

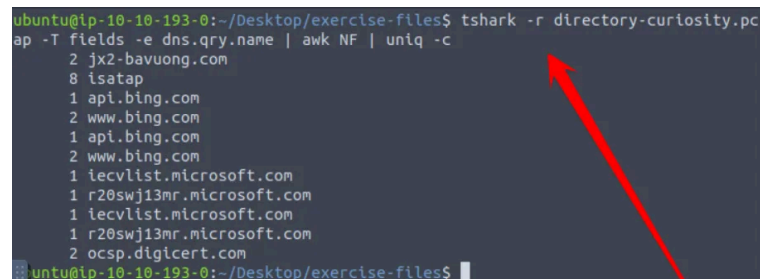
TShark Project: Active Directory Analysis

Objective: Investigate network traffic to confirm an alert regarding malicious activity triggered by a curious user accessing a poor file index.

Key Steps and Active Directory Experience

1. DNS Query and Domain Analysis:

- Inspected DNS queries to identify suspicious activity.
- Verified the flagged domain ([jx2-bavuong\[.\]com](http://jx2-bavuong.com)) using VirusTotal, confirming its malicious status.

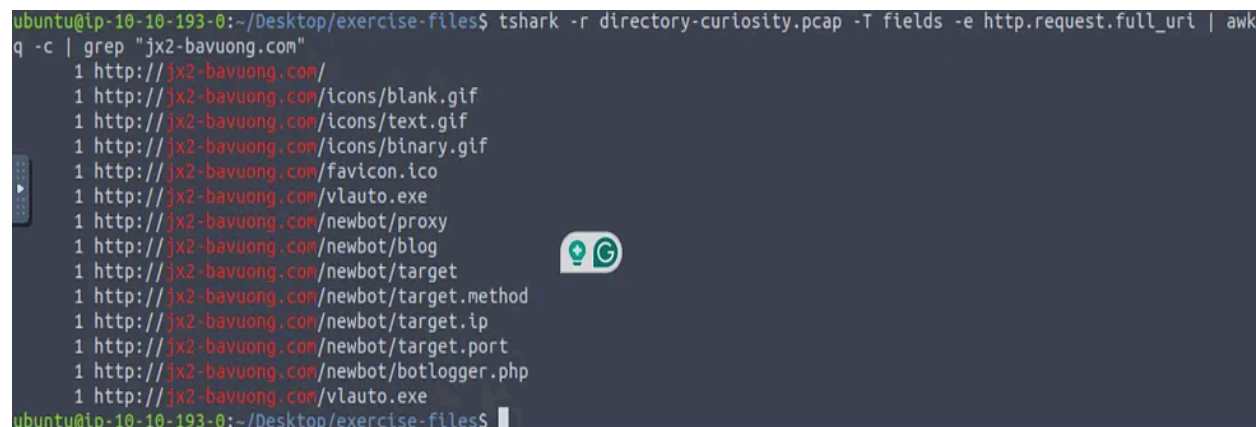


```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -T fields -e dns.qry.name | awk NF | uniq -c
  2 jx2-bavuong.com
  8 isatap
  1 api.bing.com
  2 www.bing.com
  1 api.bing.com
  2 www.bing.com
  1 iecvlist.microsoft.com
  1 r20swj13mr.microsoft.com
  1 iecvlist.microsoft.com
  1 r20swj13mr.microsoft.com
  2 ocspl.digicert.com
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

just a simple dns query
extraction command. And
here is the first link as
malicious

2. HTTP Traffic Inspection:

- Analyzed HTTP requests to determine 14 total requests to the malicious domain.
- Followed the first TCP stream to extract file information, identifying suspicious files like [123\[.\]php](http://123[.]php).



```
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -T fields -e http.request.full_uri | awk 'q -c | grep "jx2-bavuong.com"'
  1 http://jx2-bavuong.com/
  1 http://jx2-bavuong.com/icons/blank.gif
  1 http://jx2-bavuong.com/icons/text.gif
  1 http://jx2-bavuong.com/icons/binary.gif
  1 http://jx2-bavuong.com/favicon.ico
  1 http://jx2-bavuong.com/vlauto.exe
  1 http://jx2-bavuong.com/newbot/proxy
  1 http://jx2-bavuong.com/newbot/blog
  1 http://jx2-bavuong.com/newbot/target
  1 http://jx2-bavuong.com/newbot/target.method
  1 http://jx2-bavuong.com/newbot/target.ip
  1 http://jx2-bavuong.com/newbot/target.port
  1 http://jx2-bavuong.com/newbot/botlogger.php
  1 http://jx2-bavuong.com/vlauto.exe
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$
```

3. File Extraction and Malware Investigation:

- Exported HTTP traffic objects using TShark to recover a downloaded executable file (v1auto[.]exe).

