Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

tsharkchallengesone – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | tsharkchallengesone – Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/10/2024 |
| **Link** | https://tryhackme.com/r/room/tsharkchallengesone |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico Santarelli | Membro |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 02/10/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

Contextualização 3

Desenvolvimento 3

What is the full URL of the malicious/suspicious domain address 3

When was the URL of the malicious/suspicious domain address first submitted to VirusTotal? 3

Which known service was the domain trying to impersonate? 4

What is the IP address of the malicious domain? 5

What is the CyberChef defanged URL of the malicious download

location first seen on 2020-11-02? 5

What is the email address that was used? 6

Conclusão 7

Referências 7

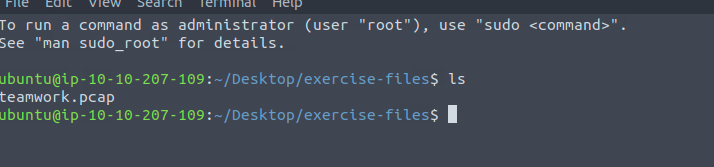
**Contextualização**

O CTF compões a trilha de SOC Level 1. A ideia da sala é treinar as habilidades de análise de pacotes de tráfego de rede utilizando a ferramenta TShark.

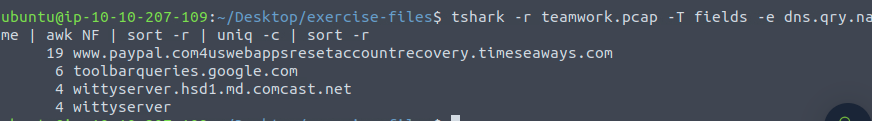
**Desenvolvimento**

**What is the full URL of the malicious/suspicious domain address?**

O arquivo a ser investigado na sala está na pasta ~/Desktop/exercise-files e se chama teamwork.pcap.

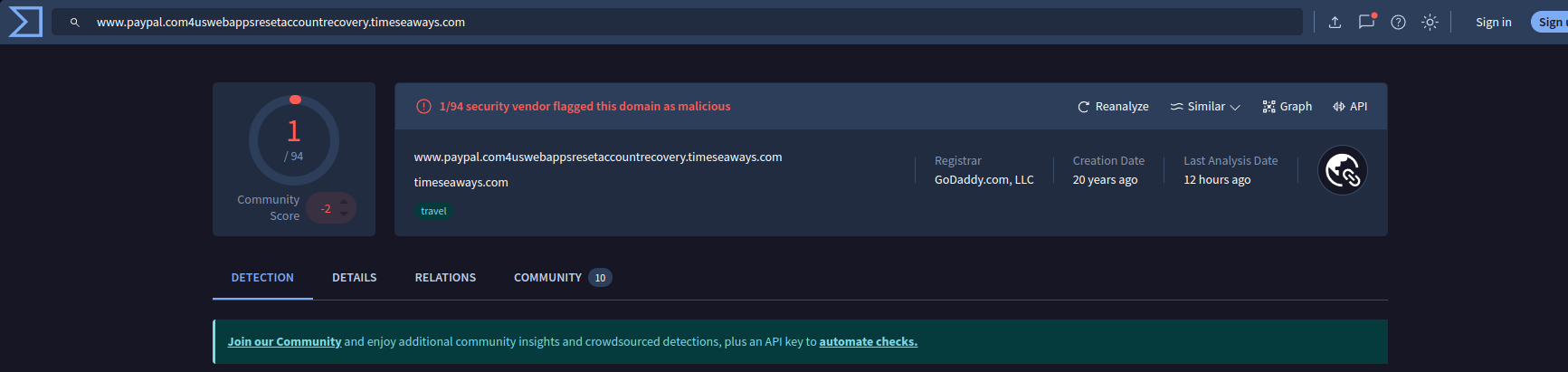


Para filtrar os nomes dos domínios no arquivo de tráfego, podemos utilizar um filtro que busca por campos extrai o campo de domínio (flag –e) e filtra por linhas únicas.



