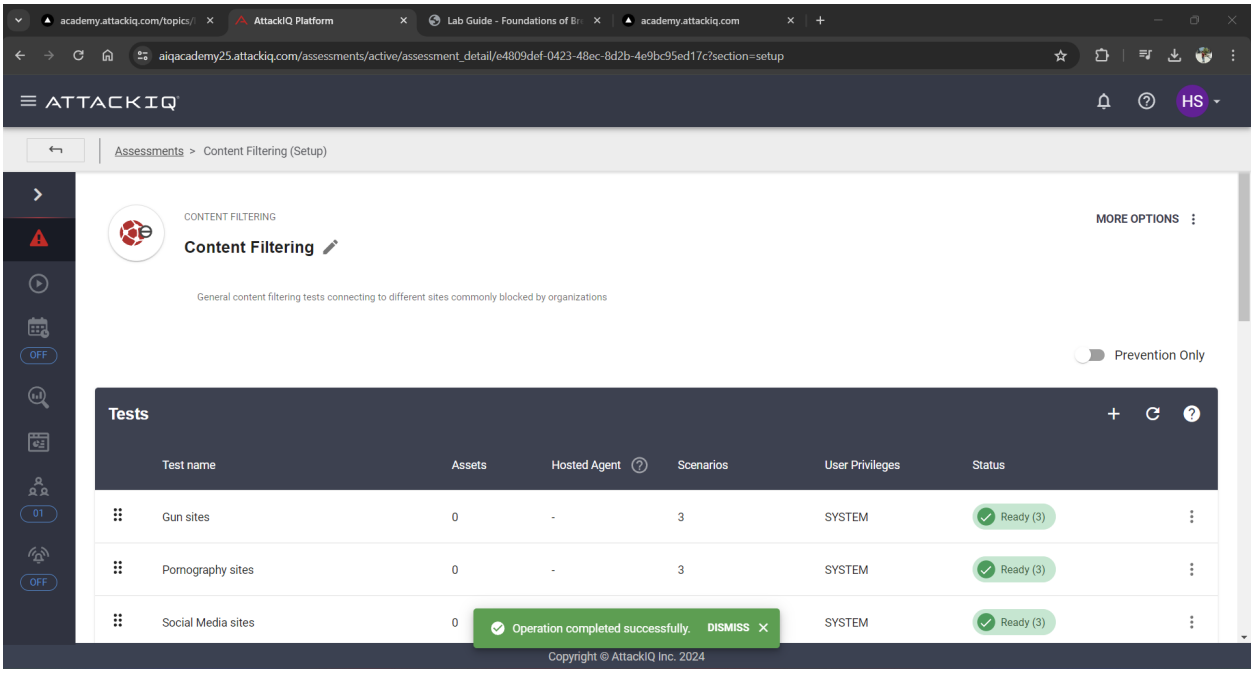
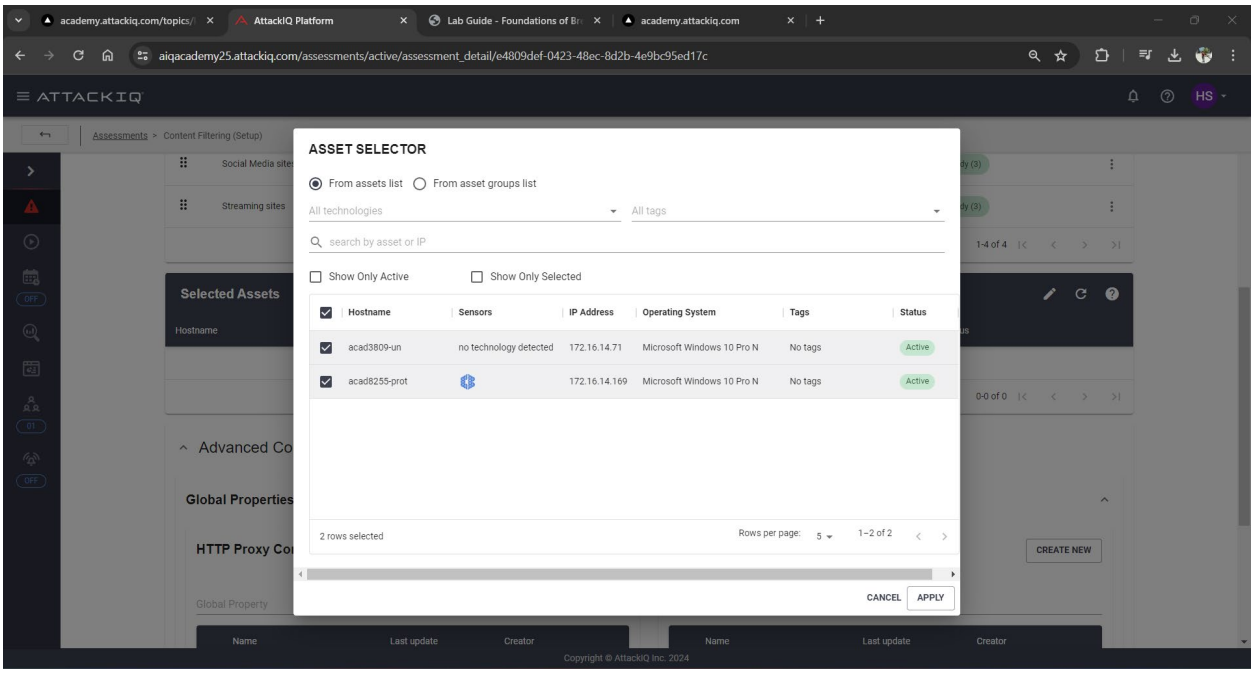
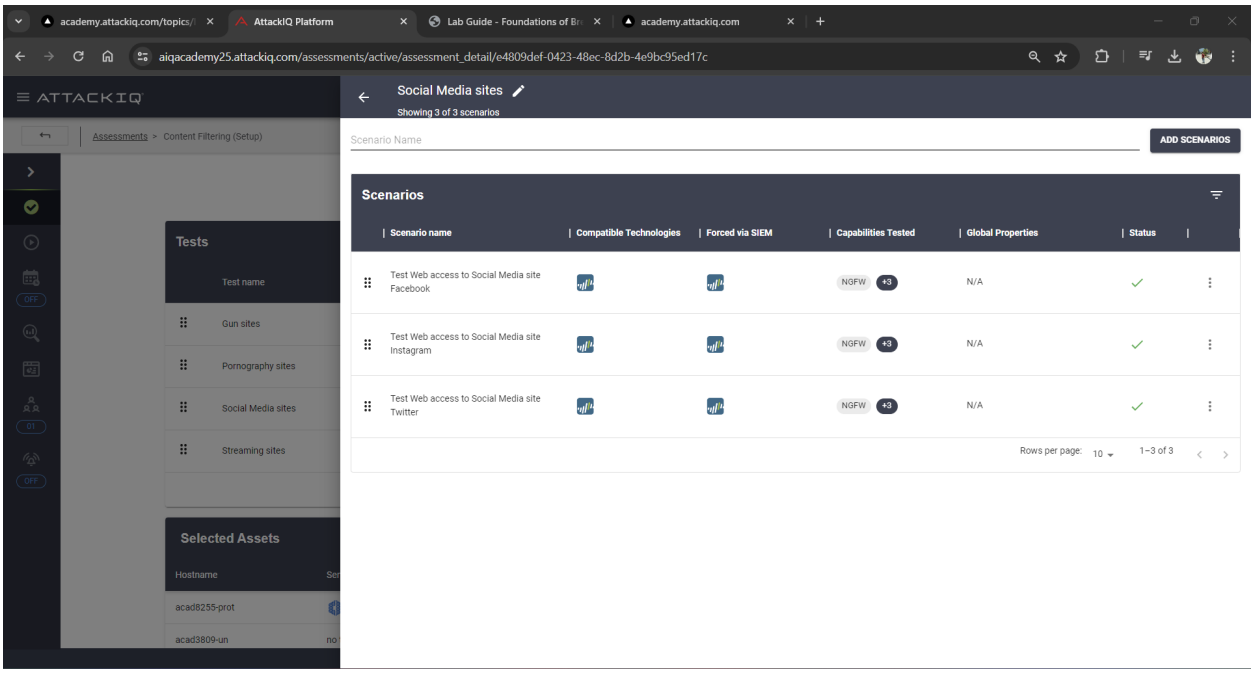
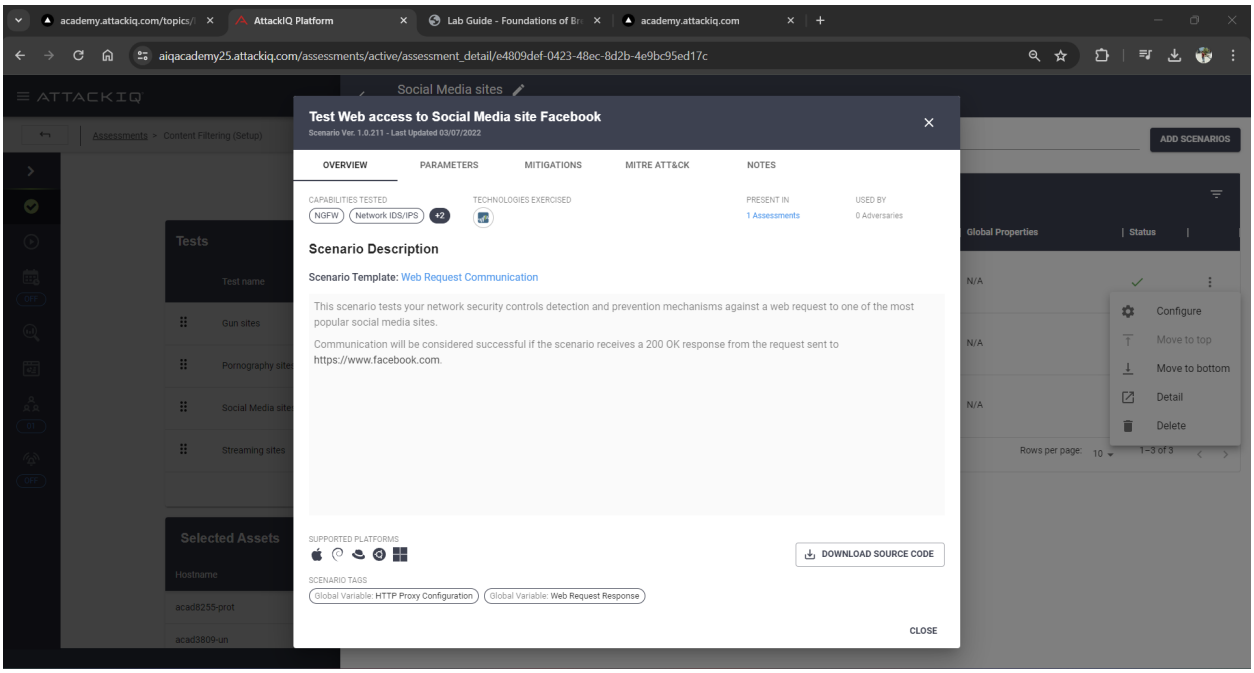
Foundations of Breach & Attack Simulation

