**Information Security:**

**Assignment 3**

***Background***

Windows event logs contain useful information related to a system, its security, the

applications on it, etc. Detailed examination of these logs helps investigators discover

potential artifacts and construct a timeline for the analysis of events based on the logging

information.

Suppose the attacker infiltrated the security of computer system at an office. The attackers

made certain changes to the hardware configurations of the system, services running on the

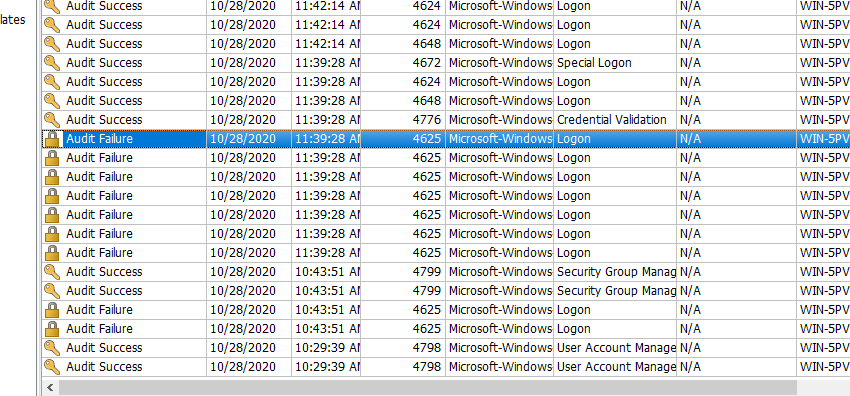
system, operating system, and some other critical programs running on that system to steal

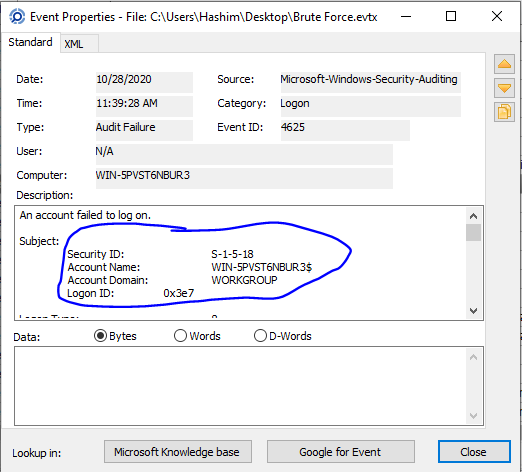
sensitive information. As a forensic investigator, you would examine all the event logs

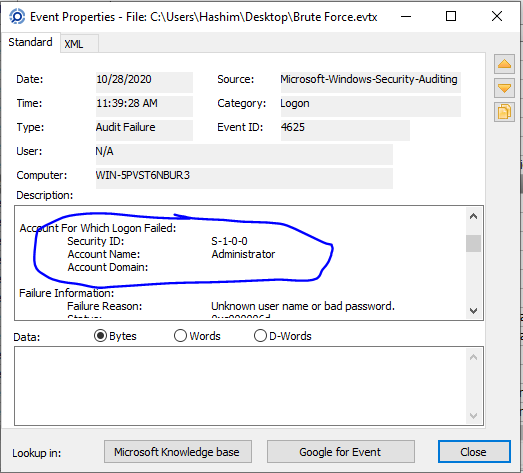
pertaining to the affected system, which include security logs, system logs, and application

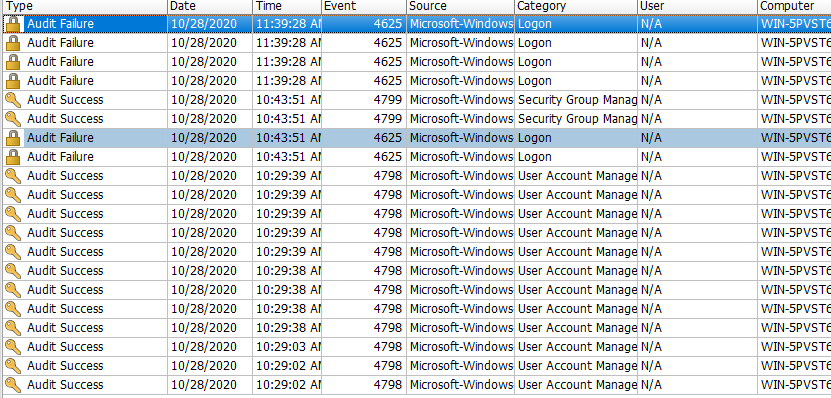
logs, to understand and analyze how this case of cyber-crime was perpetrated.