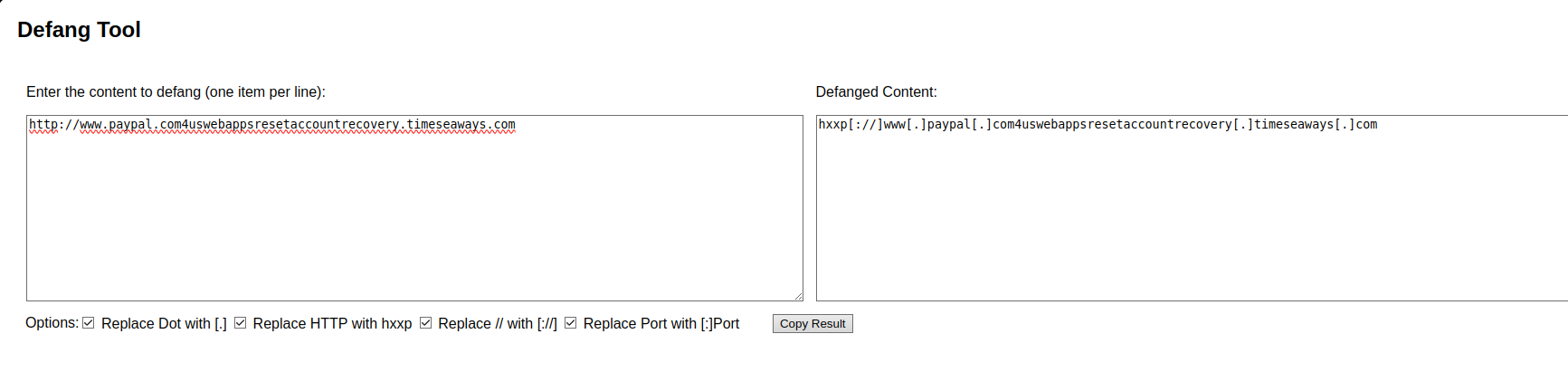
O resultado indica que o domínio [www.paypal.com4uswebappsresetaccountrecovery.timeseaways.com](http://www.paypal.com4uswebappsresetaccountrecovery.timeseaways.com) é suspeito, já que contém 19 aparições.

Utilizando o VirusTotal, o domínio é indicado como suspeito por um vendor. Ref: <https://www.virustotal.com/gui/domain/www.paypal.com4uswebappsresetaccountrecovery.timeseaways.com>.



Realizando o defang da URL pelo defa.ng nós obtemos a resposta da primeira questão. Ref: https://defa.ng

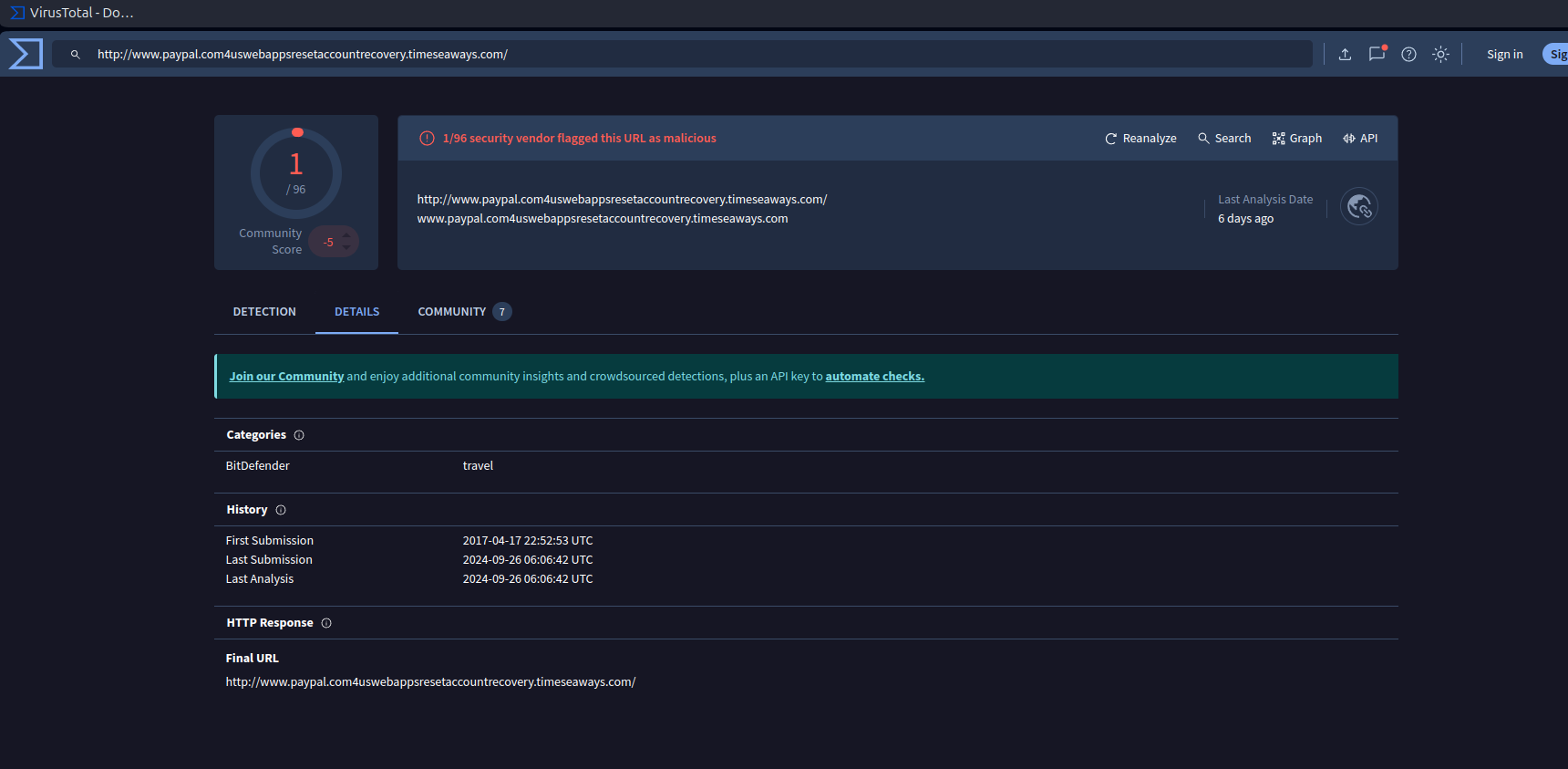
OBS: A questão pede a URL com o protocolo de comunicação web, portanto é necessário adicionar o http:// antes de fazer o defang.



