ACME

Business Confidential

Date: 2/24/2024
Project: 897-20
Version 1.0

Table of Contents

Table of Contents

EXECUTIVE SUMMARY

ACME Company, a maker of anvils, anvil covers, and anvil protectors, was recently hacked. During the investigation, the previous security team was terminated, and the new Marvin the Martian Security Operations Center (SOC) was formed. To fill the open security engineering and analyst positions, the new Chief Information Security Officer (CISO) has approved a partnership with the Road Runner Corporation for immediate staffing with qualified contractors.

As a contractor working for the Road Runner Corporation, you will be given access to the ACME Company network infrastructure. You are tasked with determining the level of the breach and making recommendations for securing the network. In some cases, the recommended actions may be done in the network, and in some cases, they will be simulated. Your instructors, playing the role of corporate consultants, will let you know which actions to take and which to simulate.

During your contract-term with the ACME Company, you will provide updates to leadership. Based on your actions, the CISO will provide further direction.
Additionally, you will be completing reports. Details and requirements will be found in each corresponding assignment. Take notes of everything you do along the way, and ensure the reports are written for the correct audience.

SCOPE

Architecture

The virtual environment is a group of preconfigured virtual machines designed to emulate the ACME Company's headquarters network. Analysts and Engineers will use the virtual environment to complete tasks and obtain information required for the successful completion of the capstone.

The virtual environment relies on six (6) virtual machines provided as OVA files, which can be found here

As an employee of a contracting organization, you will either be issued a workstation by your employer, or provided a temporary workstation by the customer. The customer will direct you where to connect to their network from a point they have designated as appropriate for the type of work you are expected to perform. In practice, you should never connect to a customer's network from anywhere other than the explicitly authorized location.

In this scenario, Road Runner has provided you with the Road Runner consultant machine. This system connects to the Security Operations Center segment of the ACME company network. This machine will allow you to perform the necessary tasks required to complete the capstone project.

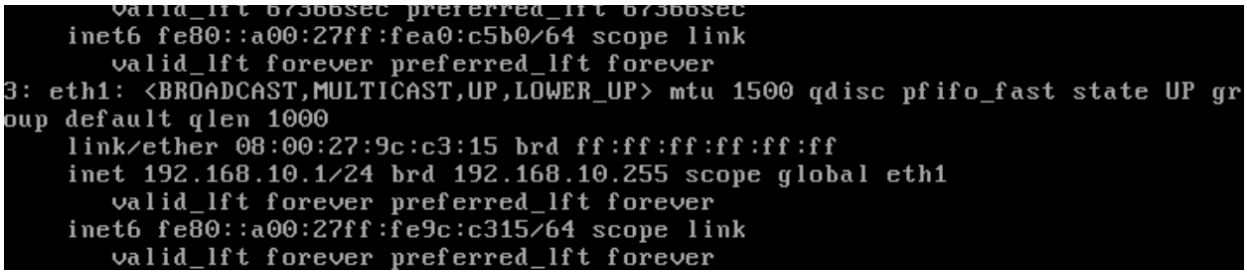
The hosts on the internal network represent typical types of systems and services found on an internal network. The virtual machines in the DMZ Network act as hosts and services normally found within a demilitarized design zone.

SCOPE

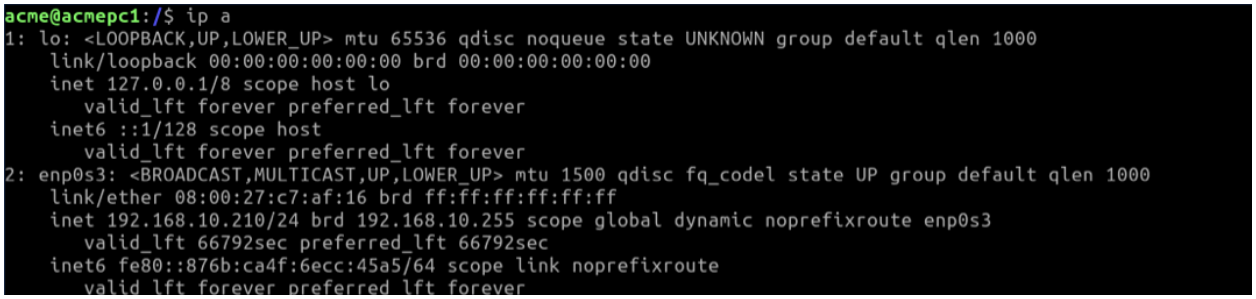
Scanning and Enumeration

The first step in connecting the machines is to find the **ip addresses** of machines within the virtual environment

