Midterm
SYS-320
Ben W
SP24

Deliverables:

1. Table scraping

```powershell
function scrapeTable {

    $page= Invoke-WebRequest 10.0.17.5/IOC.html

    $trs = $page.ParsedHtml.body.getElementsByTagName("tr")

    # Empty array to hold results
    $FullTable = @()


    for ($i=1; $i -lt $trs.length; $i++) {
        # Get every td element of current tr element
        $tds = $trs[$i].getElementsByTagName("td")

        $FullTable += [pscustomobject]@{"Pattern"     = $tds[0].innerText;
                                        "Description" = $tds[1].innerText;
                                       }

    }

    return $FullTable

}
```

```
PS C:\Users\champuser\Documents\sys320git\PowershellLabs\Midterm> C:\Users\champus

Pattern    Description
-------    -----------
etc/passwd Access attempt to Linux users list
cmd=       Windows reverse shell attempt
/bin/bash  Linux shell attempt
/bin/sh    Linux shell attempt
1=1#       SQL injection attempt
1=1--      SQL injection attempt
```

2. Parsing logs

```powershell
cd $PSScriptRoot

function accessLogs($file) {

    $rawLog = Get-Content $file

    # IP, Time, Method, Page, Protocol, Response, Referrer

    $regex = [regex] "^(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*"

    $ips = $regex.Matches($rawLog)

    # Empty array to hold results
    $FullTable = @()

    for ($i=0; $i -lt $rawLog.Count; $i++) {

        $log = $rawLog[$i].Split(" ")

        $FullTable += [pscustomobject]@{"      IP" = $log[0];
                                        "    Time" = $log[3].Trim('[');
                                        "  Method" = $log[5].Trim('"');
                                        "    Page" = $log[6];
                                        "Protocol" = $log[7];
                                        "Response" = $log[8];
                                        "Referrer" = $log[10];
                                       }


    }

    return $FullTable | Format-Table -AutoSize -Wrap
}

accessLogs ./access.log
```

```
      IP      Time              Method     Page                                                  Protocol  Response Referrer
-------- --------              -------- --------                                                  --------  -------- --------
10.0.17.5 04/Mar/2024:13:28:46 GET      /index.html                                             HTTP/1.1" 404      "-"
10.0.17.5 04/Mar/2024:13:29:21 GET      /index.html                                             HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:42:42 GET      /index.php                                              HTTP/1.1" 404      "-"
10.0.17.5 04/Mar/2024:14:43:07 GET      /index.php                                              HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:43:21 GET      /index.php?a=1&b=2                                      HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:43:50 GET      /index.php?cmd=etc/passwd                               HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:44:19 GET      /index.php?cmd=cat+etc/passwd                           HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:44:52 GET      /index.php?cmd=/bing/bash+myscript.bash                 HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:45:01 GET      /index.php?cmd=/bin/bash+myscript.bash                  HTTP/1.1" 200      "-"
```

3. I couldn't get this one done, but I got sort of close. I was eventually able to get the printing out to work but could not get the filtering to work.

```powershell
cd $PSScriptRoot

. (Join-Path $PSScriptRoot Challange1.ps1)
. (Join-Path $PSScriptRoot Challange2.ps1)

$LOG = accessLogs .\access.log

$IOC = scrapeTable

#Write-Host ($LOG.Page | Format-Table -AutoSize -Wrap | Out-String)

#$LOG | ? {$_.Page -ilike ("*"+$IOC.Pattern+"*") }

$list = @()

for ($i=0; $i -lt $LOG.Count; $i++) {
    for ($j=0; $j -lt $IOC.Count; $j++) {


        $test = "*" + $IOC[$j].Pattern + "*"
        # eg. "*etc/passwd*"

        Write-Host ($LOG[$i] | Format-Table -AutoSize -Wrap | Out-String) | ? { $_.Page -ilike $test }

        if (($LOG.Page | Out-String) -ilike $test) {

            $list += $Log[$i]
            $j = $IOC.Count
        }

    }
}
Write-Host ($list | Select -Unique IP,Time,Method,Page,Protocol,Response,Referrer | Format-Table -AutoSize -Wrap | Out-String)
```

```
IP          Time                Method Page                                                Protocol  Response Referrer
--          ----                ------ ----                                                --------  -------- --------
10.0.17.5 04/Mar/2024:13:28:46 GET    /index.html                                         HTTP/1.1" 404      "-"
10.0.17.5 04/Mar/2024:13:29:21 GET    /index.html                                         HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:42:42 GET    /index.php                                          HTTP/1.1" 404      "-"
10.0.17.5 04/Mar/2024:14:43:07 GET    /index.php                                          HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:43:21 GET    /index.php?a=1&b=2                                  HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:43:50 GET    /index.php?cmd=etc/passwd                           HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:44:19 GET    /index.php?cmd=cat+etc/passwd                       HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:44:52 GET    /index.php?cmd=/bing/bash+myscript.bash             HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:45:01 GET    /index.php?cmd=/bin/bash+myscript.bash              HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:45:19 GET    /index.php?cmd=/bin/sh+simplebackdoor.bash          HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:45:31 GET    /index.php?/bin/sh+simplebackdoor.bash              HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:46:03 GET    /index.php?a=1+OR+1=1--                             HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:46:12 GET    /index.php?a=1+OR+1=1-                              HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:46:27 GET    /index.php?a=1+OR+1=1                               HTTP/1.1" 200      "-"
10.0.17.5 04/Mar/2024:14:46:47 GET    /index.php?word=Hello+World                         HTTP/1.1" 200      "-"
10.0.17.6 04/Mar/2024:14:48:39 GET    /                                                   HTTP/1.1" 200      "-"
```

4. Github: https://github.com/benjamin-weatherill/SYS-320/tree/main/PowershellLabs/Midterm