CompTIA Security+ 601

University Cyber Attack

Project 1

DESCRIPTION

You are a cyber security officer and member of the Incident Response Team.

During the summer vacation, one of the teaching staff members, Samantha, reports to the Dean about abusive and threatening messages received over an email. Dean collects the following details from her:

Complete Name: Samantha R. Collen.

Personal Email ID: samantha.collen.r@gmail.com

Official Email ID: profsamantha@pu.edu.com

Samantha also reported that during the term examination, she obstructed one of the students, Tony Lee, due to unfair means during examination.

As an investigator, your task is to identify the following:

University Cyber Attack

Project 1

Task 1: Obtain a scanning report of the entire network and identify how many terminals are connected with the Windows operating system and the Linux-based systems.

Note: Learners can use any platform like Kali Linux.

Task 2: Identify CVE score of the victim's vulnerability.

Note: Learners can use any open-source data sets for vulnerability like NVD (National Vulnerability Database).

Task 3: Identify whether the victim's terminal is affected with MiMT attack or not and submit the incident report for the same.

Note: Learners can orchestrate any attacks like Denial-of-service attack and create reports based on it.

Task 4: Use email forensics analysis and identify the sender's IP address

Note: Learners can create a dummy email ID, perform this task, or send an email to anyone. They can identify the sender's IP address.

Task5: Submit the complete incidence report

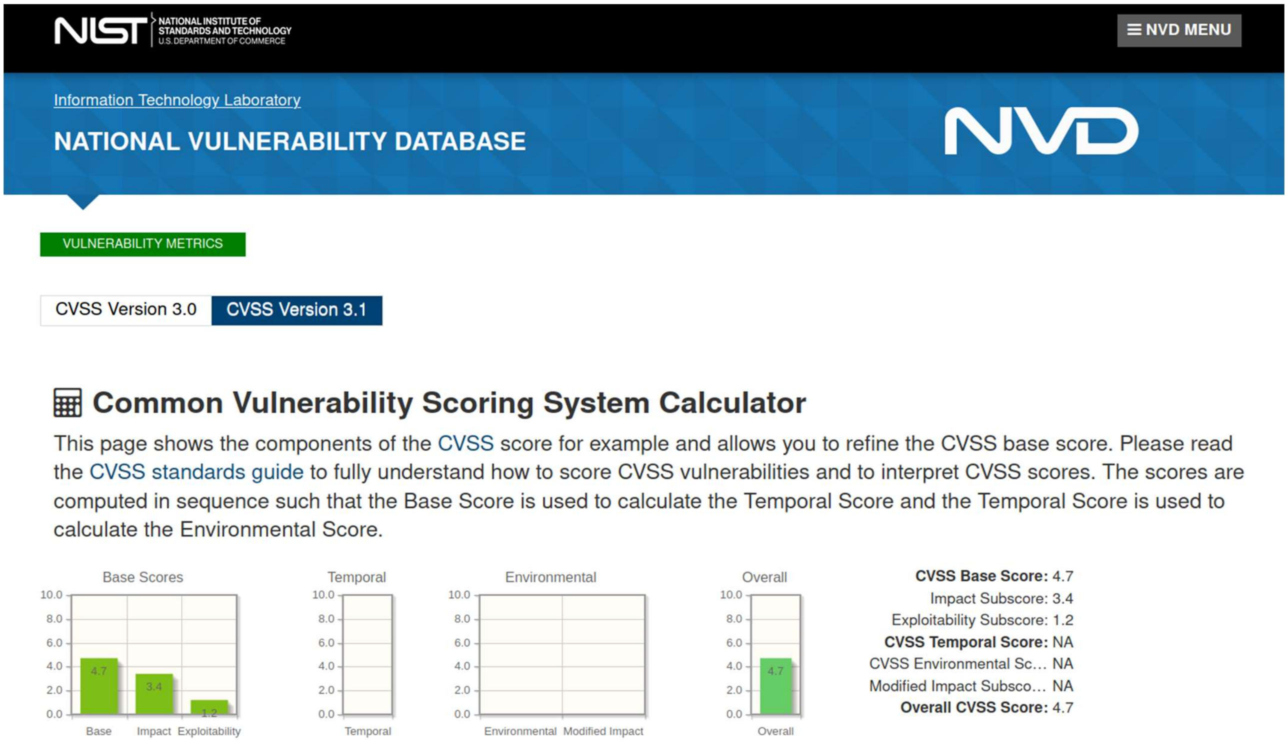
Task 1

Obtain a scanning report of the entire network and identify how many terminals are connected with the Windows operating system and the Linux-based systems.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-20 19:35 IST

Nmap scan report for 157.39.15.174

Host is up (0.025s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT     STATE SERVICE