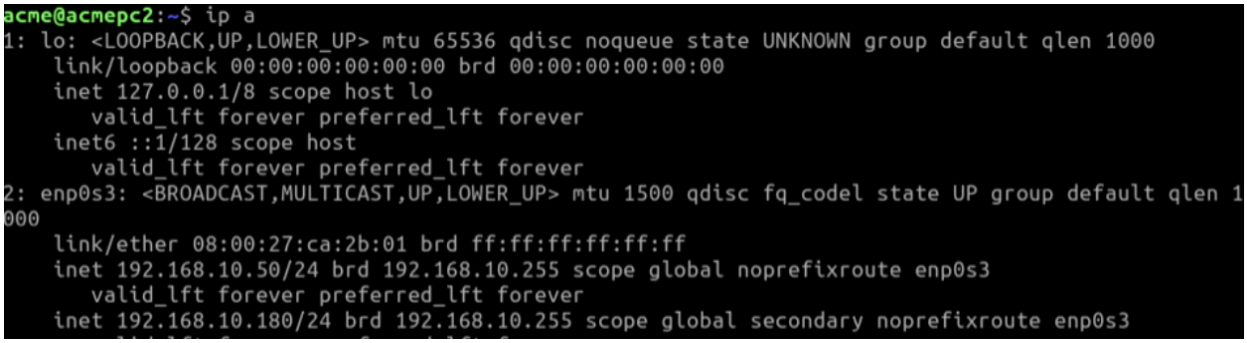
flatIronOS 1 ip: 192.168.10.1/24



Internal PC-1 ip: 192.168.10.210/24

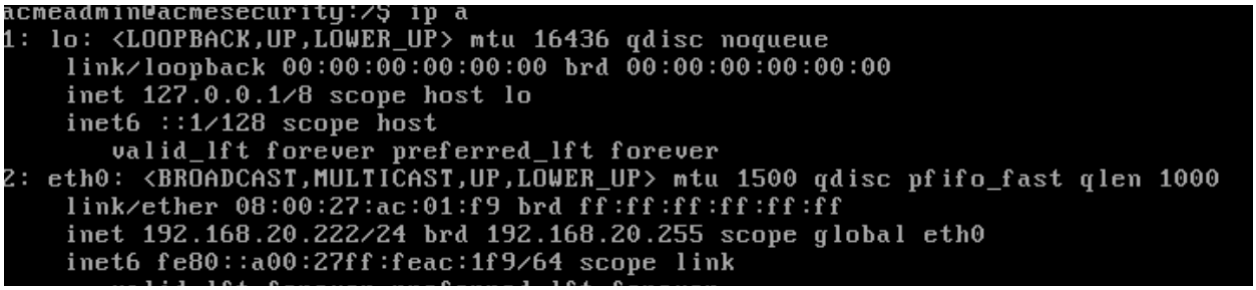


Internal PC-2 ip: 192.168.10.50/24



SCOPE

ACMEsecurity ip: 192.168.20.222/24



Consultant Machine ip: 192.168.30.204/24

Nmap

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a variety of features for probing computer networks, including host directory and service operating detection. You can run Nmap directly from the CLI. But it might be a good idea to run nmap from within metasploit so that the results are added to the MSF database.
The nmap scan of the InternalNet can be found here
The nmap scan of DMZ can be found here

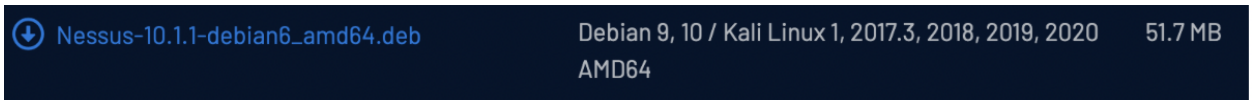
CISO DIRECTIVES - VULNERABILITY SCAN

Nessus

Nessus is a common and popular network vulnerability scanning tool for many companies.

To install Nessus on your machine, in this case the Roadrunner Consultant machine, begin by completing the form, using a valid email address, at the following site: https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true

After submitting the form, follow the link to download Nessus. Download the version appropriate for the lab machine's operating system. In the case of the Roadrunner consultant machine download this version of Nessus:



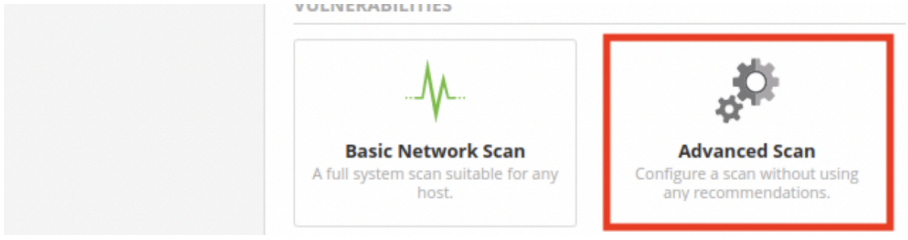
Install nessus with the following command:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.1.1-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 409383 files and directories currently installed.)
Preparing to unpack Nessus-10.1.1-debian6_amd64.deb ...
Unpacking nessus (10.1.1) ...
Setting up nessus (10.1.1) ...
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner
```

Start the service with the command **/bin/systemctl start nessusd.service**
Then go to **https://kali:8834/** to configure your scanner.

After setup for Nessus Essentials is complete select **Advanced Scan**



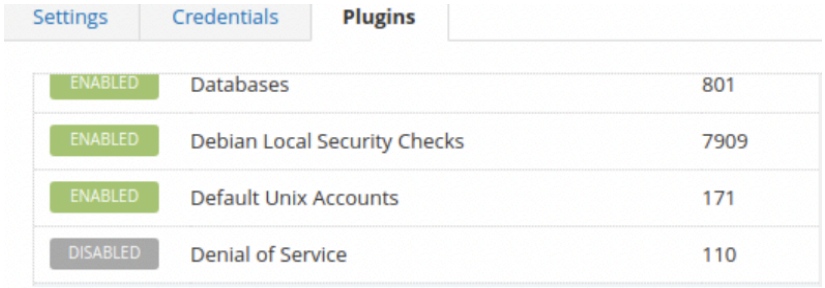
CISO DIRECTIVES - VULNERABILITY SCAN

Looking back to the nmap scans performed earlier, fill out the target section of the new scan with the IP addresses discovered from nmap.

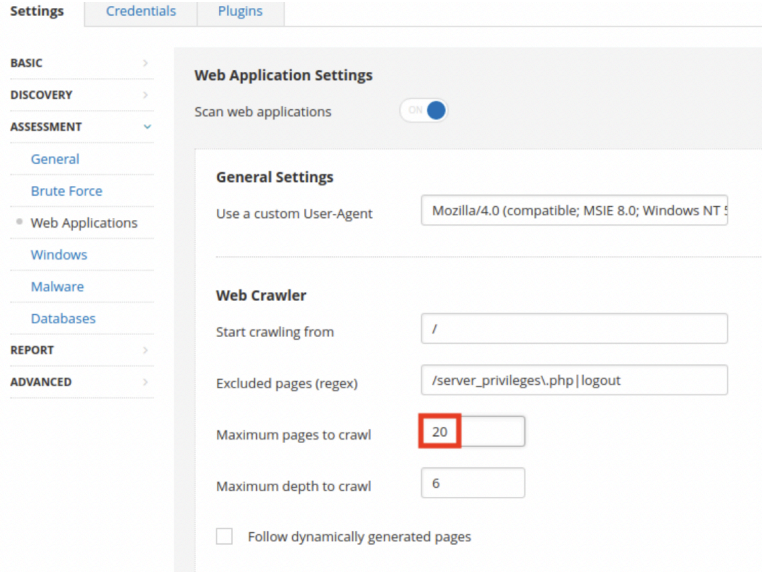
Note there are limitations in how many items may be scanned with the trial version of Nessus. Currently, there is a 16 host limit on Nessus Essentials.

Use the NMAP scan to prioritize which hosts to scan first, based on apparent risk.

Next, proceed to the **Plugins** tab and note the various categories of plugins. Disable the **Denial of Service** plugins by clicking it once, as that is beyond the scope of this lab:



Under the **Settings->ASSESSMENT->Web Applications** tab, click the button to enable this feature and change the **Maximum pages to crawl** to 20, to reduce the load on the target systems:



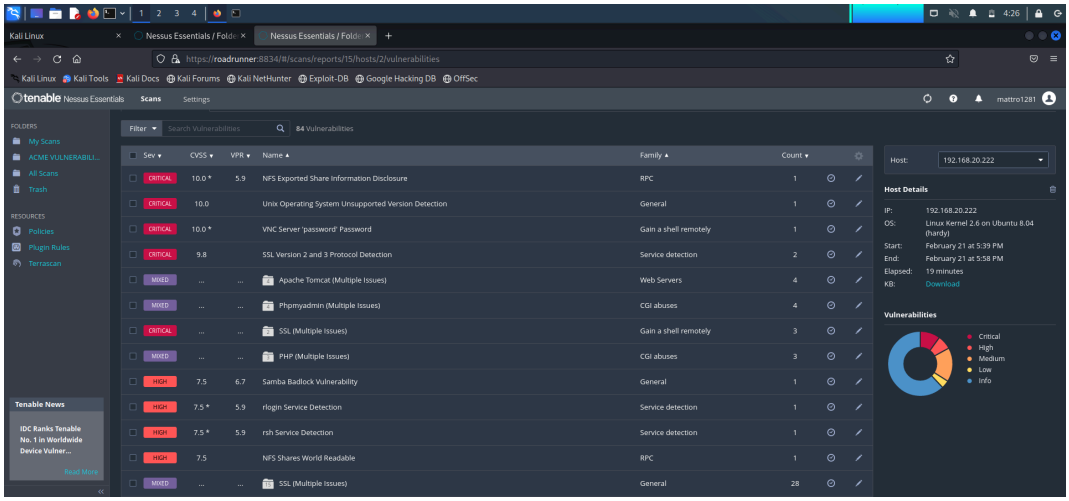
CISO DIRECTIVES - VULNERABILITY SCAN

After running the scan vulnerabilities will be separated first by host ip address. Next, within the ip address scanned vulnerabilities will be separated by “CRITICAL”, “HIGH”, “MEDIUM”, “MIXED”, to represent a vulnerability with multiple issues of different risk levels, and “INFO”, to represent low risk:

Risk Assessment

The best way to mitigate overall risk within the environment is to focus on vulnerabilities listed as, “CRITICAL”, and “HIGH.”

These are the vulnerabilities associated with the ip address 192.168.20.222, **ACMEsecurity**:



CISO DIRECTIVES - VULNERABILITY SCAN

NFS Exported Share Information Disclosure - CRITICAL

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote hosts.

Solution:

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Unix Operating System Unsupported Version Detection - CRITICAL

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution:

Upgrade to a version of the Unix operating system that is currently supported.

VNC Server ‘password’ Password - **CRITICAL**

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution:

Secure the VNC service with a strong password.

CISO DIRECTIVES - VULNERABILITY SCAN

SSL Version 2 and 3 Protocol Detection - CRITICAL

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

Apache Tomcat SEoL (<+ 5.5.x) - CRITICAL

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution:

Upgrade to a version of Apache Tomcat that is currently supported.

Apache Tomcat AJP Connector Request Injection (Ghostcat) - CRITICAL

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution:

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

CISO DIRECTIVES - VULNERABILITY SCAN

phpMyAdmin prior to 4.8.6 SQLi vulnerability(PMASA-2019-3 - CRITICAL

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in the designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data

Solution:

Upgrade to phpMyAdmin version 4.8.6 or later.
Alternatively, apply the patches referenced in the vendor advisories.

phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code injection (PMAS-2009-4) - HIGH

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input before using it to generate a config file for the application. This version is affected by the following vulnerabilities :
- The setup script inserts the unsanitized verbose server name into a C-style comment during config file generation.
- An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config.php.

An unauthenticated, remote attacker can exploit these issues to execute arbitrary PHP code.

Solution:

Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory.

CISO DIRECTIVES - VULNERABILITY SCAN

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) - CRITICAL

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian package removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution:

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness - CRITICAL

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution:

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

CISO DIRECTIVES - VULNERABILITY SCAN

Apache PHP-CGI Remote Code Execution - CRITICAL

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution:

Upgrade to PHP 5.3.13 / 5.4.3 or later.

PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution - HIGH

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc.

Solution:

If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.
Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

Samba Badlock Vulnerability - HIGH

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution:

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

CISO DIRECTIVES - VULNERABILITY SCAN

rlogin Service Detection - HIGH

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution:

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

rsh Service Detection - HIGH

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution:

Place the appropriate restrictions on all NFS shares.

NFS Shares World Readable - HIGH

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Solution:

Place the appropriate restrictions on all NFS shares.

CISO DIRECTIVES - VULNERABILITY SCAN

SSL Medium Strength Cipher Suites Supported (SWEET32) - HIGH

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution:

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

ISC BIND Service downgrade / Reflected DoS - HIGH

According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Solution:

Upgrade to the ISC BIND version referenced in the vendor advisory.

CISO DIRECTIVES - VULNERABILITY SCAN

Residual Risk

The residual risk for each associated item will be measured after the corresponding solution has been put in place. If the risk is still unacceptable additional controls may need to be put in place.

Recommendations:

As a measure of best practice it is important to **educate staff** about the importance of security. This education will prevent many security incidents from happening while **continuous monitoring** will allow security incidents to be addressed quickly.

Vulnerabilities listed within the Nessus scan as, “CRITICAL” and “HIGH” should be addressed immediately. The provided information and recommendations for solutions should be passed to the Engineering team right away to implement.

CISO DIRECTIVE: OSINT PLAN

Open Source Intelligence (OSINT) is a method of gathering information from public or other open sources, which can be used by security experts, national agencies, or cybercriminals

For example, useful information that can be revealed through OSINT includes open ports; unpatched software with known vulnerabilities; publicly available IT information such as device names, IP addresses and configurations; and other leaked information belonging to the organization.

