

index

November 20, 2024

1 Executa a extração de arquivos http usando o TSHARK

```
[ ]: rm output_directory -rf  
tshark -r pass.pcap --export-objects http,output_directory
```

```
[ ]: open System  
open System.IO
```

```
[ ]: let directoryPath = "output_directory"
```

2 Decode URI

```
[ ]: Directory.GetFiles(directoryPath)  
|> Array.mapi (fun index file -> index, Uri.UnescapeDataString(Path.  
    ↳ GetFileName(file)))  
|> Array.iter (fun (index, fileName) -> printfn "%d: %s" index fileName)
```

```
[ ]: Directory.GetFiles(directoryPath).[6] |> File.ReadAllText |> printfn "%s"
```

3 Quebrando o Hash Encontrado em “6: cat.php?id=-1 union select 1,concat(id,0x3a,login,0x3a,password),3,4 from users”

```
[ ]: hashcat -m 0 -a 0 -o cracked.txt hash.txt /usr/share/wordlists/rockyou.txt > /  
    ↳ dev/null  
hashcat -m 0 --show hash.txt
```