21/tcp   open  ftp

554/tcp  open  rtsp

1723/tcp open  pptp

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: bridge

Running: Oracle Virtualbox

OS CPE: cpe:/o:oracle:virtualbox

OS details: Oracle Virtualbox


OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds.
```

Task 2

Identify CVE score of the victim’s vulnerability.



Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 4.7
Impact Subscore: 3.4
Exploitability Subscore: 1.2
CVSS Temporal Score: NA
CVSS Environmental Sc… NA
Modified Impact Subsco… NA
Overall CVSS Score: 4.7

According to the situation, I calculate the CVE score for the victim’s system and found that the overall CVE score is 4.7.

Task 3

Identify whether the victim’s terminal is affected with MiMT attack or not and submit the incident report for the same.

In a Man-in-the-Middle (MitM) attack, an attacker inserts himself between two network nodes. For example, in a successful attack, if Bob sends a packet to Alice, the packet passes through the attacker Eve first and Eve decides to forward it to Alice with or without any modifications; when Alice receives the packet, she thinks it comes from Bob. The attack is bidirectional, so the same scenario applies when Alice sends a packet to Bob. Initially developed to attack public key encryption systems, this attack has expanded to include any form of eavesdropping in which the attacker acts as a proxy and controls the packets exchanged by the two target nodes.

Follow these steps to evaluate for MitM bugs:

- Step 1: Understand attack scenarios
- Step 2: Analyse causes and countermeasures
- Step 3: Start testing and exploring
- Step 4: Execute additional testing

After following these steps, I found that their might some chance of MiMT attack on the victim. Attacker might change some of the client’s emails to the threatening mail and send that to the victim.

Task 4

Use email forensics analysis and identify the sender’s IP address

Original Message

Message ID <CAP3xXZf1tD8uSjWRKVi6pgpxTZrtoOHWSM2NSORSgvN-cvhWyA@mail.gmail.com>

Created at: Sat, May 20, 2023 at 4:41 PM (Delivered after 11 seconds)

From: Ethical Hacker <ethicalhacker6745@gmail.com>

To: "aman.kumarverma1109@gmail.com" <aman.kumarverma1109@gmail.com>

Subject: Threat

SPF: PASS with IP **209.85.220.41**

DKIM: 'PASS' with domain gmail.com

DMARC: 'PASS'

```
Delivered-To: aman.kumarverma1109@gmail.com

Received: by 2002:a05:6a10:2927:b0:2d6:7c6c:36ce with SMTP id in39csp170221pxb;

       Sat, 20 May 2023 04:41:17 -0700 (PDT)

X-Received: by 2002:a1c:5408:0:b0:3a5:5380:1f0c with SMTP id i8-20020a1c5408000000b003a553801f0cmr4705749wmb.22.1660818076981;

       Sat, 20 May 2023 04:41:16 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; t=1660818076; cv=none;

       d=google.com; s=arc-20160816;

       b=AFEmTWVqNrH8G1vMf3JJWRRoCGppO+Lh1YnTUzPyoL70JWbDPObw4oT2cGDJByMMBy

        sTSJ0ZpCWXIW0sdq6jDDWW2nbakRxGodUStWH6Hq4Eiqu2iIQarcy/aQ4c3tKZnEHNME

        xhDJhgE+kBIJIT2AazauDfWDLPiS6X7BhO0qMTuL7DAt4dLI+lUrhLs4Tq1TtBzHScyV

        1siANn/Zl29l5bERdUJrPagMeL6aAM5Qnr3VTSNnD4J2PIkMJx5GelMO2OxPavZEeUxl

        hZ2w/85l7ofLiTU6tGdZI/5ufjciQ5m+k9LhXmch6HqqOihD7DP03Obl42QtIdS8awGO

        oB3A==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
```

```
        h=to:subject:message-id:date:from:mime-version:dkim-signature;

        bh=Q0htjMuvaisa0jDuMOrdvjOypYXTaxH+xEQKpufTMqc=;

        b=ZffRk0wmQ4PFjkBkeaPyJraSdOgdidmaslIbUFO3r07AQl/Ih233HMUwMCTcKpZJ7D

         VW+D3Snu34Vgvv19Vo4fEs7zw6e4RI5m4DDzghoL4UmXzmZysIHg84YJdU9Dgwg006fs

         ieQdGck/PqsFBIuHBWkSkbd//MlP4z6WjNUbFG+uL8L04KA1vb8jWJNPfN/1ez8HzxN2

         f+TS+bIb4Q2FQZv7jLOiNXS+gezhBW1wtc6Lg6TAdwcClyXU1n7MktgDOb1D+tnP6WM9

         Nhmv8j2U7a0EApml8dGsOW8sJMcoqSVRY+g7tHtFmxpWOkpdyS/VOQOwZkCd2EI+C2Fr

         9JLg==

ARC-Authentication-Results: i=1; mx.google.com;

       dkim=pass header.i=@gmail.com header.s=20210112 header.b=gIe5vWLn;

       spf=pass (google.com: domain of ethicalhacker6745@gmail.com designates 209.85.220.41 as
permitted sender) smtp.mailfrom=ethicalhacker6745@gmail.com;

