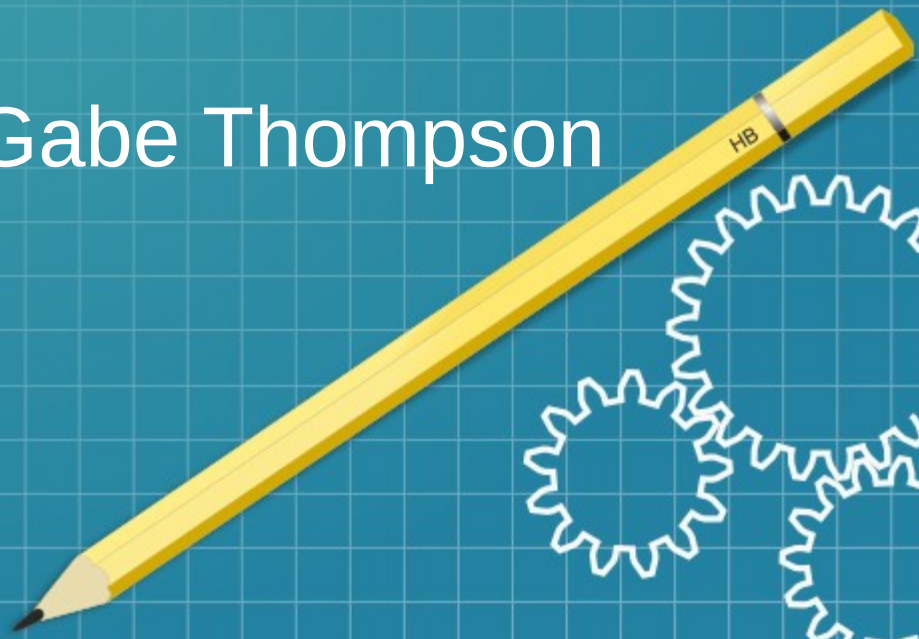
Elevate your Tenable/Nessus Pro game to the next level

By: Eric Schwartz and Gabe Thompson



This is not a sponsored talk.

- Views and opinions are our own, not of Tenable nor our employer.
- Use what you are given.
- The sales person said we could have system wide results in a few days.
- We paid for this so add it to your plate and remember: everything is mission critical.

:~$ whoami

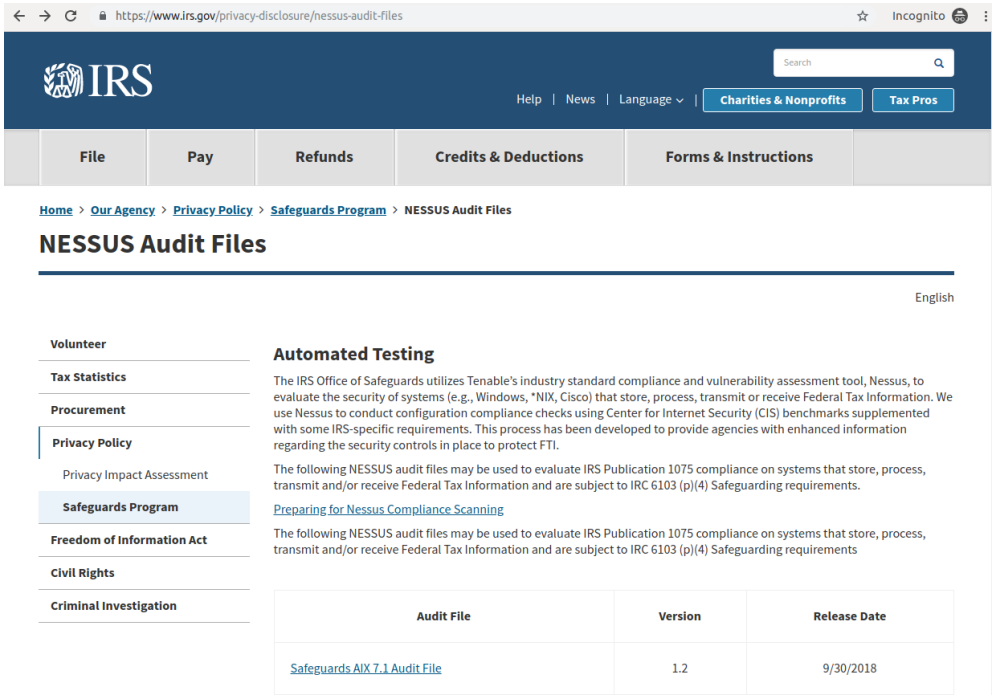
- Security Engineer for U.S. Bank
- Former Elementary School teacher
- Transplant here to MN

:~$ whoami

- Internal Penetration Tester for U.S. Bank
- Master’s degree in Cybersecurity.
- Ultramarathon trail runner

CIS Benchmarks

- Pros:
  - It's a place to start.
  - Better than nothing.
- Cons:
  - Some are simply policy checks, no pass or fail check occurs.
  - Not organization specific.
  - Lack flexibility out of the box.



https://www.irs.gov/privacy-disclosure/nessus-audit-files
https://www.cisecurity.org/partner/tenable/

User Rights Assignment Example 1

```
<custom_item>
  type        : USER_RIGHTS_POLICY
  description : "2.2.11 Ensure 'Create a pagefile' is set to 'Administrators'"
  info        : “Redacted for brevity”
  reference   : "LEVEL|1S,CCE|CCE-35821-8,CSCv6|5.1"
  see_also    :
"https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_Server_2016_RTM_Release%201607_Benchmark_v1.0.0.pdf"
  value_type  : USER_RIGHT
  value_data  : "Administrators"
  right_type  : SeCreatePagefilePrivilege
</custom_item>
```

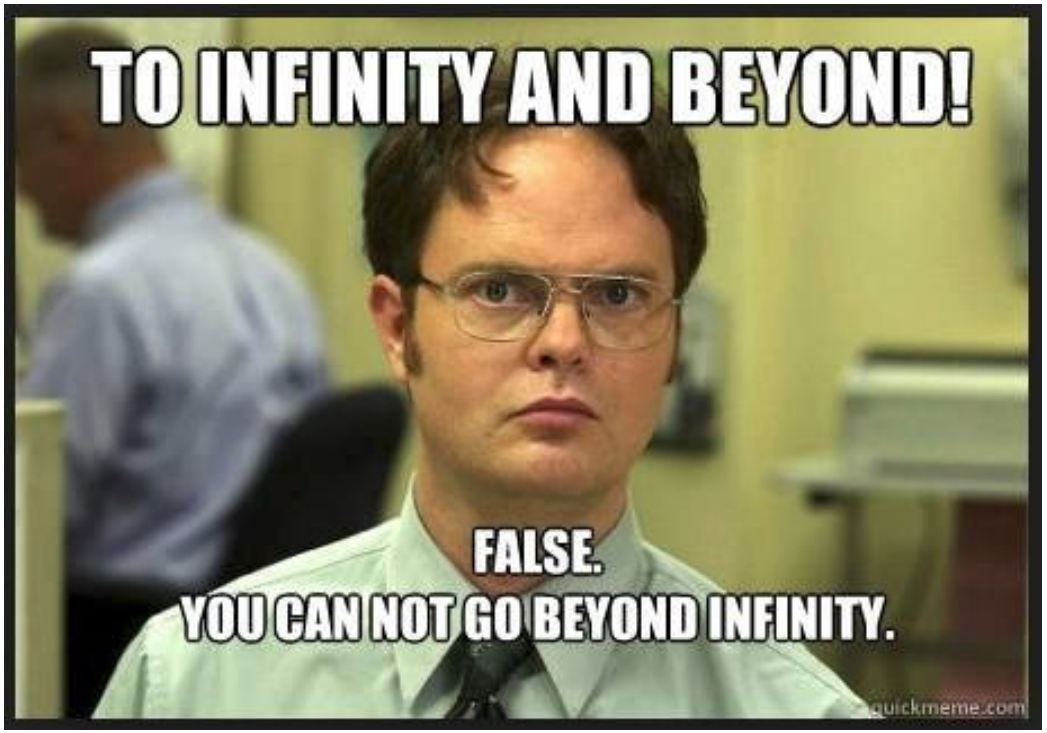
Combinations not Permutations

- Repetition
- No repetition

$$\frac{n!}{r!(n-r)!}$$

Math can be difficult

Combinations of combinations: a,b,c,ab,ac,bc,abc.