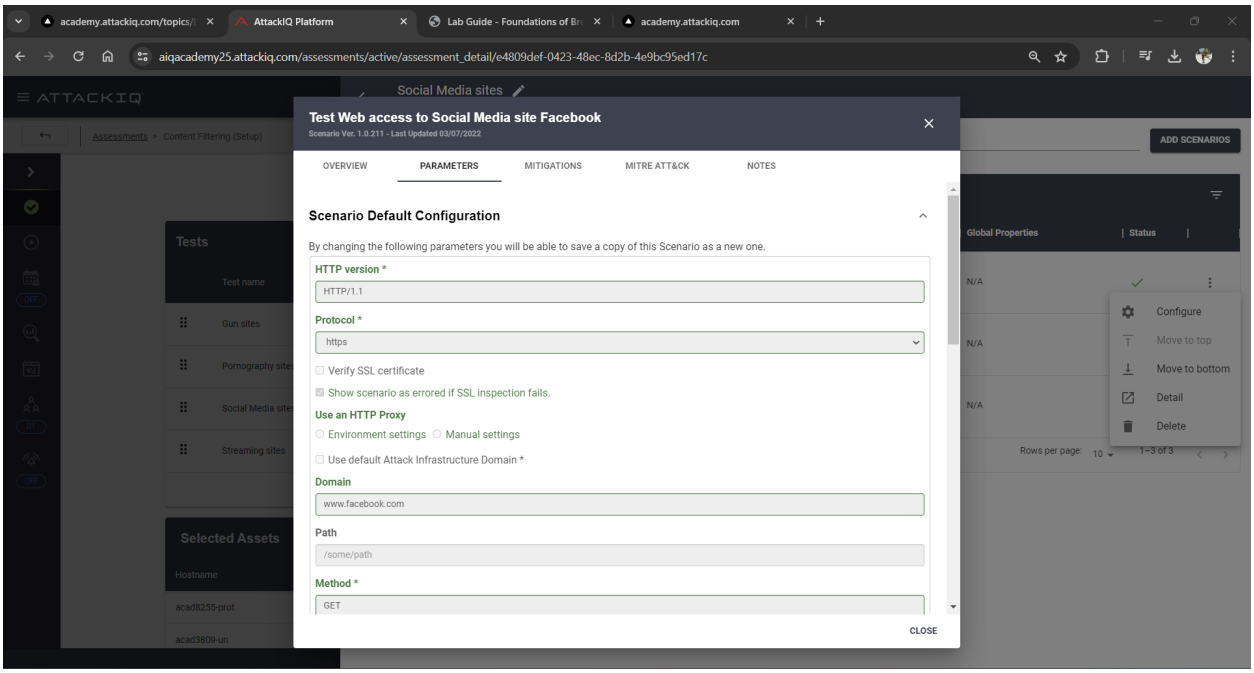
Exercise 1: Continuous Security Validation 1. Click on the CREATE NEW ASSESSMENT button 2. Click CHOOSE TEMPLATE. 3. On the Assessment Templates page, click the dropdown under Select template type, and choose Security Controls. 4 4. Find the Content Filtering assessment template on the page, and click it. 5. Click Create New. 6. Add both assets to the Assessment. a. Click the Manage Assets button b. Click the checkboxes of BOTH assets listed. c. Click Apply 5 7. Under the assets, where it lists the tests configured, click on the three dots under the ACTION column for the test name Social Media sites. 8. Click Manage Scenarios. 9. Under the details column, click on the icon to see the details for Test Web access to Social Media site Facebook. 6 10. On the resulting scenario details page for Test Web Access to Social Media Site Facebook, read and make a note of the scenario description. 11. Click on the heading for Scenario Configuration to expand the configuration details. 12. Review the configuration settings and make note of the Headers sent during the test. Also, make a note of the method being used. 13. Return to the assessment page and click Done to close the scenario listing for the Social Media sites test. 14. Click the Continue button in the bottom right-hand corner of the page. 15. Click the Run Now button.