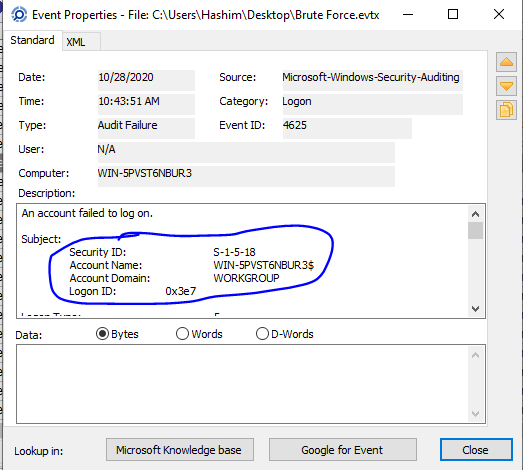
Part 1:

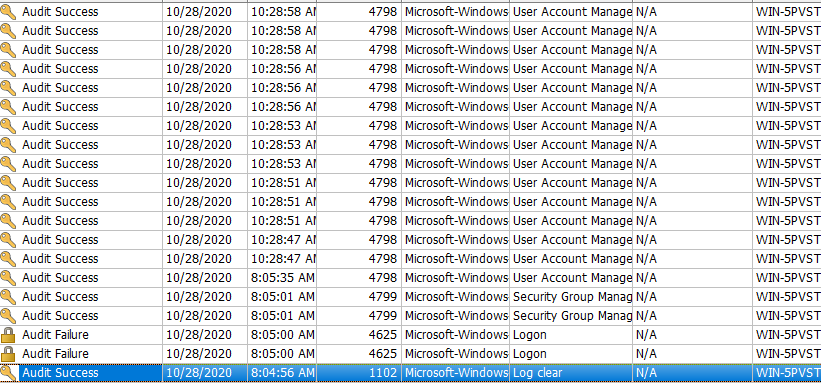
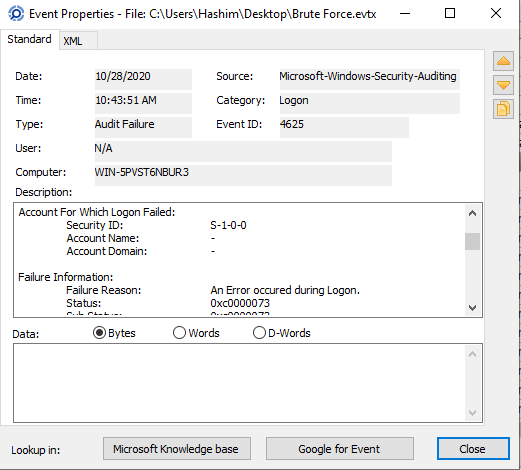
****

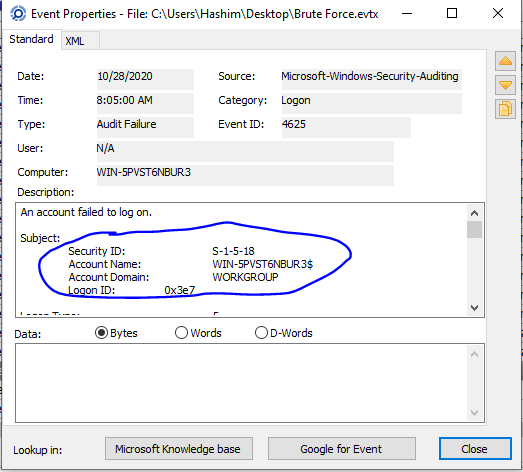
****

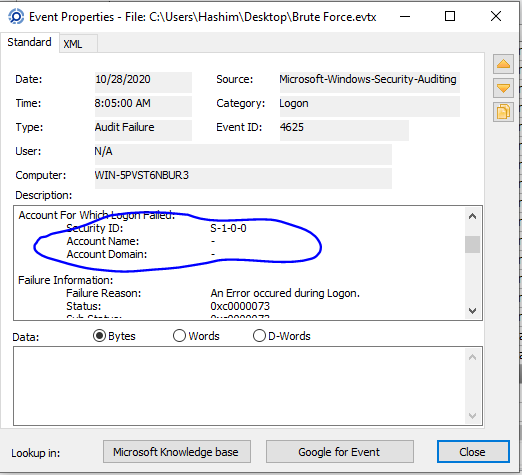
****

****

****

****

****

****

**Part B:**

Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-07 15:36 EST

NSE: Loaded 156 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 15:36

Completed NSE at 15:36, 0.00s elapsed

Initiating NSE at 15:36

Completed NSE at 15:36, 0.00s elapsed

Initiating NSE at 15:36

Completed NSE at 15:36, 0.01s elapsed

Initiating Ping Scan at 15:36

Scanning 192.168.10.15 [2 ports]