User Rights Assignment Example 2

```
# Allow log on through Remote Desktop Services
# Setting: Administrators, Remote Desktop Users
# seremoteinteractivelogonright
<custom_item>
type          : USER_RIGHTS_POLICY
description   : "Allow log on through Remote Desktop
Services"
value_type    : USER_RIGHT
value_data    : ("Remote Desktop Users" ) ||
("Administrators" ) || ("Administrators" && "Remote Desktop
Users")
right_type      : SeRemoteInteractiveLogonRight
info          : ""
    </custom_item>
```

User Rights Assignment Example 3

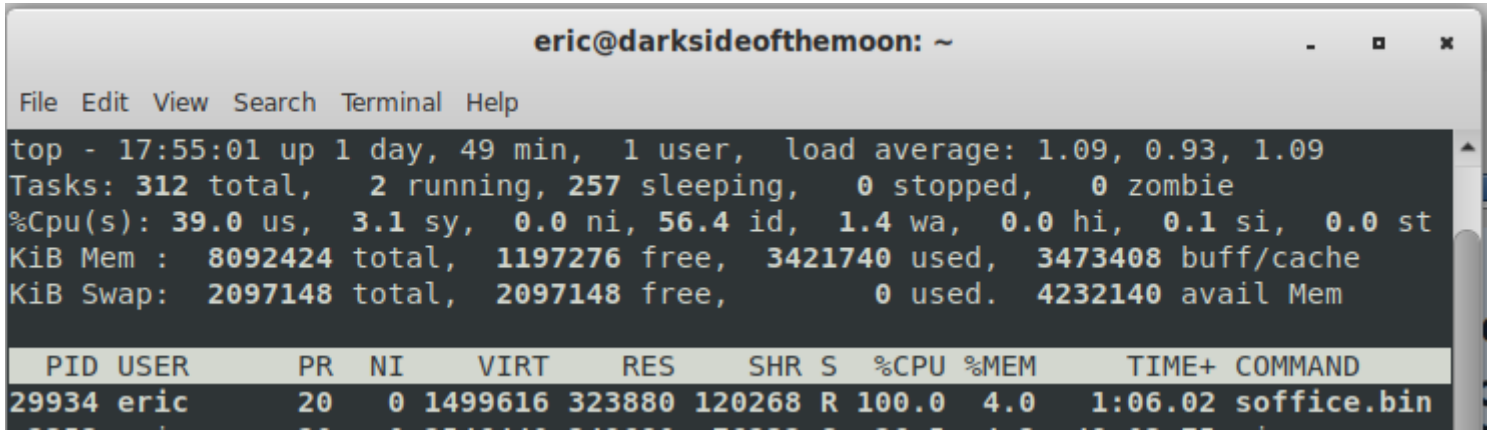
Setting: "Administrators" || "SERVICE" || "Local Service" || "Network Service"
value_data : ("SERVICE") || ("Network Service") || ("Network Service" && "SERVICE") || ("Local Service") || ("Local Service" && "SERVICE") || ("Local Service" && "Network Service") || ("Local Service" && "Network Service" && "SERVICE") || ("Administrators") || ("Administrators" && "SERVICE") || ("Administrators" && "Network Service") || ("Administrators" && "Network Service" && "SERVICE") || ("Administrators" && "Local Service") || ("Administrators" && "Local Service" && "SERVICE") || ("Administrators" && "Local Service" && "Network Service") || ("Administrators" && "Local Service" && "Network Service" && "SERVICE")