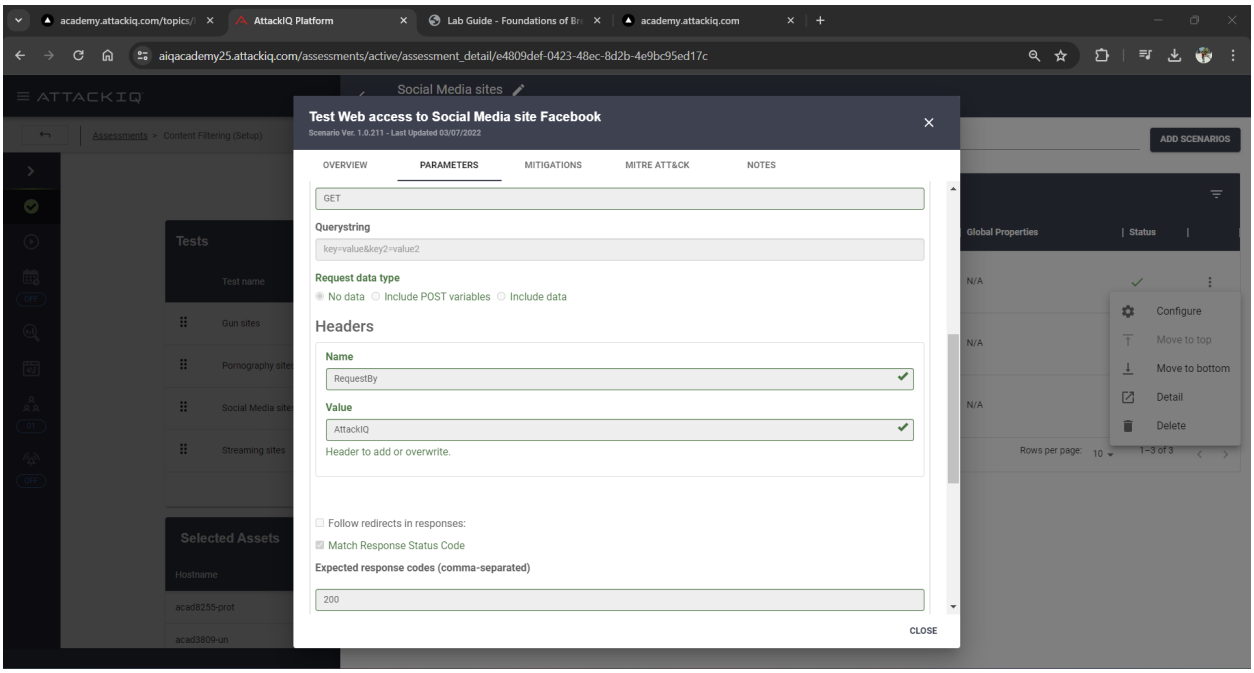


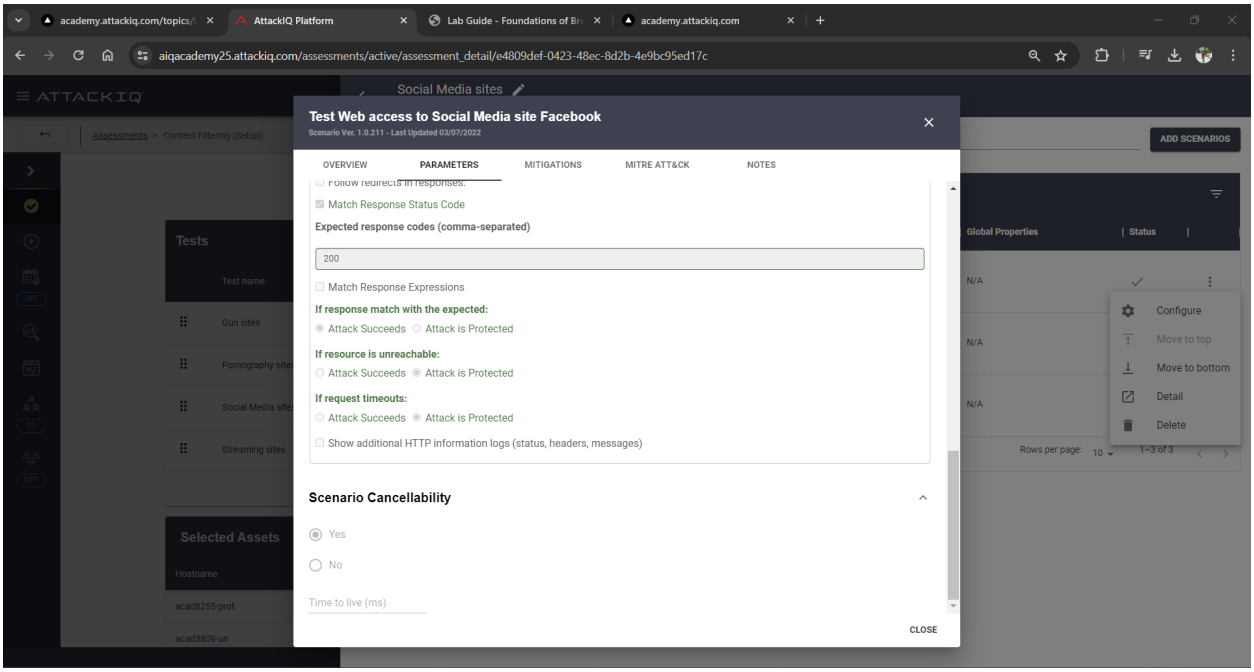

academy.attackiq.com/topics/
AttackIQ Platform
Lab Guide - Foundations of Br
academy.attackiq.com
aiqacademy25.attackiq.com/assessments/active/assessment_detail/e4809def-0423-48ec-8d2b-4e9bc95ed17c
ATTACKIQ
HS
Assessments > Content Filtering (Setup)
Social Media sites
Streaming sites
ASSET SELECTOR
From assets list
From asset groups list
All technologies
All tags
search by asset or IP
Show Only Active
Show Only Selected
Hostname
Sensors
IP Address
Operating System
Tags
Status
acad3809-un
no technology detected
172.16.14.71
Microsoft Windows 10 Pro N
No tags
Active
acad8255-prot
172.16.14.169
Microsoft Windows 10 Pro N
No tags
Active
2 rows selected
Rows per page: 5
1–2 of 2
CANCEL
APPLY
Selected Assets
Hostname
Advanced Co
Global Properties
HTTP Proxy Co
Global Property
CREATE NEW
Name
Last update
Creator
Copyright © AttackIQ Inc. 2024

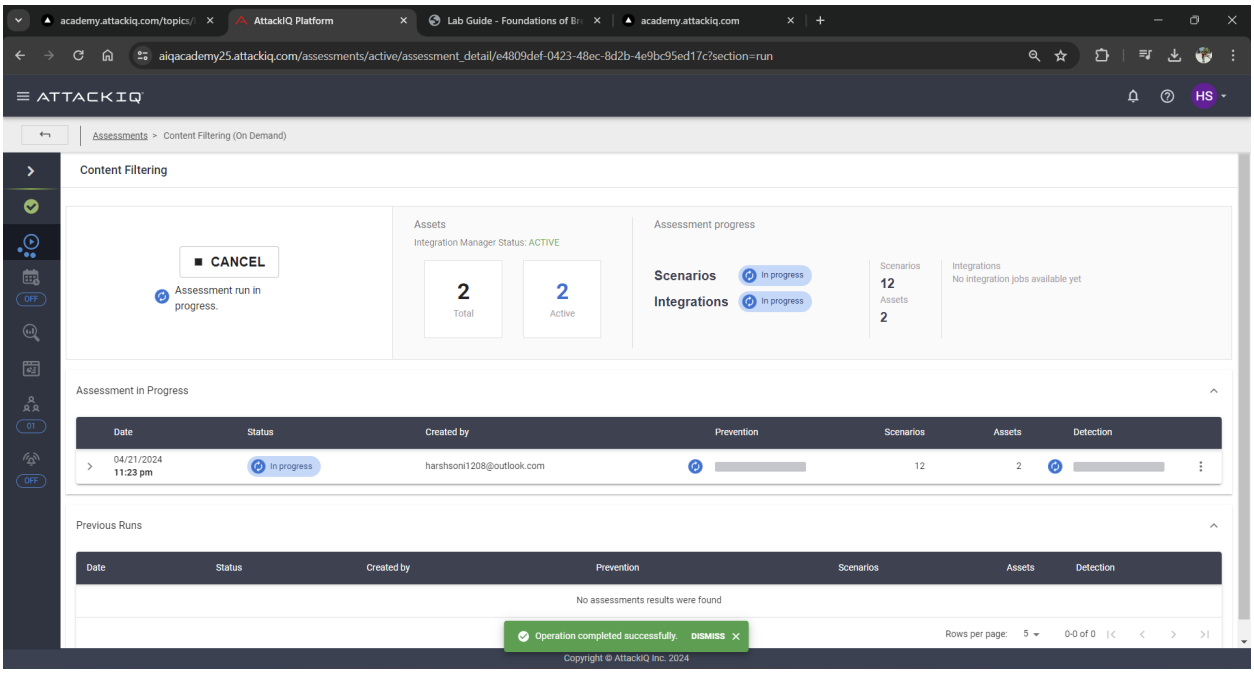

academy.attackiq.com/topics/
AttackIQ Platform
Lab Guide - Foundations of Br
academy.attackiq.com
aiqacademy25.attackiq.com/assessments/active/assessment_detail/e4809def-0423-48ec-8d2b-4e9bc95ed17c
ATTACKIQ
Assessments > Content Filtering (Setup)
Social Media sites
Showing 3 of 3 scenarios
Scenario Name
ADD SCENARIOS
Scenarios
Scenario name
Compatible Technologies
Forced via SIEM
Capabilities Tested
Global Properties
Status
Test Web access to Social Media site Facebook
Test Web access to Social Media site Instagram