R: hxxp[://]www[.]paypal[.]com4uswebappsresetaccountrecovery[.]timeseaways[.]com.

**What was the URL of the malicious/suspicious domain address first submitted to VirusTotal.**

Dentro do mesmo link do VirusTotal da questão anterior, encontra-se a data procurada na aba de "Details" no campo de "History" em "First Submission". Ref: <https://www.virustotal.com/gui/url/16db0aadc2423a67cd3a01af39655146b0f15d20dc2fd0e14b325026d8d1717e/details>.



R: 2017-04-17 22:52:53 UTC.

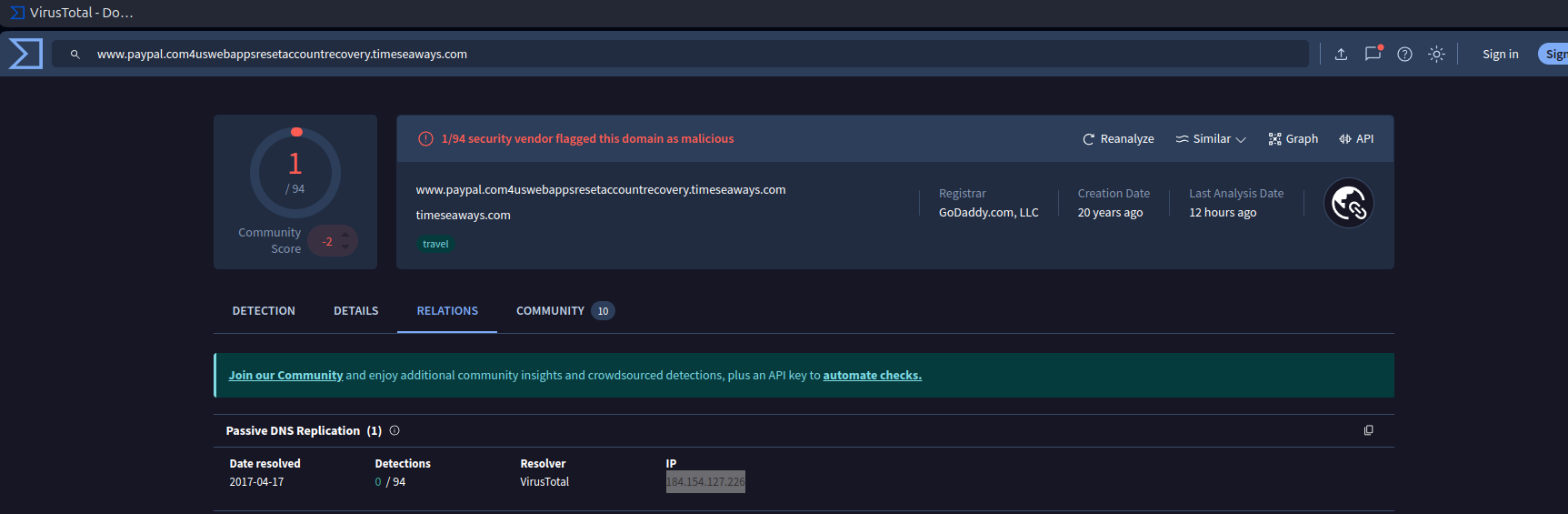
**Which known service was the domain trying to impersonate.**

A resposta para essa pergunta se dá pela observação da URL verificando que o termo "paypal" nela. Assim, concluindo que o domínio tenta imitar esse serviço de pagamento digital.

R: PayPal.