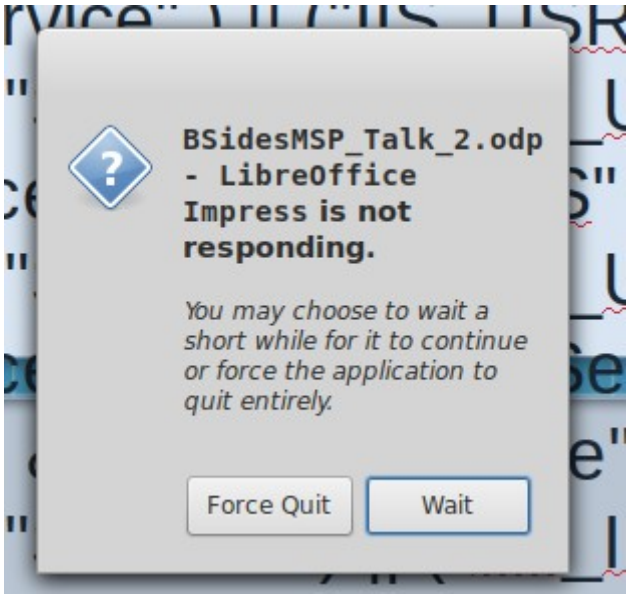
6 Accounts/Groups

value_data : ("") || ("Local_BTC") || ("Network Service") || ("Network Service" && "Local_BTC") || ("Local Service") || ("Local Service" && "Local_BTC") || ("Local Service" && "Network Service") || ("Local Service" && "Network Service" && "Local_BTC") || ("Backup Operators") || ("Backup Operators" && "Local_BTC") || ("Backup Operators" && "Network Service") || ("Backup Operators" && "Network Service" && "Local_BTC") || ("Backup Operators" && "Local Service") || ("Backup Operators" && "Local Service" && "Local_BTC") || ("Backup Operators" && "Local Service" && "Network Service") || ("Backup Operators" && "Local Service" && "Network Service" && "Local_BTC") || ("Authenticated Users") || ("Authenticated Users" && "Local_BTC") || ("Authenticated Users" && "Network Service") || ("Authenticated Users" && "Network Service" && "Local_BTC") || ("Authenticated Users" && "Local Service") || ("Authenticated Users" && "Local Service" && "Local_BTC") || ("Authenticated Users" && "Local Service" && "Network Service") || ("Authenticated Users" && "Local Service" && "Network Service" && "Local_BTC") || ("Authenticated Users" && "Backup Operators") || ("Authenticated Users" && "Backup Operators" && "Local_BTC") || ("Authenticated Users" && "Backup Operators" && "Network Service") || ("Authenticated Users" && "Backup Operators" && "Network Service" && "Local_BTC") || ("Authenticated Users" && "Backup Operators" && "Local Service") || ("Authenticated Users" && "Backup Operators" && "Local Service" && "Local_BTC") || ("Authenticated Users" && "Backup Operators" && "Local Service" && "Network Service") || ("Authenticated Users" && "Backup Operators" && "Local Service" && "Network Service" && "Local_BTC") || ("Administrators") || ("Administrators" && "Local_BTC") || ("Administrators" && "Network Service") || ("Administrators" && "Network Service" && "Local_BTC") || ("Administrators" && "Local Service") || ("Administrators" && "Local Service" && "Local_BTC") || ("Administrators" && "Local Service" && "Network Service") || ("Administrators" && "Local Service" && "Network Service" && "Local_BTC") || ("Administrators" && "Backup Operators") || ("Administrators" && "Backup Operators" && "Local_BTC") || ("Administrators" && "Backup Operators" && "Network Service") || ("Administrators" && "Backup Operators" && "Network Service" && "Local_BTC") || ("Administrators" && "Backup Operators" && "Local Service") || ("Administrators" && "Backup Operators" && "Local Service" && "Local_BTC") || ("Administrators" && "Backup Operators" && "Local Service" && "Network Service") || ("Administrators" && "Backup Operators" && "Local Service" && "Network Service" && "Local_BTC") || ("Administrators" && "Authenticated Users") || ("Administrators" && "Authenticated Users" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Network Service") || ("Administrators" && "Authenticated Users" && "Network Service" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Local Service") || ("Administrators" && "Authenticated Users" && "Local Service" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Local Service" && "Network Service") || ("Administrators" && "Authenticated Users" && "Local Service" && "Network Service" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Backup Operators") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Network Service") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Network Service" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Local Service") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Local Service" && "Local_BTC") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Local Service" && "Network Service") || ("Administrators" && "Authenticated Users" && "Backup Operators" && "Local Service" && "Network Service" && "Local_BTC")

7 Accounts/Groups

- Putting the text for that in here, kills LibreOffice





Using the Power in PowerShell

```
<custom_item>
type: AUDIT_POWERSHELL
description: "Allow Log on as a Service"
value_type: POLICY_TEXT
value_data: "Pass"
powershell_args  : '$allowedArray
= \\"aspnet\\", \\"wsadmin\\", \\"rsa_user0\\", \\"sqladmin\\", \\"mmsservice\\", \\"Local_LOS\\", \\"iOS\\",
\\"user_agent\\", \\"db2admin\\", \\"iis_user999\\", \\"blackberryservice\\", \\"DR_rsa_user0\\", \\"UAT__
rsa_user0\\", \\"All Services\\";$allowedCounter = 0;$objectCounter = 0;$resultSet = gwmi -
Namespace root/rsop/computer -Class RSOP_UserPrivilegeRight -
Filter \\"UserRight=\'seservicelogonright\' and precedence=1\\";$resultSet\.PSObject\.Properties |
foreach{if($_\.Name -eq \\"AccountList\\"){$users = $_\.Value -split \\" \\";}};if($users.Count -gt 0)
{Write-Host $users;foreach ($user in $users){$objectCounter = $objectCounter + 1;foreach($allowed
in $allowedArray){if($user\.ToLower()\.Contains($allowed\.ToLower())){$allowedCounter =
$allowedCounter + 1;}}};}if($allowedCounter -ge $objectCounter){Write-Host \\"Pass\\";};'
check_type : CHECK_REGEX
info       : ""
      </item>
```

*I don’t make the baselines, I just have to write the checks for them.

Yes, that’s 14 accounts that could have “Allow Log on as a Service” rights.

So what is happening here?

- powershell_args:
- '$allowedArray = \\"aspnet\\", \\"wsadmin\\", \\"rsa_user0\\", \\"sqladmin\\", \\"mmsservice\\", \\"Local_LOS\\", \\"iOS\\", \\"user_agent\\", \\"db2admin\\", \\"iis_user999\\", \\"blackberryservice\\", \\"DR_rsa_user0\\", \\"UAT__rsa_user0\\", \\"All Services\\";$allowedCounter = 0;
- $objectCounter = 0;
- $resultSet = gwmi -Namespace root/rsop/computer -Class RSOP_UserPrivilegeRight -Filter \\"UserRight=\'seservicelogonright\' and precedence=1\\";
- $resultSet\.PSObject\.Properties | foreach{if($_\.Name -eq \\"AccountList\\") {$users = $_\.Value -split \\" \\";}};
- if($users.Count -gt 0){Write-Host $users;foreach ($user in $users) {$objectCounter = $objectCounter + 1;
- foreach($allowed in $allowedArray) {if($user\.ToLower()\.Contains($allowed\.ToLower())){$allowedCounter = $allowedCounter + 1;}}};}
- if($allowedCounter -ge $objectCounter){Write-Host \\"Pass\\";};'

Insert some tabs to make it look presentable:

```
'$allowedArray = \\"ctx_user0\\", \\"ctx_user1\\", \\"aspnet\\", \\"wsadmin\\", \
\"rsa_user0\\", \\"sqladmin\\", \\"mmsservice\\", \\"Local_LOS\\", \\"iOS\\", \
\"user_agent\\", \\"db2admin\\", #\\"iis_user999\\", \\"blackberryservice\\", \
\"DR_rsa_user0\\", \\"UAT__rsa_user0\\, \\"All Services\\";
$allowedCounter = 0;
$objectCounter = 0;
$resultSet = gwmi -Namespace root/rsop/computer -Class RSOP_UserPrivilegeRight -Filter \
\"UserRight=\'seservicelogonright\' and precedence=1\\";
$resultSet\.PSObject\.Properties | foreach{if($_\.Name -eq \\"AccountList\\"){$users =
$_\.Value -split \\" \\";}};
if($users.Count -gt 0){
        Write-Host $users;
        foreach ($user in $users){
                $objectCounter = $objectCounter + 1;
                foreach($allowed in $allowedArray){
                        if($user\.ToLower()\.Contains($allowed\.ToLower())){
                                $allowedCounter = $allowedCounter + 1;
                        }
                }
        };
}
if($allowedCounter -ge $objectCounter){
        Write-Host \\"Pass\\";
};'
```

Windows Registry?
We can do that.

```
# Security Options\Network access: Named Pipes that can be accessed
anonymously Setting: COMNAP, COMNODE, SQL\QUERY, LLSRPC, netlogon,
samr
# HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
LanManServer\Parameters\NullSessionPipes
<custom_item>
type         : REGISTRY_SETTING
description  : "Network access: Named Pipes that can be accessed
anonymously"
value_type   : POLICY_MULTI_TEXT
value_data   : (redacted)
reg_key      : "HKLM\System\CurrentControlSet\Services\LanManServer\
Parameters\"
reg_item     : "NullSessionPipes"
reg_option   : CAN_BE_NULL
info         : ""
      </custom_item>
```

PowerShell and Windows Registry

- <custom_item>
- type: AUDIT_POWERSHELL
- description: "SNMP: Permitted Managers - Receive Requests"
- value_type: POLICY_TEXT
- value_data: "Pass"
- powershell_args : <redacted, next slide>
- check_type : CHECK_REGEX
- info : ""
- </custom_item>

