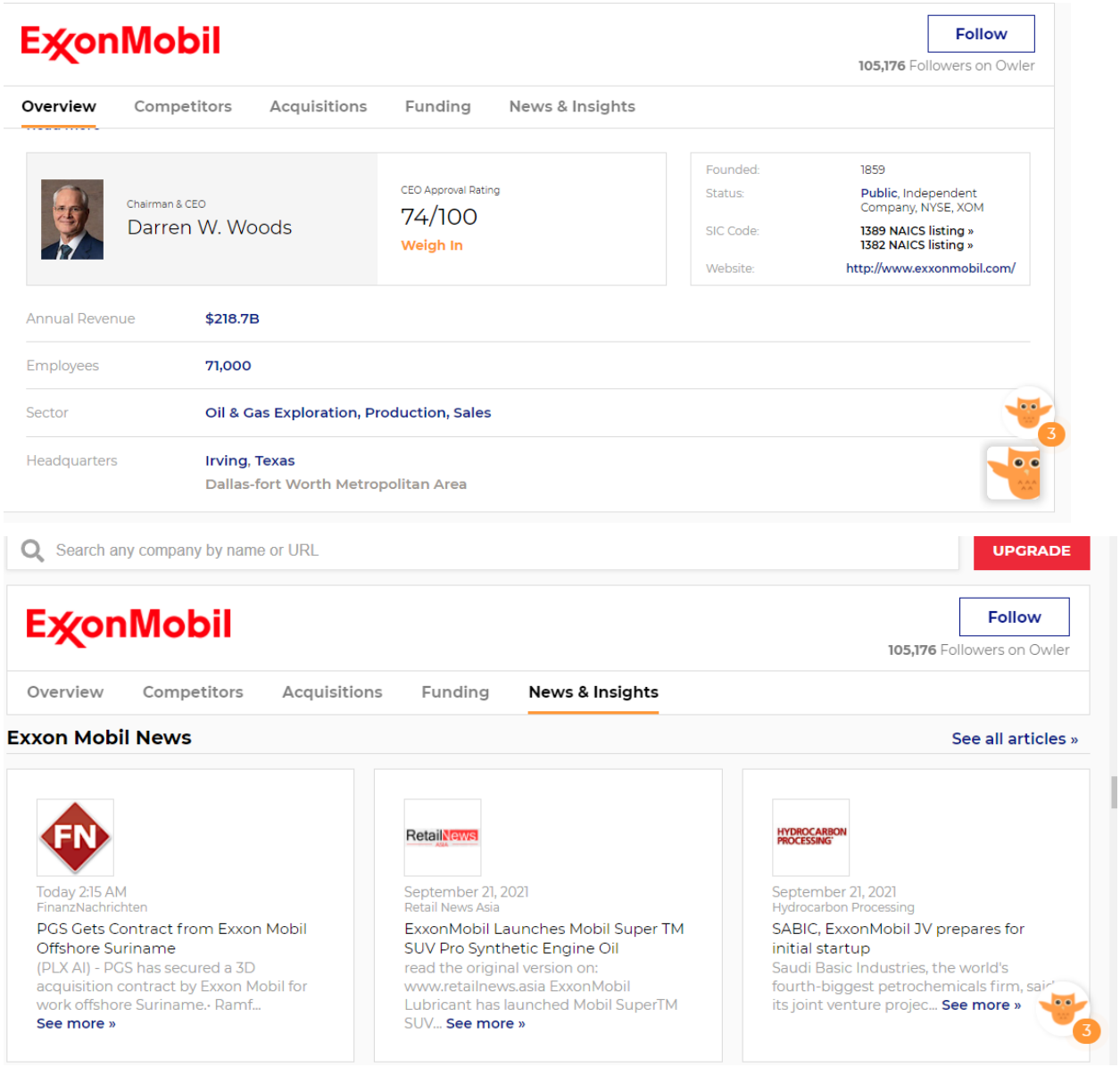


```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nmap -sV winserver
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-29 10:35 EDT
Nmap scan report for winserver (192.168.134.140)
Host is up (0.00058s latency).
Not shown: 987 filtered ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
80/tcp   open  http         Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-09-29 14:35:38Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: artemisdev.com, Site: Default
-First-Site-Name)
443/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: ARTEMISDEV)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: artemisdev.com, Site: Default
-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds

┌──(kali㉿kali)-[~]
```

Tool 13: Nslookup is used at the Artemis company to get the canonical name of the website. The canonical name is the properly denoted host name of a computer or network server. A CNAME specifies an alias or nickname for a canonical host name record in a domain name system (DNS) database. The example below shows the canonical name for artemisdev.000webhostapp.com. After googling the CNAME http://us-east-1.route-1.000webhost.awex.io , it is discovered that this server is a Windows 7.

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nslookup artemisdev.000webhostapp.com
Server:         192.168.134.2
Address:        192.168.134.2#53

Non-authoritative answer:
artemisdev.000webhostapp.com    canonical name = us-east-1.route-1.000webhost.awex.io.
Name:   us-east-1.route-1.000webhost.awex.io
Address: 145.14.145.223
Name:   us-east-1.route-1.000webhost.awex.io
Address: 2a02:4780:dead:1a83::1


┌──(kali㉿kali)-[~]
└─$
```

Tool 14: Artemis company will be added to owler.com to collect private company data. Owler uses a mix of crawling, algorithms, machine learning, and human input to collect the company data and profile. Some of this information includes the name of the CEO, any data breaches in the news or mergers.



Tool 15: Webshag which is part of Kali Linux can be used for reconnaissance at Artemis company. It's main features include port scanning, URL scanning, file fuzzing and website crawling. For Artemis, getting information on company files can reveal such information as the IT and OT technologies they use, the people who work there, usernames and passwords, and location of the offices.