Websites outside of your organization, especially social media, contain huge amounts of relevant information, especially information about employees. Vendors and partners may also be sharing specific details about an organization's IT environment. When a company acquires other companies, their publicly available information becomes relevant as well.

OSINT Gathering Techniques

Here are three methods commonly used to gain open intelligence data.

Passive Collection

This is the most commonly used way to gather OSINT intelligence. It involves scraping publicly available websites, retrieving data from open APIs such as the Twitter API, or pulling data from deep web information sources. The data is then parsed and organized for consumption.

Semi-Passive

This type of collection requires more expertise. It directs traffic to a target server to obtain information about the server. Scanner traffic must be similar to normal Internet traffic to avoid detection.

CISO DIRECTIVE: OSINT PLAN

Active Collection

This type of information collection interacts directly with a system to gather information about it. Active collection systems use advanced technologies to access open ports, and scan servers or web applications for vulnerabilities.

This type of data collection can be detected by the target and reveals the reconnaissance process. It leaves a trail in the target's firewall, Intrusion Detection System (IDS), or Intrusion Prevention System (IPS). Social engineering attacks on targets are also considered a form of active intelligence gathering.

Exploitation - Open Ports

Referring back to the Internal and DMZ nmap scans we discover the open ports running on the system. Understanding what runs on the assigned ports we are able to exploit the vulnerabilities of each.

Recommendations to mitigate risk are listed within each of the following ports:

Port 21 FTP

FTP (File Transfer Protocol) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.

Recommendations:

1. Require a password. Require a password for all your file transfers. ...
2. Limit IP addresses. It is also recommended that you limit IP addresses when using FTP and connecting through Port 21.

CISO DIRECTIVE: OSINT PLAN

Port 22 SSH

The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network.

Recommendations:

A highly effective deterrent and to improve security is to simply turn Port 22 off and run the service on a seemingly random port above 1024

Port 25 SMTP

SMTP is an application used by mail servers to enable communication between the sending and receiving servers when delivering an email message to a recipient.

Recommendations:

Port 25 is unencrypted and therefore less secure. Consider running the service on a different port, like Port 587.

Port 53 DNS

DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port. Port 53 is used for both TCP and UDP communication.

Recommendations:

Port 53 needs to be open for servers listening for DNS queries, same as port 80 needs to be open for servers listening for HTTP requests. Consider building a firewall to protect.

Port 80 HTTP

Port 80 is the default network port for web servers using HTTP. It operates on the application layer of the TCP/IP networking model and serves as the communication gateway for HTTP requests and responses between client computers and servers.

Recommendations:

1. Set up a firewall to monitor, control, and log all incoming and outgoing traffic.
2. Switch to HTTPS (operates on port 443 and uses SSL/TLS for encryption).