PowerShell FTW

```
powershell_args  :
'$allowedArray
= \\"\\", \\"localhost\\", \\"127\.0\.0\.1\\", \\"127\.0\.0\.2\\", \\"127\.0\.0\.3\\", \\"127\.0\.0\.4\\", \\"127\.0\.0\.5\\", \\
"127\.0\.0\.6\\", \\"127\.0\.0\.7\\", \\"127\.0\.0\.8\\", \\"127\.0\.0\.9\\", \\"127\.0\.0\.10\\", \\"127\.0\.0\.11\\", \\"12
7\.0\.0\.12\\", \\"127\.0\.0\.13\\", \\"127\.0\.0\.14\\", \\"127\.0\.0\.15\\", \\"127\.0\.0\.16\\", \\"127\.0\.0\.17\\", \\"1
27\.0\.0\.18\\", \\"127\.0\.0\.19\\", \\"127\.0\.0\.20\\", \\"127\.0\.0\.21\\", \\"127\.0\.0\.22\\", \\"127\.0\.0\.23\\", \\"
127\.0\.0\.24\\", \\"127\.0\.0\.25\\", \\"127\.0\.0\.26\\", \\"127\.0\.0\.27\\", \\"127\.0\.0\.28\\", \\"127\.0\.0\.29\\", \\
"127\.0\.0\.30\\", \\"127\.0\.0\.31\\", \\"127\.0\.0\.32\\", \\"127\.0\.0\.33\\";
$RegKey = (Get-ItemProperty \\"HKLM:\\Software\\Policies\\SNMP\\Parameters\\PermittedManagers\\" -
ErrorAction SilentlyContinue);
$results = ($RegKey\.PSObject\.Properties);
$allowedCounter = 0;
$objectCounter = 0;
ForEach ($result in $results){If ($result -match \\"[0-9]\\") {Write-Host \\"Entry found: \\"
$result\.Value$objectCounter = $objectCounter + 1;ForEach ($setting in $allowedArray) {If ($result\.Value -
eq $setting) {$allowedCounter = $allowedCounter + 1;}}}}
If ($objectCounter -eq 0){Write-Host \\"No values found in the SNMP Permitted Managers Policies
location\\";}
ElseIf ($objectCounter -eq $allowedCounter) {Write-Host \\"Pass\\";}
Else {Write-Host \\"Objects Count: \\" $objectCounter \\" and Allowed Count: \\" $allowedCounter;}'
```

What do you mean? I don’t know why you wouldn’t have 32 SNMP Permitted Managers.

Beautify?

```
'$allowedArray = \\"\\", \\"localhost\\" <redacted because: seriously>;
$RegKey = (Get-ItemProperty \\"HKLM:\\Software\\Policies\\SNMP\\Parameters\
\PermittedManagers\\" -ErrorAction SilentlyContinue);
$results = ($RegKey\.PSObject\.Properties);$allowedCounter = 0;
$objectCounter = 0;
ForEach ($result in $results){
        If ($result -match \\"[0-9]\\") {
                Write-Host \\"Entry found: \\" $result\.Value;
                $objectCounter = $objectCounter + 1;
                ForEach ($setting in $allowedArray) {
                        If ($result\.Value -eq $setting) {
                                $allowedCounter = $allowedCounter + 1;
                        }
                }
        }
}
If ($objectCounter -eq 0){
        Write-Host \\"No values found in the SNMP Permitted Managers Policies location\\";
}
ElseIf ($objectCounter -eq $allowedCounter) {
        Write-Host \\"Pass\\";
}
Else {Write-Host \\"Objects Count: \\" $objectCounter \\" and Allowed Count: \\"
$allowedCounter;
}'
```

Results!

BSidesMSP

Configure | Launch | Export

Assets 2 | Vulnerabilities 2 | **Audits 9** | History 1

More Details

CURRENT CHECKS

2	0	7
FAILED	WARNING	PASSED

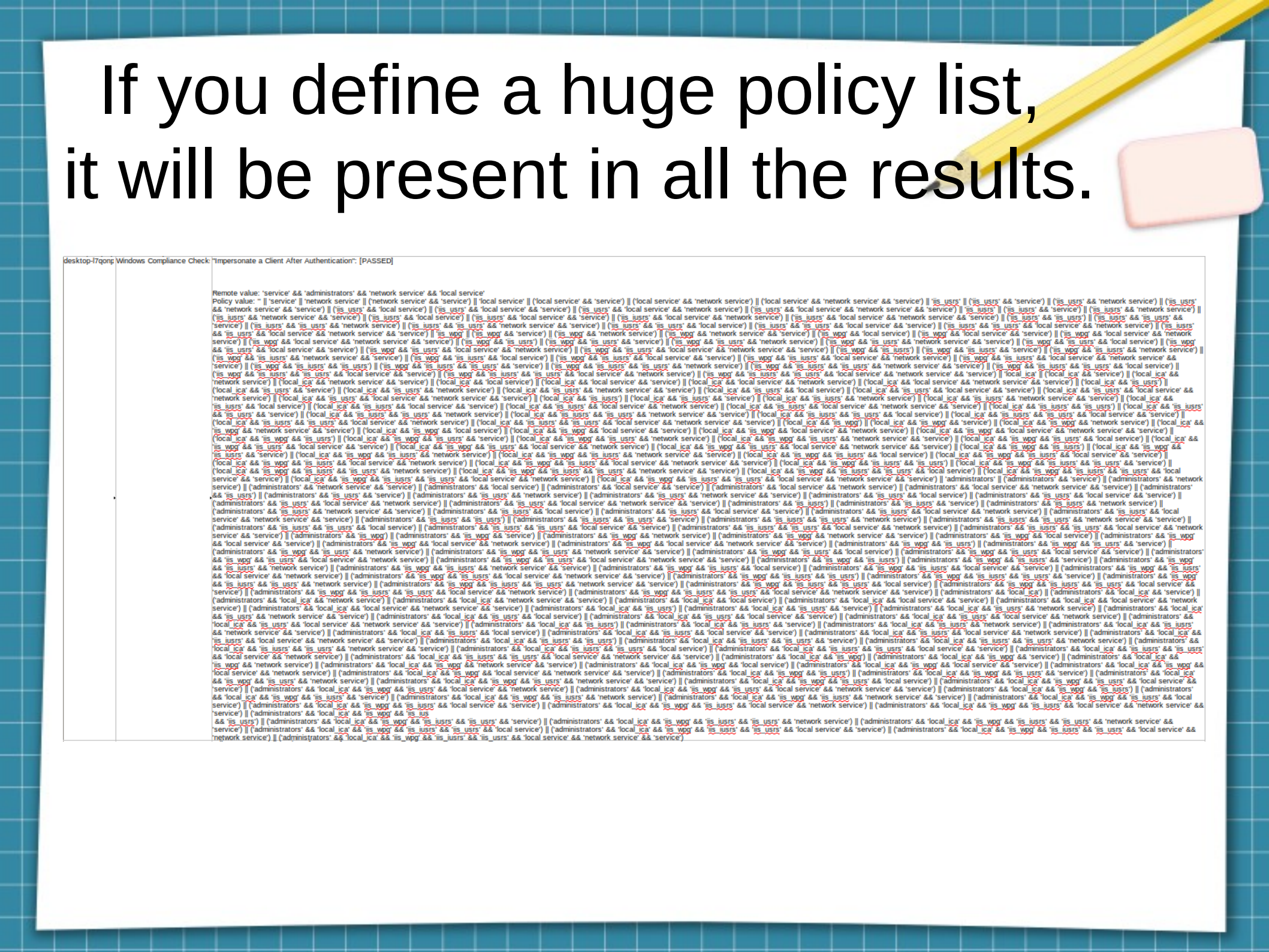
	Name ▲	Family	Count
●	Allow Log on Locally	Windows Compliance Checks	2
●	Bypass Traverse Checking	Windows Compliance Checks	2
●	Allow Log on as a Service	Windows Compliance Checks	2
●	Allow log on through Remote Desktop Services	Windows Compliance Checks	2
●	Deny logon as a batch job	Windows Compliance Checks	2

Results, exported.