       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com

Return-Path: <ethicalhacker6745@gmail.com>

Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])

        by mx.google.com with SMTPS id i16-
20020a05600c401000b003a5c10d264esor1052745wmm.37.2022.08.18.03.21.16

        for <sahusk104@gmail.com>

        (Google Transport Security);

        Sat, 20 May 2023 04:41:16 -0700 (PDT)

Received-SPF: pass (google.com: domain of ethicalhacker6745@gmail.com designates 209.85.220.41
as permitted sender) client-ip=209.85.220.41;

Authentication-Results: mx.google.com;

       dkim=pass header.i=@gmail.com header.s=20210112 header.b=gIe5vWLn;

       spf=pass (google.com: domain of ethicalhacker6745@gmail.com designates 209.85.220.41 as
permitted sender) smtp.mailfrom=ethicalhacker6745@gmail.com;

       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

        d=gmail.com; s=20210112;

        h=to:subject:message-id:date:from:mime-version:from:to:cc;

        bh=Q0htjMuvaisa0jDuMOrdvjOypYXTaxH+xEQKpufTMqc=;

        b=gIe5vWLnc352T/9BBl5a8P6JoXmPEmgHYUf/vGeAFLj5u3LvO1SgEC/daFiac550Wl
         XHWzZi1RCzPftJjM+JXOkCfwumhNlGRRwiJvkueYTizAFYmvK3MuXqUIIRvdPHQSoqcv
         omShuOeBQp7NtNv8tyEIm1GwodPd99DAIciJmQ9TrlkD7KRyavDnnagTVW1ckNO8EmjZ
         Ehym9UexwJjAKr8US2torfjoLXOBsLMQgQXBxZTlLayMZOqPzaHZ25WBoXGoJhWLeSqq
         KAd/kovCf75iio2pMerAyaopux3eeC6K2OJQ54cf9Pp8itLDp6mUyQFSRLvu9DCmnfDp
         jwjQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

       d=1e100.net; s=20210112;
        h=to:subject:message-id:date:from:mime-version:x-gm-message-state
         :from:to:cc;
        bh=Q0htjMuvaisa0jDuMOrdvjOypYXTaxH+xEQKpufTMqc=;
        b=AHVxTsugRah/KPGfKRYBeo/9lcaOIL0B6Ltv93Si3sc0Byps8XXzTb3C2OSOA3HDdo
         sxlYwZqUPgcceunMU3geh4YB/+n4SzX1hJkVwSYQkCer5oow7jvVrMKnFozEoP4rZjqY
         nqqMXvTfjmZTfyphxNXhuZXGYNkqsCaRm6xEFUs8LQAfsxEVg2zm9/FqAaHHqzO0jLQq
         UveFcC0yhP1iaW24qENTwp4BFh3T1dzgsQ5kSHcd7siduhj5nw7E8etJcR8FNLwVnA6P
         1vz6PTte1LHhmWKTcC3n1QeO0lSqUolv6by3MUt15SA+5WMQE6x9BSOdY2tsnDe+Jzse
         92zg==
X-Gm-Message-State: ACgBeo1/AwGqx1QOuBjTMGfKs35nKj2X/Hc9oVgSTwO6LuKs6/MAF/0C
B70UidNjHiHM5VRXqoE9fCd939rgyXnJ441IXNcmKtgq5aBOWg==
X-Google-Smtp-Source:
AA6agR7W/7XuH7nYHGJ9aDAh0l/6ZYkSMzk9qzaWvirXcaph1E2687c50SJJUS0/lHI63O/HLwpSZoQMS
1O1cBuAo8I=
X-Received: by 2002:a7b:c38e:0:b0:3a5:c383:c68 with SMTP id s14-
20020a7bc38e000000b003a5c3830c68mr1414690wmj.163.1660818076536; Thu, 18 Aug 2022
03:21:16 -0700 (PDT)
MIME-Version: 1.0
From: Ethical Hacker <ethicalhacker6745@gmail.com>
Date: Sat, 20 May 2023 15:51:05 +0530
Message-ID: <CAP3xXZf1tD8uSjWRKVi6pgpxTZrtoOHWSM2NSORSgvN-cvhWyA@mail.gmail.com>
Subject: Threat
To: " aman.kumarverma1109@gmail.com " <aman.kumarverma1109@gmail.com>
Content-Type: multipart/alternative; boundary="0000000000007d152205e6815757"
```

```
--0000000000007d152205e6815757

Content-Type: text/plain; charset="UTF-8"


Hello,

I have some private pictures of you and your boy-friend. If you send me

10000$, then I will delete these pictures or I will post them in public.

Thank you. Regards Hacker


--0000000000007d152205e6815757

Content-Type: text/html; charset="UTF-8"


Content-Transfer-Encoding: quoted-printable


<div dir=3D"ltr">Hello,<div>I have some private pictures of you and your=C2=

=A0boy-friend. If you send me 10000$, then I will delete these pictures or =

I will post them in public.</div><div>Thank you. Regards Hacker</div></div>


--0000000000007d152205e6815757—
```

This is what I found after doing email forensics. The IP Address of the sender is **209.85.220.41.**