3. Use IDS to detect suspicious activities or violations.
4. Keep your server software up to date.

Port 135 TCP

Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network.

Recommendations:

Stop lateral movement by deploying a network-wide policy that can limit communication on ports like TCP 135 by denying it between user's machines. Limit these ports to a select few administrator systems.

Port 139+445 SMB/NetBIOS

Server Message Block shares files between different operating systems.
NetBIOS is (Network Basic Input/Output System) allows applications on separate computers to communicate and establish sessions to access shared resources.

Recommendations:

One approach to mitigating risk on Port 139 is to block NETBIOS traffic to/from the internet, or limit its use to specific IP addresses, using firewall rules. The best way to keep SMB secure is to disable port 445 in your firewall. This will prevent devices outside of your network from remotely connecting to devices inside it over the port, they can still do so by using a VPN.

Port 1723 PPTP (Remote Control Access)

Point-to-Point Tunneling Protocol (PPTP) provides a low-cost, private connection to a corporate network through the Internet. PPTP works well for people who work from home or travel and need to access their corporate networks.

Recommendations:

Consider closing the port and using remote control utilities such as TeamViewer and Log-Me-In and any other “out bound, https-based” remote control utility. These remote utilities don’t need an open port on your Firewall. Instead they reach out from the computer inside your network, through the Internet over https (encrypted with SSL), to a central server that in turn connects a client requesting that machine. Think of it as a “server” that sits in-between the two connections, brokering the connections.

CISO DIRECTIVE: OSINT PLAN

Port 3389 RDP

Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389. It provides network access for a remote user over an encrypted channel.

Recommendations:

Basic tips to improve RDP security include: using strong passwords, using two-factor authentication, updating software, restricting access using firewalls, enabling network level authentication, limiting users who can log on to RDP, and setting an account lockout policy.

Port 8080 HTTP

Port number 8080 is usually used for **web servers**. When a port number is added to the end of the domain name, it drives traffic to the web server. However, users can not reserve port 8080 for secondary web servers.

Recommendations:

Implement network security controls, such as firewalls and access control lists (ACLs), to restrict access to TCP port 8080 to only authorized users and systems.

Port 8443 HTTPS

Port number 8443 is an alternative HTTPS port and a primary protocol that the Apache Tomcat web server utilizes **to open the SSL text service**. In addition, this port is primarily used as an HTTPS Client Authentication connection protocol. A service called **Plesk Hostname** runs on this port.

Recommendations:

1. Log in to Plesk.
2. In Plesk, go to Tools & Settings and click SSL/TLS Certificates.
3. On the SSL/TLS Certificates page, add your certificate: ...
4. Click [Change] next to Certificate for securing Plesk > select an uploaded certificate > click OK.
5. Click **Install**. At this stage, an SSL certificate from Let's Encrypt is generated and set to secure Plesk on port 8443. This certificate will be auto-renewed every 90 days. Here is the final look:
6. Now, access Plesk over *https://server.example.com:8443*.

Port 9100 Printing