	A	B	C
1	Host	Name	Description
2	win-c9jr72ccq0j	Windows Compliance Checks	"SNMP is not installed.": [PASSED]
3	win-c9jr72ccq0j	Windows Compliance Checks	"Allow Log on as a Service": [PASSED] Remote value: 'Pass' Policy value: 'pass'
4	win-c9jr72ccq0j	Windows Compliance Checks	"Impersonate a client after authentication": [PASSED] Remote value: 'service' && 'administrators' && 'network service' && 'local service' Policy value: 'service' || 'network service' || ('network service' && 'service') || 'local service' || ('local service' && 'service') || ('local service' && 'network service') || ('local service' && 'network service' && 'service') || 'administrators' || ('administrators' && 'service') || ('administrators' && 'network service') || ('administrators' && 'network service' && 'service') || ('administrators' && 'local service') || ('administrators' && 'local service' && 'service') || ('administrators' && 'local service' && 'network service') || ('administrators' && 'local service' && 'network service' && 'service')
5	win-c9jr72ccq0j	Windows Compliance Checks	"Allow log on through Remote Desktop Services": [PASSED] Remote value: 'remote desktop users' && 'administrators' Policy value: 'remote desktop users' || 'administrators' || ('administrators' && 'remote desktop users')

If you define a huge policy list, it will be present in all the results.

desktop-l7qonp	Windows Compliance Check	"Impersonate a Client After Authentication": [PASSED] Remote value: 'service' && 'administrators' && 'network service' && 'local service' Policy value: '' || 'service' || 'network service' || ('network service' && 'service') || 'local service' || ('local service' && 'service') || ('local service' && 'network service') || ('local service' && 'network service' && 'service') || 'iis_usrs' || ('iis_usrs' && 'service') || ('iis_usrs' && 'network service') || ('iis_usrs' && 'network service' && 'service') || ('iis_usrs' && 'local service') || ('iis_usrs' && 'local service' && 'service') || ('iis_usrs' && 'local service' && 'network service') || ('iis_usrs' && 'local service' && 'network service' && 'service') || ('iis_usrs' && 'iis_usrs') || ('iis_usrs' && 'iis_usrs' && 'service') || ('iis_usrs' && 'iis_usrs' && 'network service') || ('iis_usrs' && 'iis_usrs' && 'local service') || ('iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || 'iis_wpg' || ('iis_wpg' && 'service') || ('iis_wpg' && 'network service') || ('iis_wpg' && 'network service' && 'service') || ('iis_wpg' && 'local service') || ('iis_wpg' && 'local service' && 'service') || ('iis_wpg' && 'local service' && 'network service') || ('iis_wpg' && 'local service' && 'network service' && 'service') || ('iis_wpg' && 'iis_usrs') || ('iis_wpg' && 'iis_usrs' && 'service') || ('iis_wpg' && 'iis_usrs' && 'network service') || ('iis_wpg' && 'iis_usrs' && 'network service' && 'service') || ('iis_wpg' && 'iis_usrs' && 'local service') || ('iis_wpg' && 'iis_usrs' && 'local service' && 'service') || ('iis_wpg' && 'iis_usrs' && 'local service' && 'network service') || ('iis_wpg' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || 'local_ica' || ('local_ica' && 'service') || ('local_ica' && 'network service') || ('local_ica' && 'network service' && 'service') || ('local_ica' && 'local service') || ('local_ica' && 'local service' && 'service') || ('local_ica' && 'local service' && 'network service') || ('local_ica' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_usrs') || ('local_ica' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_wpg') || ('local_ica' && 'iis_wpg' && 'service') || ('local_ica' && 'iis_wpg' && 'network service') || ('local_ica' && 'iis_wpg' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'local service') || ('local_ica' && 'iis_wpg' && 'local service' && 'service') || ('local_ica' && 'iis_wpg' && 'local service' && 'network service') || ('local_ica' && 'iis_wpg' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('administrators' || ('administrators' && 'service') || ('administrators' && 'network service') || ('administrators' && 'network service' && 'service') || ('administrators' && 'local service') || ('administrators' && 'local service' && 'service') || ('administrators' && 'local service' && 'network service') || ('administrators' && 'local service' && 'network service' && 'service') || ('administrators' && 'iis_usrs') || ('administrators' && 'iis_usrs' && 'service') || ('administrators' && 'iis_usrs' && 'network service') || ('administrators' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'iis_usrs' && 'local service') || ('administrators' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('administrators' && 'iis_usrs' && 'iis_usrs') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'service') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('administrators' && 'iis_wpg') || ('administrators' && 'iis_wpg' && 'service') || ('administrators' && 'iis_wpg' && 'network service') || ('administrators' && 'iis_wpg' && 'network service' && 'service') || ('administrators' && 'iis_wpg' && 'local service') || ('administrators' && 'iis_wpg' && 'local service' && 'service') || ('administrators' && 'iis_wpg' && 'local service' && 'network service') || ('administrators' && 'iis_wpg' && 'local service' && 'network service' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'network service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'local service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'local_ica') || ('administrators' && 'local_ica' && 'service') || ('administrators' && 'local_ica' && 'network service') || ('administrators' && 'local_ica' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'local service') || ('administrators' && 'local_ica' && 'local service' && 'service') || ('administrators' && 'local_ica' && 'local service' && 'network service') || ('administrators' && 'local_ica' && 'local service' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_usrs') || ('administrators' && 'local_ica' && 'iis_usrs' && 'service') || ('administrators' && 'local_ica' && 'iis_usrs' && 'network service') || ('administrators' && 'local_ica' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_usrs' && 'local service') || ('administrators' && 'local_ica' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'local_ica' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'local_ica' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg') || ('administrators' && 'local_ica' && 'iis_wpg' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'network service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'local service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'local service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'local service' && 'network service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'local service' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'network service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'local service' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'network service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service') || ('administrators' && 'local_ica' && 'iis_wpg' && 'iis_usrs' && 'iis_usrs' && 'local service' && 'network service' && 'service')



What else can I do with audit files?