Test Web access to Social Media site Twitter
NGFW
+3
N/A
Rows per page: 10
1–3 of 3
Tests
Test name
Gun sites
Pornography sites
Social Media sites
Streaming sites
Selected Assets
Hostname
acad8255-prot
acad3809-un


academy.attackiq.com/topics/
AttackIQ Platform
Lab Guide - Foundations of Br
academy.attackiq.com
aiqacademy25.attackiq.com/assessments/active/assessment_detail/e4809def-0423-48ec-8d2b-4e9bc95ed17c
ATTACKIQ
Social Media sites
Assessments > Content Filtering (Setup)
ADD SCENARIOS
Test Web access to Social Media site Facebook
Scenario Ver. 1.0.211 - Last Updated 03/07/2022
OVERVIEW
PARAMETERS
MITIGATIONS
MITRE ATT&CK
NOTES
CAPABILITIES TESTED
NGFW
Network IDS/IPS
+2
TECHNOLOGIES EXERCISED
PRESENT IN
1 Assessments
USED BY
0 Adversaries
Scenario Description
Scenario Template: Web Request Communication
This scenario tests your network security controls detection and prevention mechanisms against a web request to one of the most popular social media sites.
Communication will be considered successful if the scenario receives a 200 OK response from the request sent to https://www.facebook.com.
SUPPORTED PLATFORMS
DOWNLOAD SOURCE CODE
SCENARIO TAGS
Global Variable: HTTP Proxy Configuration
Global Variable: Web Request Response
CLOSE
Tests
Test name
Gun sites
Pornography sites
Social Media sites
Streaming sites
Selected Assets
Hostname
acad8255-prot
acad3809-un
Global Properties
Status
N/A
Configure
Move to top
Move to bottom
Detail
Delete
Rows per page: 10
1–3 of 3