```

ubuntu@ip-10-10-193-0: ~/Desktop/exercise-files
File Edit View Search Terminal Help
Date: Sun, 13 Dec 2020 00:51:46 GMT
Server: Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
Last-Modified: Sat, 20 Nov 2004 13:16:24 GMT
ETag: "20000000053c6-94-3e9506e1a3a00"
Accept-Ranges: bytes
Content-Length: 148
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/gif

GIF89a.....!.NThis art is in the public domain. Kevin Hughes, kevinh@eit.com, September
1995.!.....,.....I..;
=====
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap export-objects htt
p,/home/ubuntu/Desktop/exercise-files -q
tshark: Syntax error near "http".
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ pwd
/home/ubuntu/Desktop/exercise-files
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap export-objects htt
p,/home/ubuntu/Desktop/exercise-files -q
tshark: Syntax error near "http".
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap --export-objects h
tp,/home/ubuntu/Desktop/exercise-files -q

```

- Found the file's SHA256 hash and used VirusTotal to confirm it as malware (MALWARE TROJAN).

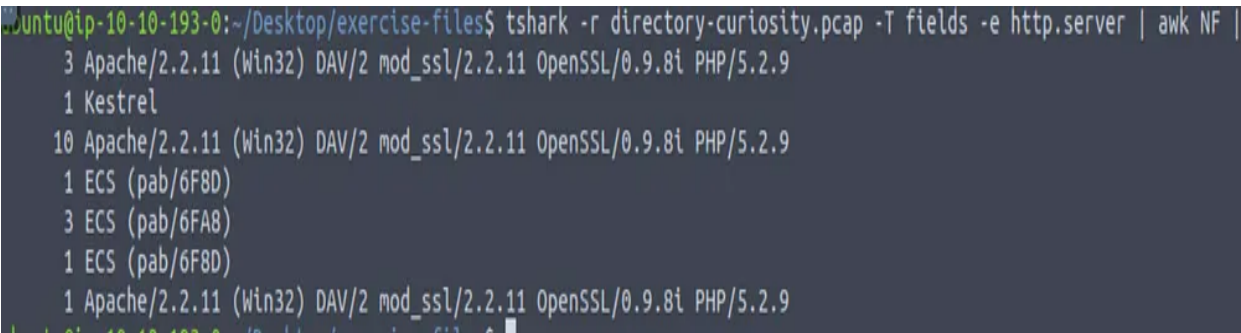
```

ubuntu@ip-10-10-193-0: ~/Desktop/exercise-files
File Edit View Search Terminal Help
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ sha256sum v1auto
sha256sum: v1auto: No such file or directory
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$ sha256sum v1auto.exe
d4851333e7a1399889450f78eac0f0532e908/91023a80a19402c1104aed020de v1auto.exe
ubuntu@ip-10-10-193-0:~/Desktop/exercise-files$

```

4. Server Analysis:

- Retrieved server information for the suspicious domain, noting it ran outdated and vulnerable software (Apache/2.2.11, PHP/5.2.9).

○ A terminal window showing the output of a TShark command. The command is: tshark -r directory-curiosity.pcap -T fields -e http.server | awk NF |. The output lists the HTTP server information for several connections. The first connection is from 10.10.10.10 to 10.10.10.10, identified as Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9. The second connection is from 10.10.10.10 to 10.10.10.10, identified as Kestrel. The third connection is from 10.10.10.10 to 10.10.10.10, identified as Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9. The fourth connection is from 10.10.10.10 to 10.10.10.10, identified as ECS (pab/6F8D). The fifth connection is from 10.10.10.10 to 10.10.10.10, identified as ECS (pab/6FA8). The sixth connection is from 10.10.10.10 to 10.10.10.10, identified as ECS (pab/6F8D). The seventh connection is from 10.10.10.10 to 10.10.10.10, identified as Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9.

Active Directory Experience Gained

- Investigated traffic originating from and targeting Active Directory services.
- Correlated DNS queries and HTTP traffic with potential compromises in user access behavior.
- Strengthened understanding of how compromised endpoints in a directory service environment can escalate security risks.

Conclusion

This project demonstrated my ability to analyze packet captures using TShark, identify malicious activity, and investigate network-based threats. It reinforced my skills in working with DNS, HTTP, and Active Directory logs to confirm alerts and assess malware risks.