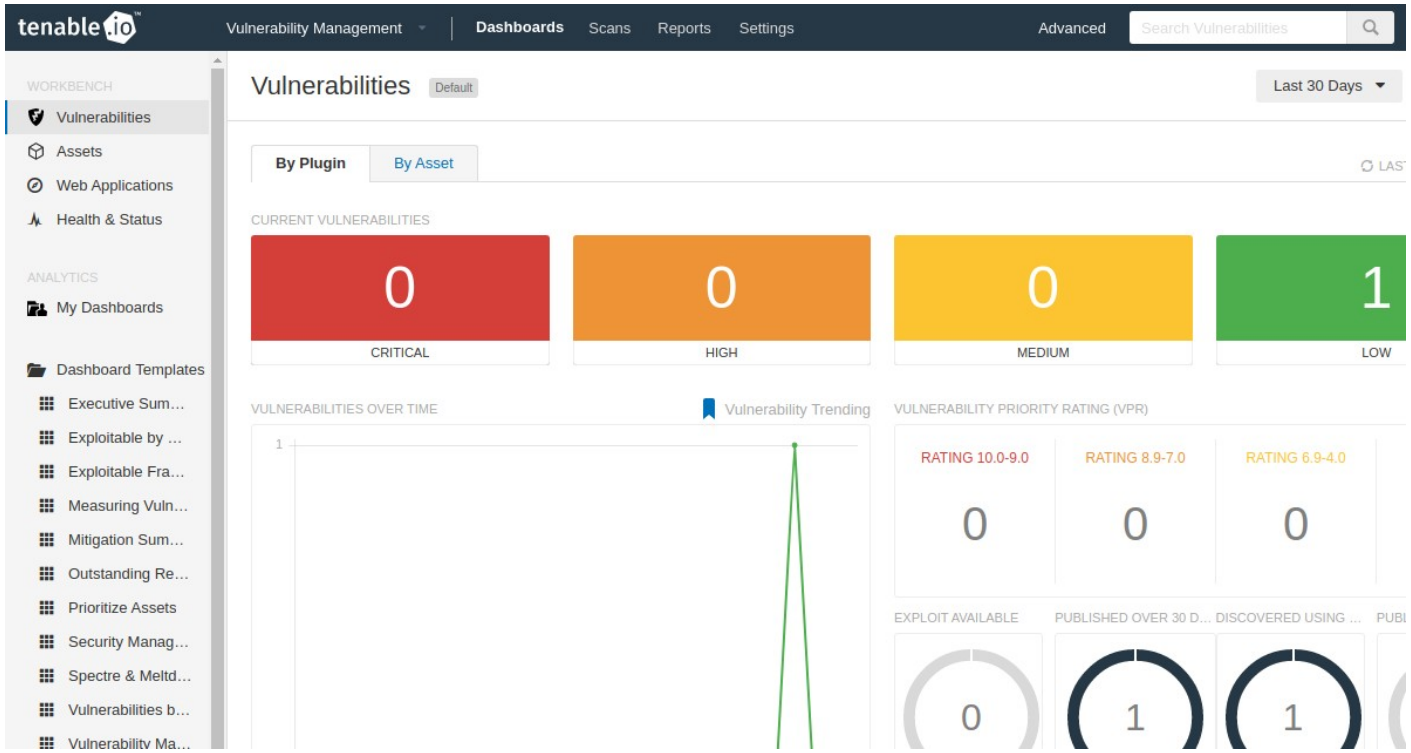
```
<if>
        <condition type:"or">
                <custom_item>
                        # check
                </custom_item>
        </condition>
        <then>
                <custom_item>
                        # check
                </custom_item>
        </then>
<else>
        <if>
                <condition type:"or">
                        <custom_item>
                                # check
                        </custom_item>
                </condition>
        <then>
                <custom_item>
                        # check
                </custom_item>
        </then>
        <else>
                <custom_item>
                        # check
                </custom_item>
        </else>
        </if>
</else>
</if>
```

After getting our results, how do we see them?

Sometimes finding what you want in Tenable/SecurityCenter seems like an unintended birdbox challenge.

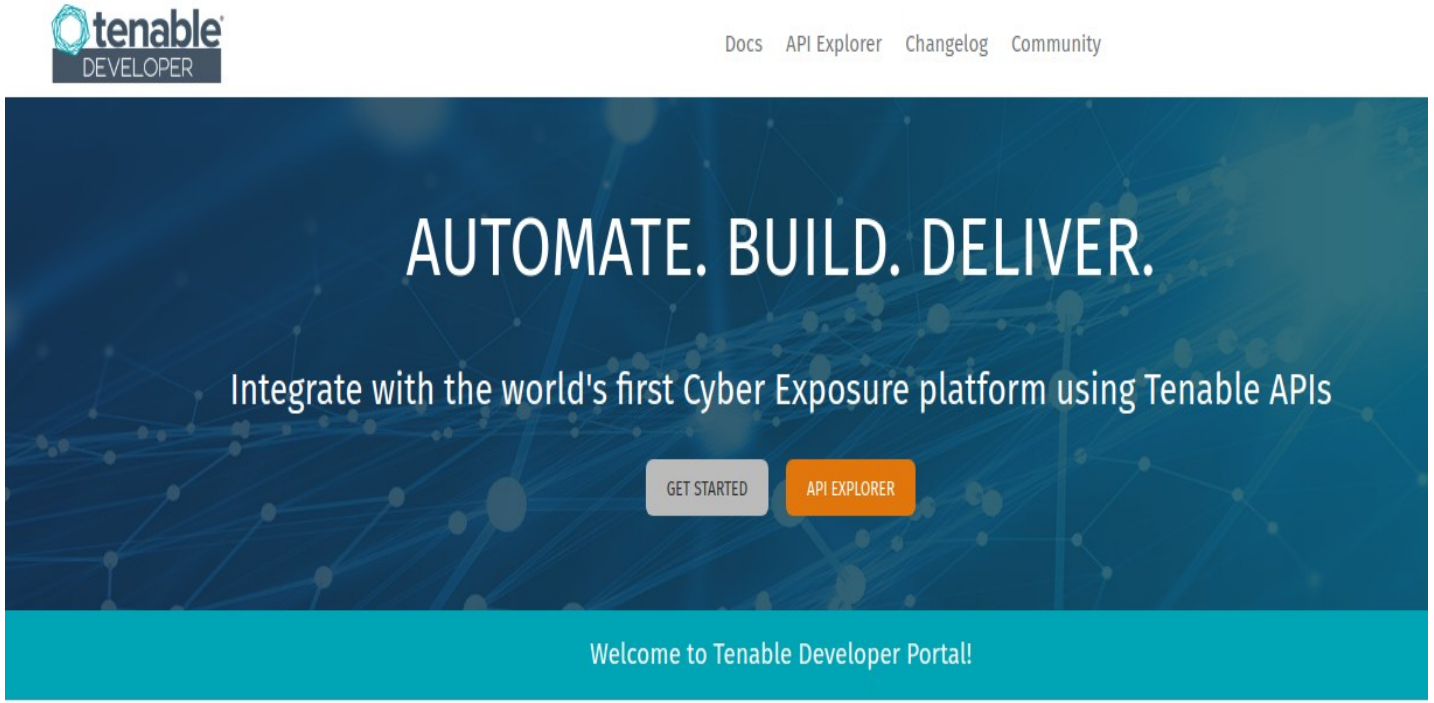
Problem

- Compliance is not in the GUI
- Third Party Tools don’t ingest the data
- Leaves data dead in the cloud