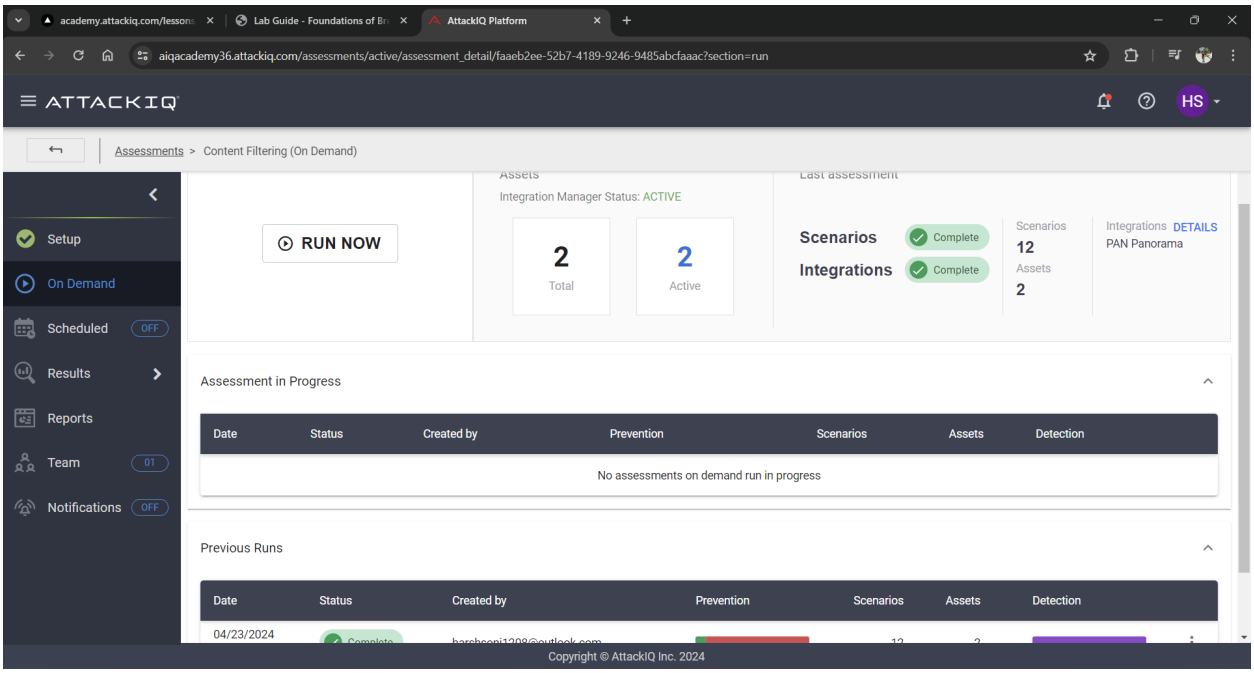

academy.attackiq.com/topics/
AttackIQ Platform
Lab Guide - Foundations of Br
academy.attackiq.com
aiqacademy25.attackiq.com/assessments/active/assessment_detail/e4809def-0423-48ec-8d2b-4e9bc95ed17c
ATTACKIQ
Social Media sites
Assessments > Content Filtering (Setup)
ADD SCENARIOS
Test Web access to Social Media site Facebook
Scenario Ver. 1.0.211 - Last Updated 03/07/2022
OVERVIEW
PARAMETERS
MITIGATIONS
MITRE ATT&CK
NOTES
Scenario Default Configuration
By changing the following parameters you will be able to save a copy of this Scenario as a new one.
HTTP version *
HTTP/1.1
Protocol *
https
Verify SSL certificate
Show scenario as errored if SSL inspection fails.
Use an HTTP Proxy
Environment settings
Manual settings
Use default Attack Infrastructure Domain *
Domain
www.facebook.com
Path
/some/path
Method *
GET
CLOSE
Tests
Test name
Gun sites
Pornography sites
Social Media sites
Streaming sites
Selected Assets
Hostname
acad8255-prot
acad3809-un
Global Properties
Status
N/A
Configure
Move to top
Move to bottom
Detail
Delete
Rows per page: 10
1–3 of 3