9100 TCP port is used **for printing**. Port numbers 9101 and 9102 are for parallel ports 2 and 3 on the three-port HP Jetdirect external print servers.

Recommendations:

Close port 9100 externally. If there is a requirement to print remotely, this is possible in a number of ways:

- Use a VPN to connect to the network, making the printer accessible as if it's in your local network
- Use a different printing protocol
    - IPP. This is designed to be used over the internet and has built in support for authentication.
    - Google Cloud Print

Port 17790 TCP

Used to communicate with the SolarWinds Platform server.

Recommendations:

Consider putting Port 17790 on a firewall. Any open ports will be vulnerable to an attack.

Port 10000 NDMP

Network Data Management Protocol (NDMP) runs on TCP port 10000 and is used primarily for **backup of network-attached storage (NAS) devices**, such as your storage systems.

Recommendations:

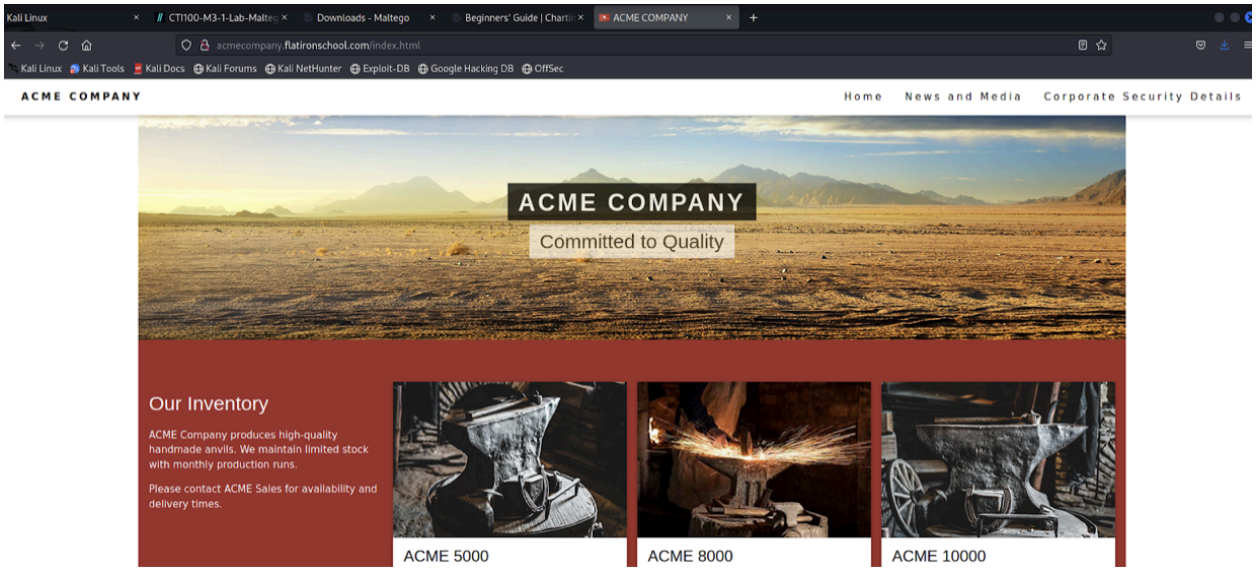
Consider putting Port 10000 on a firewall. Any open ports will be vulnerable to an attack.

CISO DIRECTIVE: OSINT PLAN

Social Media

Often, the easiest step to start with in an OSINT Plan is Passive Collection through publicly available information, like social media.

Begin by navigating to the html version of the ACME Company website:

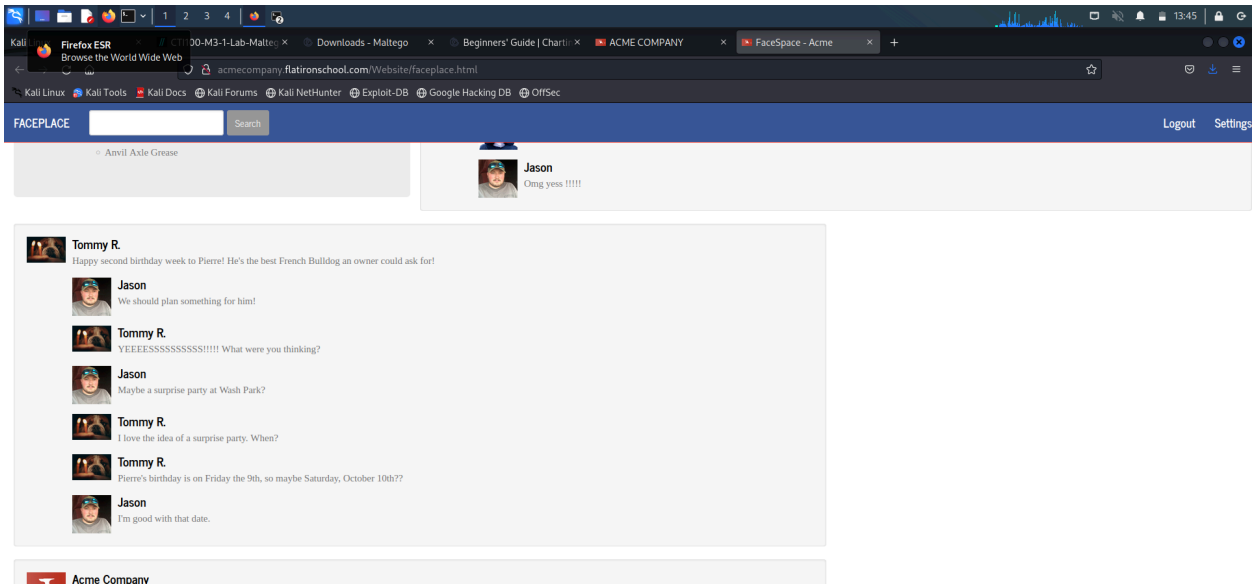


Navigate to the bottom of the page and there will be clickable links to Facebook, Instagram, and Twitter

CISO DIRECTIVE: OSINT PLAN

Facebook

Navigate to the facebook page:



Observing the information through a basic form of web reconnaissance we can find information for a user's password! After navigating through the IPC1 system we found a user to be named **triddle**. That looks oftly similar to Tommy R. After inspecting the text we can see Tom reveal he has a dog named **Pierre** whose birthday is on **October 10th**.

Brute forcing, or attempting to crack the password for triddle by educated guesses, we are able to switch user into the **triddle** account, which is also **root**. Now that we have root privileges we can move laterally and attack the system more thoroughly in a variety of ways. The associated password for **triddle** is **pierre1009**

There are also links to the company's Twitter and Instagram pages where further information could be collected.

CISO DIRECTIVE: OSINT PLAN

Maltego

Maltego is one of the most common methods utilized in an **OSINT Plan**. Maltego is a comprehensive tool that offers real-time data mining and information gathering. It allows for visual mapping of the mined data and discovered information.

Install Maltego directly from their website, https://www.maltego.com/downloads/. Maltego is also available in Kali Linux, though the version installed may be older and require an update. Note that Maltego requires an account to use their software, which in turn requires a valid email address to set up an account. It is possible to download and install the software without creating an account, but it will not be possible to open and use it without a valid account. In the setup process, make sure to choose **Maltego CE**, which is the free community version.

Follow Maltego's tutorial Links to an external site. to create a graph.

Maltego is very versatile. Maltego allows us to quickly pull data from posts, and comments into one graph, where we can conduct text searches and see connections. In just a few minutes, we can narrow initial research to a handful individuals using variations of aliases connected to suspected local traffickers.