Our Solution

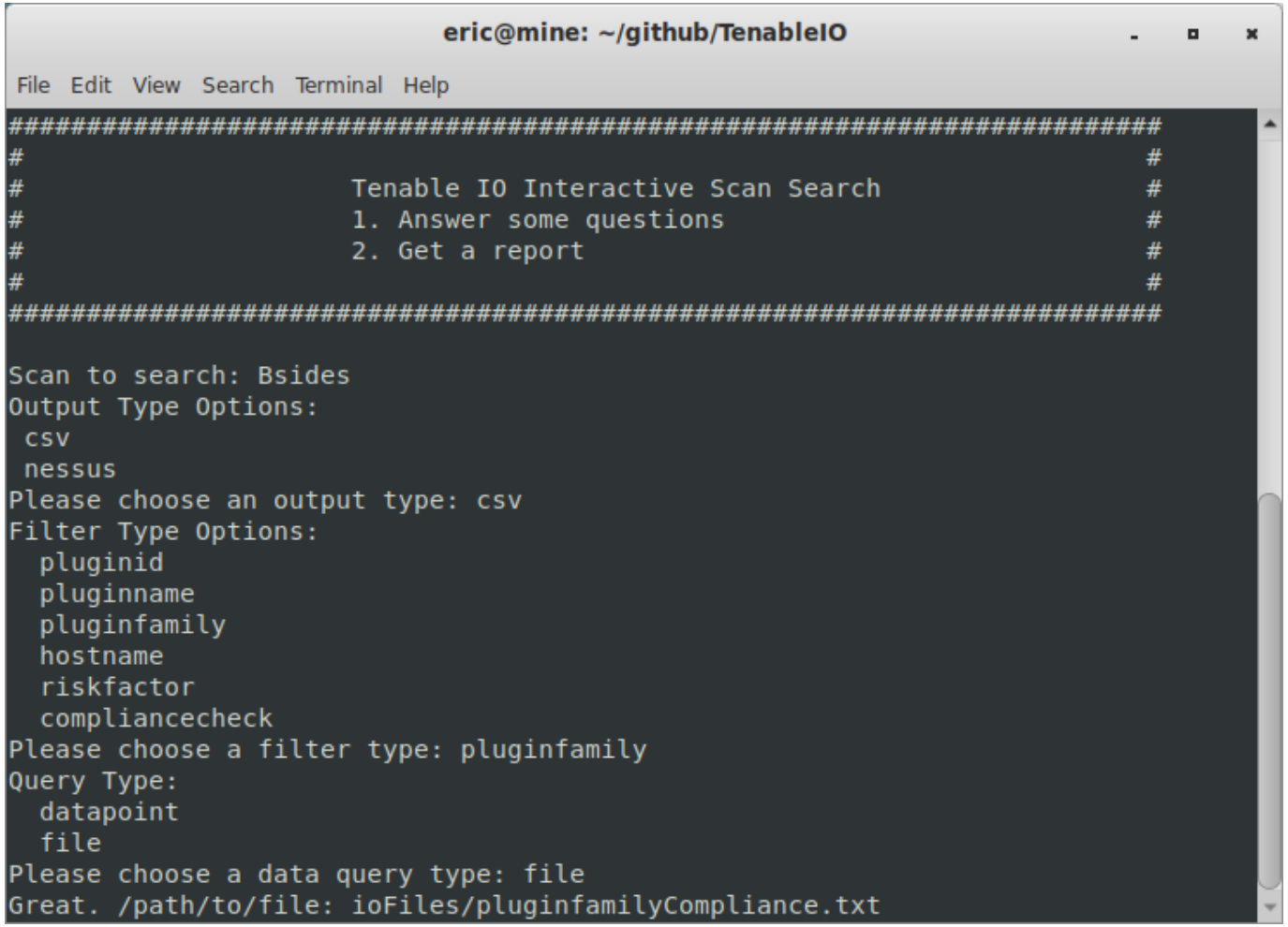
- API + python



Cyber Exposure Management Made Easy

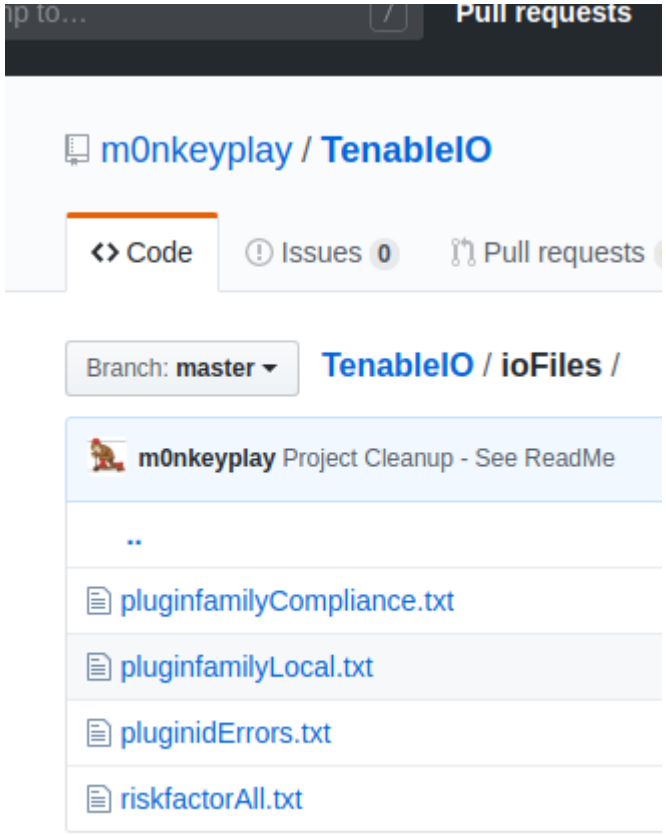
What does it do?

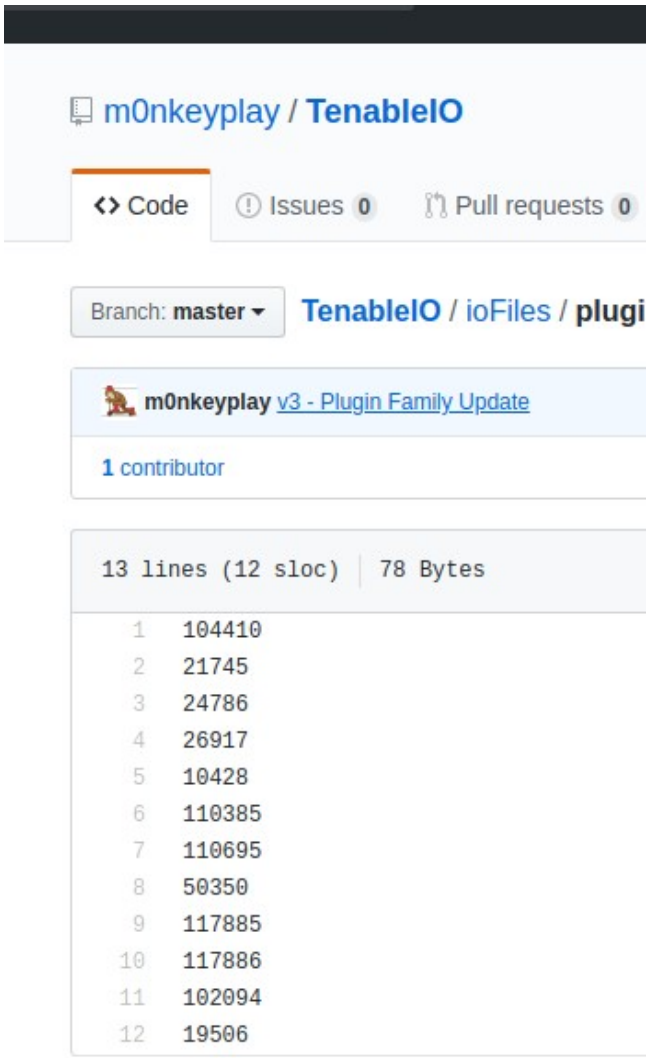
- Pulls down scan data based on search criteria



What does it do?