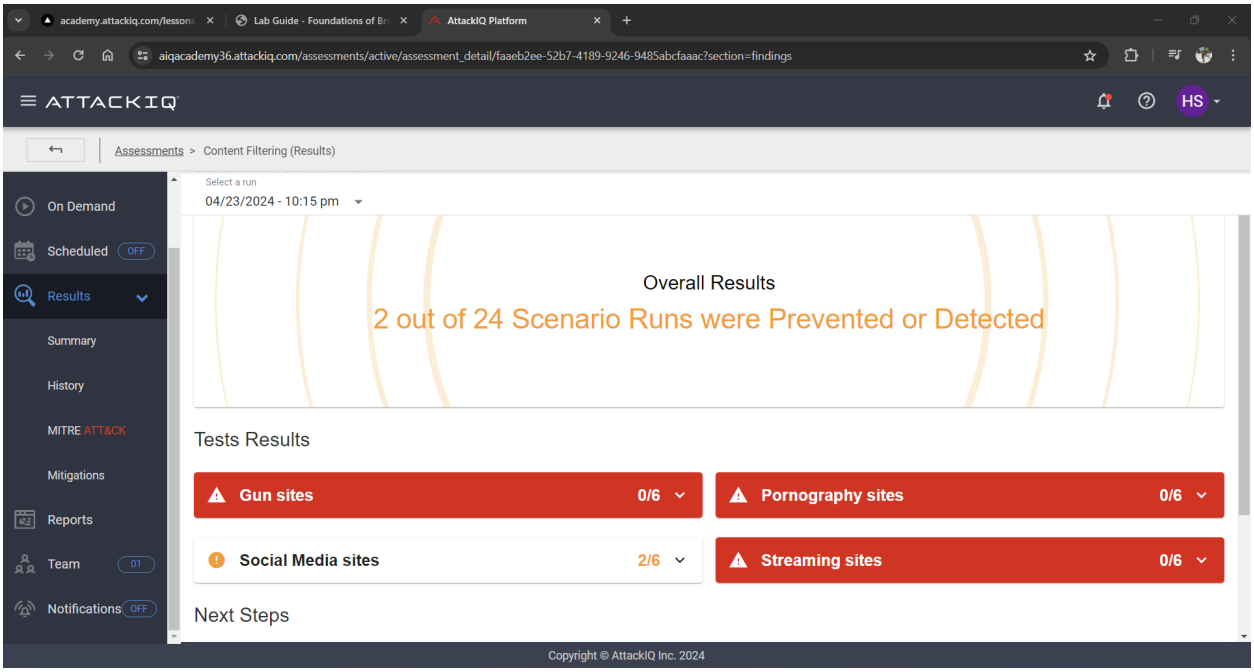

academy.attackiq.com/topics/
AttackIQ Platform
Lab Guide - Foundations of Br
academy.attackiq.com
aiqacademy25.attackiq.com/assessments/active/assessment_detail/e4809def-0423-48ec-8d2b-4e9bc95ed17c
ATTACKIQ
Social Media sites
Assessments > Content Filtering (Setup)
ADD SCENARIOS
Test Web access to Social Media site Facebook
Scenario Ver. 1.0.211 - Last Updated 03/07/2022
OVERVIEW
PARAMETERS
MITIGATIONS
MITRE ATT&CK
NOTES
GET
Querystring
key=value&key2=value2
Request data type
No data
Include POST variables
Include data
Headers
Name
RequestBy
Value
AttackIQ
Header to add or overwrite.
Follow redirects in responses:
Match Response Status Code
Expected response codes (comma-separated)
200
CLOSE
Tests
Test name
Gun sites
Pornography sites
Social Media sites
Streaming sites
Selected Assets
Hostname
acad8255-prot
acad3809-un
Global Properties
Status
N/A
Configure
Move to top
Move to bottom
Detail
Delete
Rows per page:
10
1–3 of 3

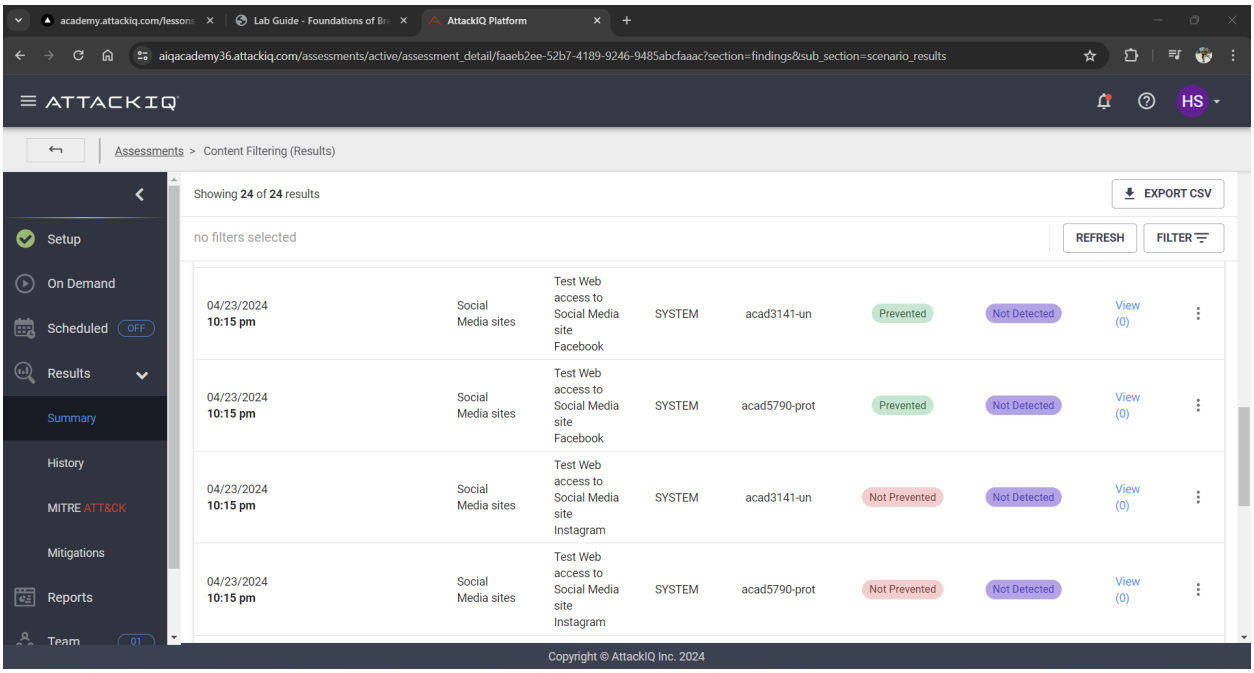

academy.attackiq.com/topics/
AttackIQ Platform
Lab Guide - Foundations of Br
academy.attackiq.com
aiqacademy25.attackiq.com/assessments/active/assessment_detail/e4809def-0423-48ec-8d2b-4e9bc95ed17c
ATTACKIQ
Social Media sites
Assessments > Content Filtering (Setup)
ADD SCENARIOS
Test Web access to Social Media site Facebook
Scenario Ver. 1.0.211 - Last Updated 03/07/2022
OVERVIEW
PARAMETERS
MITIGATIONS
MITRE ATT&CK
NOTES
Match Response Status Code
Expected response codes (comma-separated)
200
Match Response Expressions
If response match with the expected:
Attack Succeeds
Attack is Protected
If resource is unreachable:
Attack Succeeds
Attack is Protected
If request timeouts:
Attack Succeeds
Attack is Protected
Show additional HTTP information logs (status, headers, messages)
Scenario Cancellability
Yes
No
Time to live (ms)
CLOSE
Tests
Test name
Gun sites
Pornography sites
Social Media sites
Streaming sites
Selected Assets
Hostname
acad8255-prot
acad3809-un
Global Properties
Status
N/A
Configure
Move to top
Move to bottom
Detail
Delete
Rows per page:
10
1–3 of 3