Completed Ping Scan at 15:36, 0.00s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 15:36

Completed Parallel DNS resolution of 1 host. at 15:36, 0.00s elapsed

Initiating Connect Scan at 15:36

Scanning debian.home (192.168.10.15) [1000 ports]

Discovered open port 80/tcp on 192.168.10.15

Discovered open port 3306/tcp on 192.168.10.15

Discovered open port 22/tcp on 192.168.10.15

Completed Connect Scan at 15:36, 0.12s elapsed (1000 total ports)

Initiating Service scan at 15:36

Scanning 3 services on debian.home (192.168.10.15)

Completed Service scan at 15:36, 6.65s elapsed (3 services on 1 host)

NSE: Script scanning 192.168.10.15.

Initiating NSE at 15:36

Completed NSE at 15:36, 1.12s elapsed

Initiating NSE at 15:36

Completed NSE at 15:36, 0.13s elapsed

Initiating NSE at 15:36

Completed NSE at 15:36, 0.01s elapsed

Nmap scan report for debian.home (192.168.10.15)

Host is up (0.00068s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.4p1 Debian 5 (protocol 2.0)

| ssh-hostkey:

| 3072 0e:77:d9:cb:f8:05:41:b9:e4:45:71:c1:01:ac:da:93 (RSA)

| 256 40:51:93:4b:f8:37:85:fd:a5:f4:d7:27:41:6c:a0:a5 (ECDSA)

|\_ 256 09:85:60:c5:35:c1:4d:83:76:93:fb:c7:f0:cd:7b:8e (ED25519)

80/tcp open http Apache httpd 2.4.48 ((Debian))

|\_http-favicon: Unknown favicon MD5: B0BD48E57FD398C5DA8AE8F2CCC8D90D

|\_http-title: qdPM | Login

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-server-header: Apache/2.4.48 (Debian)

3306/tcp open mysql MySQL 8.0.26

| mysql-info:

| Protocol: 10

| Version: 8.0.26

| Thread ID: 12

| Capabilities flags: 65535

| Some Capabilities: Support41Auth, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, SupportsCompression, SupportsLoadDataLocal, LongPassword, InteractiveClient, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ODBCClient, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, LongColumnFlag, FoundRows, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults

| Status: Autocommit

| Salt: O\x17\x12)a\x14J\x0D"sobl\x04\x12\x0CF){\x13

|\_ Auth Plugin Name: caching\_sha2\_password

|\_ssl-date: ERROR: Script execution failed (use -d to debug)

| ssl-cert: Subject: commonName=MySQL\_Server\_8.0.26\_Auto\_Generated\_Server\_Certificate

| Issuer: commonName=MySQL\_Server\_8.0.26\_Auto\_Generated\_CA\_Certificate

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2021-09-25T10:47:29

| Not valid after: 2031-09-23T10:47:29

| MD5: 5b43:7361:8d5b:1938:656d:44a3:4e07:bbcc

|\_SHA-1: 5d26:f9ad:743c:f316:6aa5:32ae:fdf8:2571:bb44:91c3

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

NSE: Script Post-scanning.

Initiating NSE at 15:36

Completed NSE at 15:36, 0.01s elapsed

Initiating NSE at 15:36

Completed NSE at 15:36, 0.00s elapsed

Initiating NSE at 15:36

Completed NSE at 15:36, 0.01s elapsed

Read data files from: /usr/bin/../share/nmap

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

Nmap done: 1 IP address (1 host up) scanned in 9.32 seconds

***Conclusion:***

The scan involves multiple steps, starting with script pre-scanning, ping scanning, parallel DNS resolution, connect scanning of 1000 ports on the host, and subsequent service scanning. The results reveal open ports (22/SSH, 80/HTTP, 3306/MySQL), along with version information and service details such as OpenSSH 8.4p1 Debian 5, Apache httpd 2.4.48 (Debian), and MySQL 8.0.26. The log also includes additional information such as SSL certificate details for the MySQL service, operating system detection (Linux), and the completion time of the scan. The NSE (Nmap Scripting Engine) is employed for pre-scanning and post-scanning tasks, providing additional insights into the target system. Overall, the log provides a comprehensive snapshot of the scanned host's network services, their versions, and other relevant details obtained through Nmap's diverse scanning capabilities.