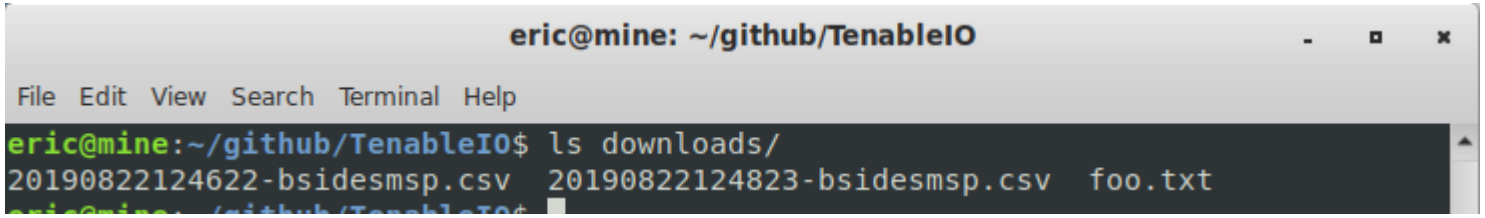
- Configurable





What does it do?

- Pretty standard output format (csv)



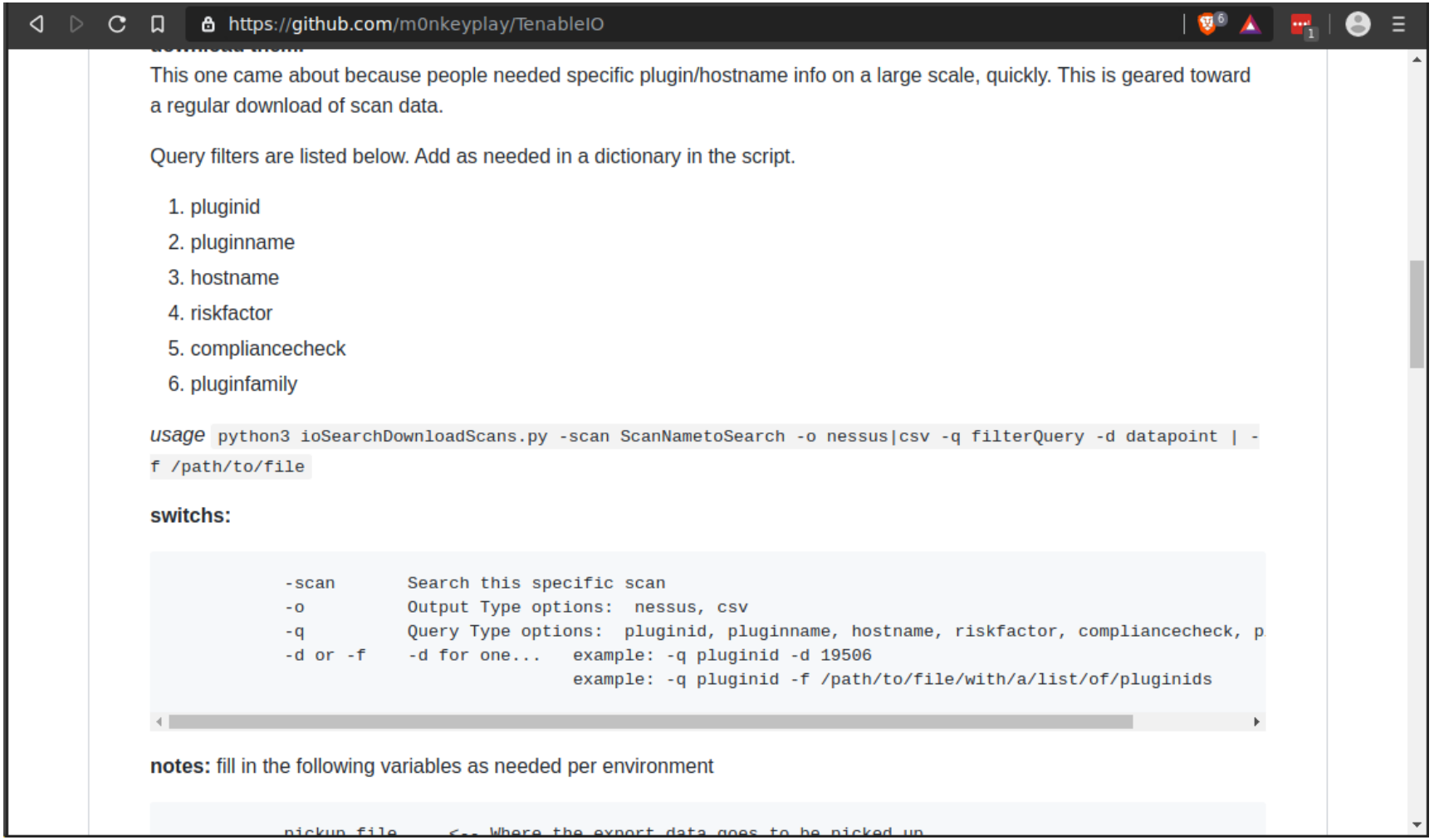
	A	B	C	D	E	F	G	H	I	J
6	21156		0	High	win-c9jr72ccq0j	tcp	0	Windows Compliance Checks	Compliance checks for Windows systems.	"Bypass Traverse Checking": [FAILED] Remote value: 'backup operators' && 'users' && 'administrators' && 'network service' Policy value: '' || 'local_btc' || 'network service' || ('network service' && 'local_btc') || 'loc
8	21156		0	High	win-c9jr72ccq0j	tcp	0	Windows Compliance Checks	Compliance checks for Windows systems.	"Allow Log on Locally": [FAILED] Remote value: 'backup operators' && 'users' && 'administrators' Policy value: '' || 'administrators' || 'cduser' || ('cduser' && 'administrators') || 'local_lol' ||
12	21156		0	High	desktop-l7qonpc	tcp	0	Windows Compliance Checks	Compliance checks for Windows systems.	"Bypass Traverse Checking": [FAILED] Remote value: 'backup operators' && 'users' && 'administrators' && 'network service' Policy value: '' || 'local_btc' || 'network service' || ('network service' && 'local_btc') || 'loc
13	21156		0	High	desktop-l7qonpc	tcp	0	Windows Compliance Checks	Compliance checks for Windows systems.	"Allow Log on Locally": [FAILED] Remote value: 'backup operators' && 'users' && 'administrators' && 'guest' Policy value: '' || 'administrators' || 'cduser' || ('cduser' && 'administrators') || 'local_lol' ||

Who is it for?

- Remediation Team
  - Quick results for compliance or vulnerability scans
  - Pin point results
  - No access to the GUI needed
- Reporting Team
  - Script raw data pulls
  - Transform data

Sold!

- https://github.com/m0nkeyplay/tenableIO



References

- CIS Benchmarks
  - https://www.cisecurity.org/partner/tenable/
  - https://www.irs.gov/privacy-disclosure/nessus-audit-files
- Nessus Development
  - https://developer.tenable.com
- Nessus Parser
  - http://www.melcara.com
- TenableIO Scripts by ~eric
  - https://github.com/m0nkeyplay/

Questions???

Contact Info:

Eric’s twitter: @435ftw
Gabe’s twitter: @grnbeltwarrior