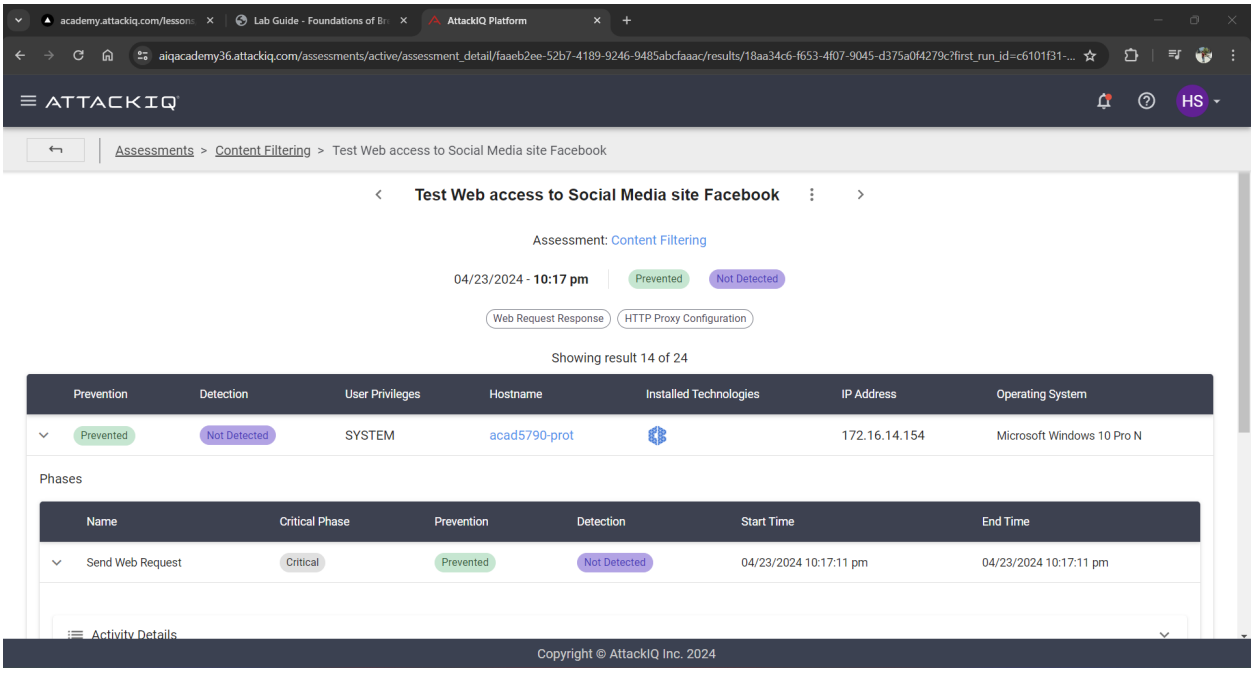


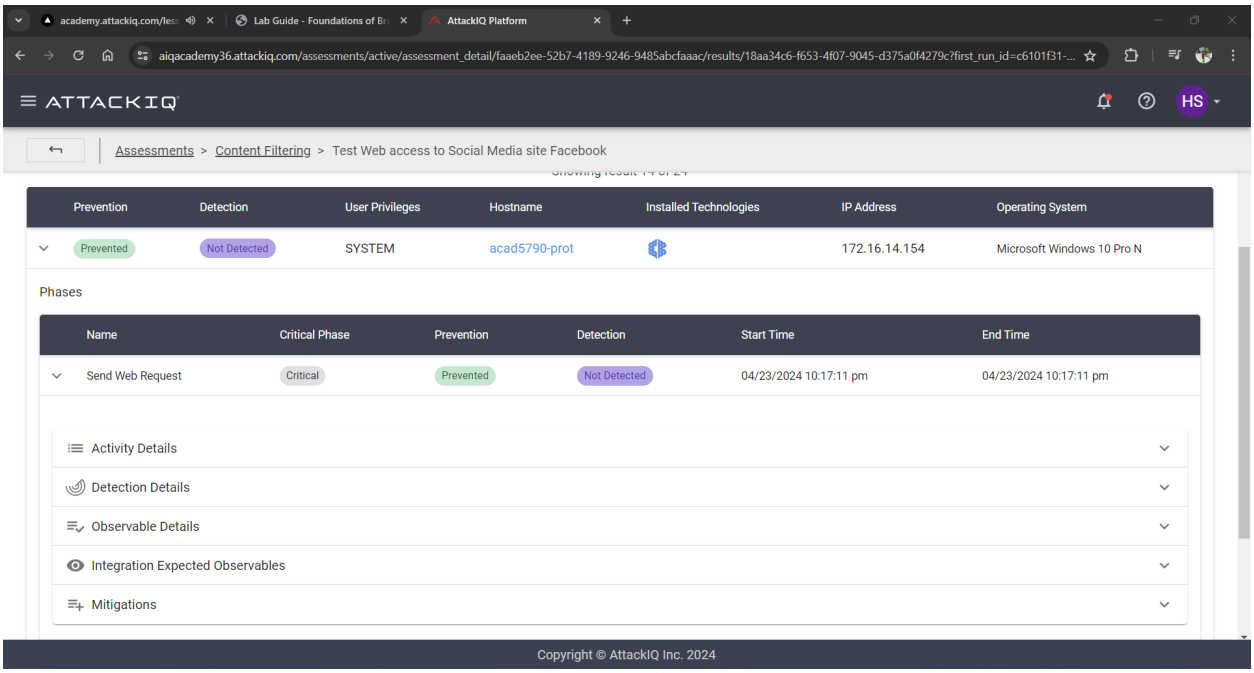
Exercise 2: Continuous Security Validation - Reviewing The Data With the testing from Excercise 1 completed, we can begin to explore the results of the emulation. 1. Note the results in the top three panels for Overall Combined, Overall Prevention, and Overall Detection scores. 2. In the Overall Detection score panel, expand Security Controls to see detection rates for security controls involved in testing. 8 3. Under the Results menu item, click on Summary 4. Scroll down the results page until you find the Scenario results for Test Web access to Social Media site Facebook. 5. Click on the entry for Test Web access to Social Media site Facebook. 9 6. If you've forgotten what this scenario is trying to accomplish, click the ? icon next to the scenario title. 7. Expand the Activity Details and make note of the response code received vs. the response code anticipated. 8. Expand the INDICATORS OF COMPROMISE (IOCS) DETAILS a. Make a note of the following information: i. Destination: ii. HTTP Method iii. Protocols iv. Request Path v. Source Port