Maltego is centered on pulling data, pieces of information for an Entity. An Entity is a piece of information shown as a node on the graph. Different Entity types are used to differentiate between the different pieces of information that can be represented in Maltego. Entitities can be anything from a DNS name, Person name, Phone number,

There are a variety of possible entities that could be run for the ACME company (i.e. URL, email address, etc.). Consider viewing information on the ACME Company html site, as well as all social media pages to find entities to run on Maltego.

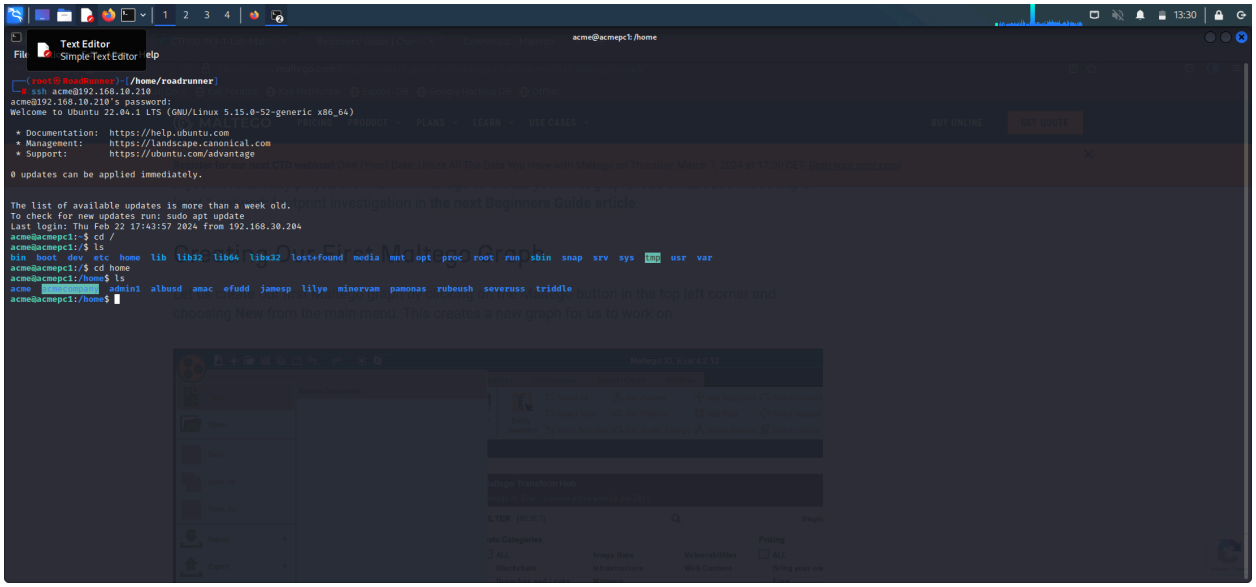
CISO DIRECTIVE: OSINT PLAN

Internal PC1

Taking more of an active form of reconnaissance these are the steps taken to collect information from Internal PC1:

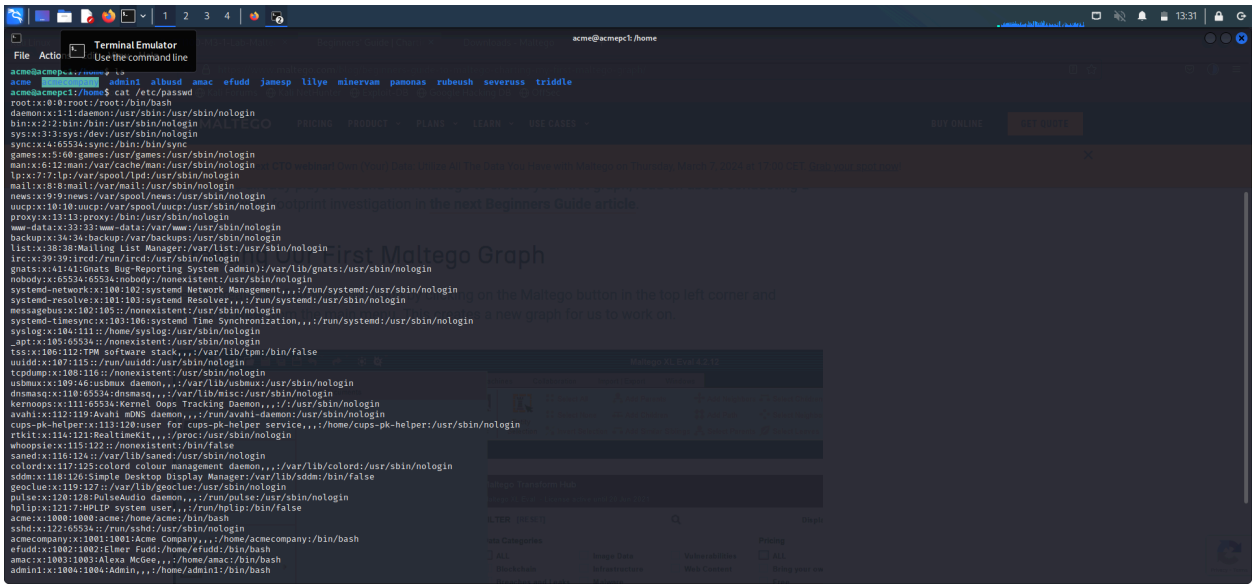
Working from the command line as **root user** on the Road Runner Consultant Machine we are able to ssh into the Internal PC1 from the following command:
ssh acme@192.168.10.210 in the form of
ssh [user]@[user-ip address] and providing the password for acme when asked

The list of **usernames** found on Internal PC1 can be found at the path **/home**



CISO DIRECTIVE: OSINT PLAN

The list of all **usernames and hashes** can be found running the command **cat /etc/psswd**



Hydra

Hydra is a brute-forcing tool that helps penetration testers and ethical hackers crack the passwords of network services.

Rockyou.txt serves as a dictionary for them, providing a list of potential passwords to try. Rather than attach the rockyou.txt file to this command in this instance consider creating a custom wordlist with relevant words found from social media reconnaissance. Rockyou.txt contains over 14 million possible passwords so running this exploit would take a considerable amount of time.

It was important to gain root access because without it we would not be able to run the command **hydra** or **hashcat**.

After switching users into **triddle** - which is root - issue the command:
**sudo hydra -l “triddle” -P wordlist.txt **
>192.168.10.210 ssh

CISO DIRECTIVE: OSINT PLAN

Hashcat

A common exploit used by hackers is utilizing a tool called **hashcat**, a password recovery tool. First, copy all the information from **cat /etc/passwd** and insert it into a newly created text file, lets say, **hashes.txt**.

To do so issue the command:
sudo vi hashes.txt

After switching users into **triddle** - which is root - pair both the hashcat and the hydra commands to run your exploit:
**sudo hashcat -a 0 -m 1800 crackedpasswords.txt **
>hasches1PC1.txt wordlist.txt

This would run hashcat with the flag -a(attack mode) option0 (straight dictionary attack) -m(hashing type) 1800(sha-512) -o (filename) carackedpasswords.txt (where to store the results) >hashesIPC1.txt (text file containing hashes from cat /etc/passwd) wordlist.txt (created wordlist from relevant words on social media pages).

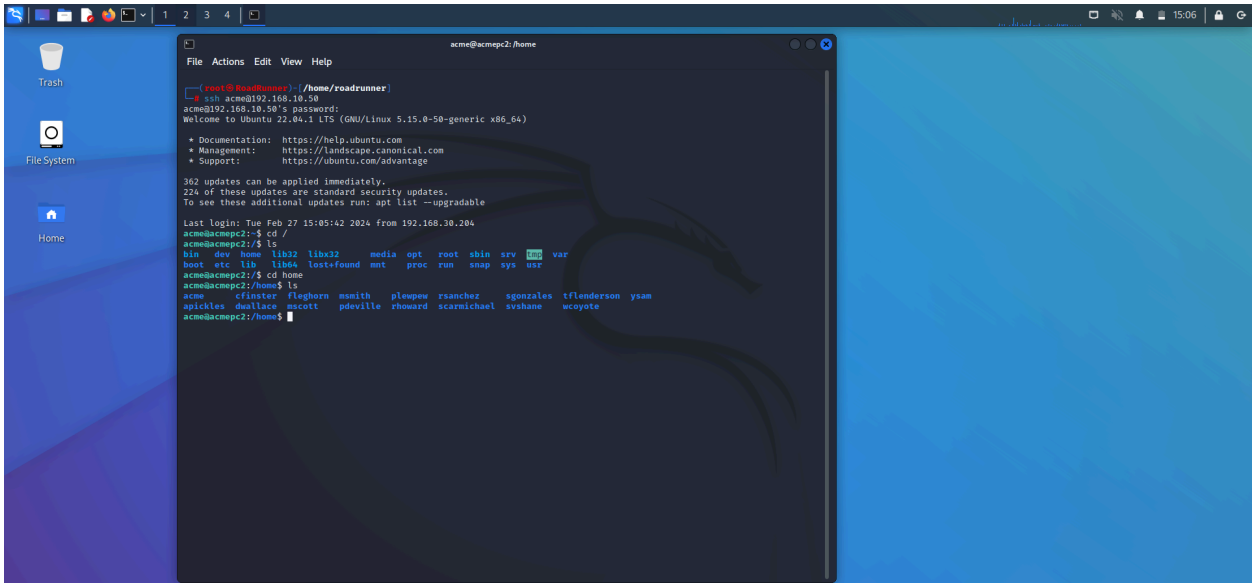
CISO DIRECTIVE: OSINT PLAN

Internal PC2

Taking more of an active form of reconnaissance these are the steps taken to collect information from Internal PC1:

Working from the command line as **root user** on the Road Runner Consultant Machine we are able to ssh into the Internal PC1 from the following command:
ssh acme@192.168.10.50 in the form of
ssh [user]@[user-ip address] and providing the password for acme when asked

The list of **usernames** found on Internal PC1 can be found at the path **/home**



The list of all **usernames and hashes** can be found running the command **cat /etc/psswd**

Similarly to **IPC1** you can run the same **hydra** and **hashcat** commands for **IPC2**