**Which known service was the domain trying to impersonate.**

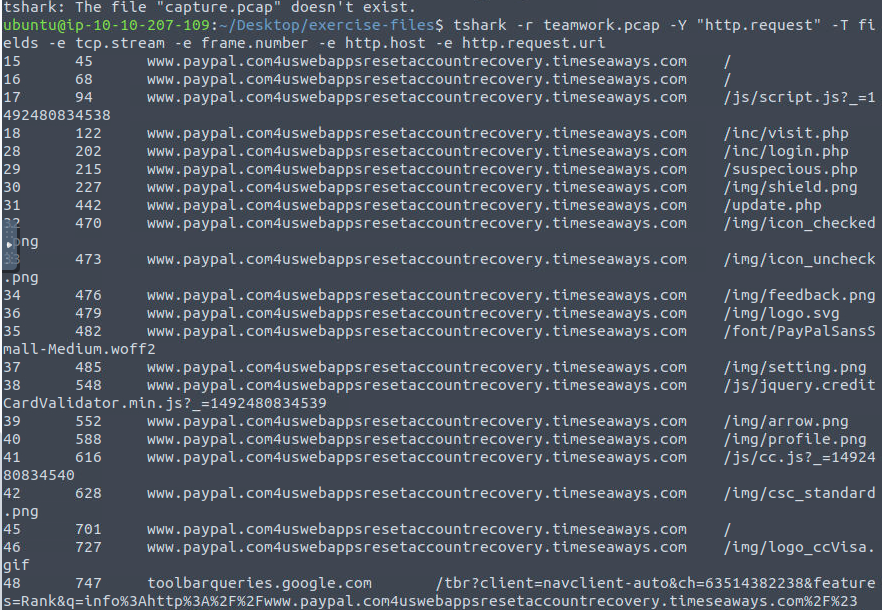
O VirusTotal também possuí uma aba de "Relations" que mostra as resoluções DNS feitas para o domínio, logo podemos usar a plataforma para a questão.



R: 184.154.127.226

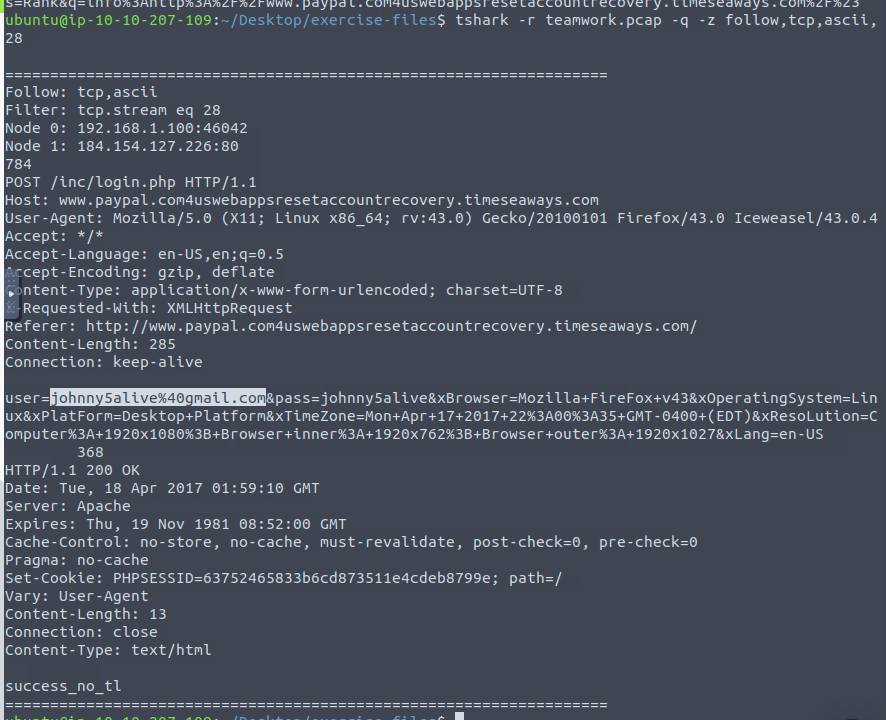
**What is the email adderss that was used?**

Primeiro, vamos rellizar uma leitura para procurar as requisições http e exibir o número do fluxo tcp do pacote, ele será usado para filtrar e fazer o follow sobre o pacote.



Vamos explorar o conteúdo da requisição do login que pode conter emails. Para isso salvamos o número 28 da stream TCP.

Fazendo o Follow sobre o pacote em questão, encontramos o email no corpo da request de login.



Do e-mail é necessário realizar o processo de Defang manualmente, trocando o @ por [at] e o . por [.].

R: johnny5alive[at]gmail[.]com

**Conclusão**

Este CTF oferece uma experiência prática de nível fácil, ideal para iniciantes na área de Blue Team que desejam colocar em prática os aprendizados de análise de pacote. Uma indiicação é realizar estudos a respeito da ferramenta TShark antes de trabalhar com o CTF.

**Referências**

* <https://defa.ng>.
* <https://virustotal.com>.