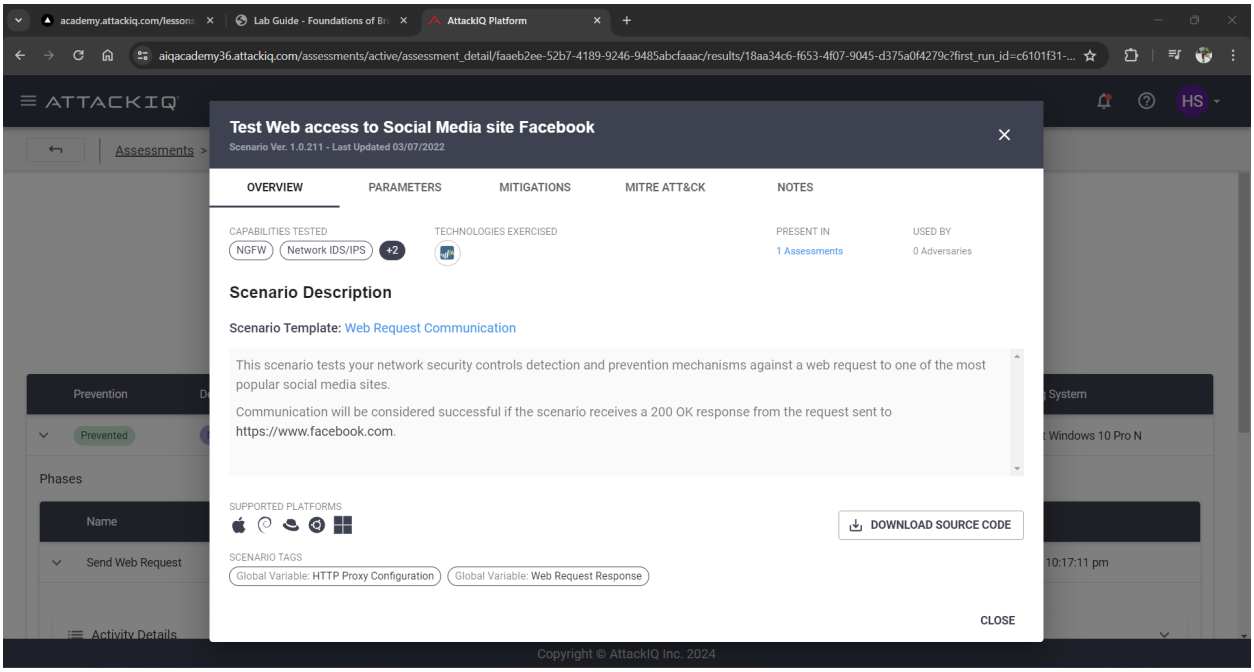

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac?section=run
ATTACKIQ
HS
Assessments > Content Filtering (On Demand)
Setup
On Demand
Scheduled OFF
Results
Reports
Team 01
Notifications OFF
RUN NOW
Integration Manager Status: ACTIVE
2
Total
2
Active
Scenarios Complete
Integrations Complete
Scenarios 12
Assets 2
Integrations DETAILS
PAN Panorama
Assessment in Progress
Date Status Created by Prevention Scenarios Assets Detection
No assessments on demand run in progress
Previous Runs
Date Status Created by Prevention Scenarios Assets Detection
04/23/2024
Copyright © AttackIQ Inc. 2024

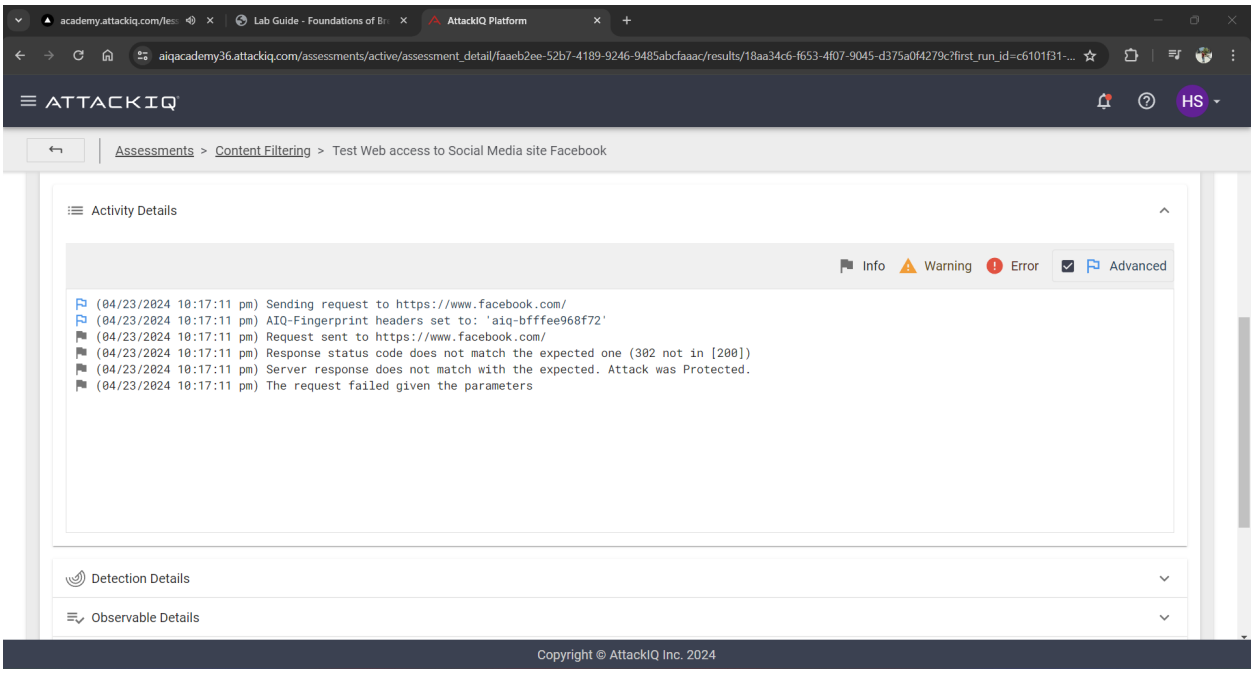

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac?section=findings
ATTACKIQ
HS
Assessments > Content Filtering (Results)
On Demand
Scheduled OFF
Results
Summary
History
MITRE ATT&CK
Mitigations
Reports
Team 01
Notifications OFF
Select a run
04/23/2024 - 10:15 pm
Overall Results
2 out of 24 Scenario Runs were Prevented or Detected
Tests Results
Gun sites 0/6
Pornography sites 0/6
Social Media sites 2/6
Streaming sites 0/6
Next Steps
Copyright © AttackIQ Inc. 2024

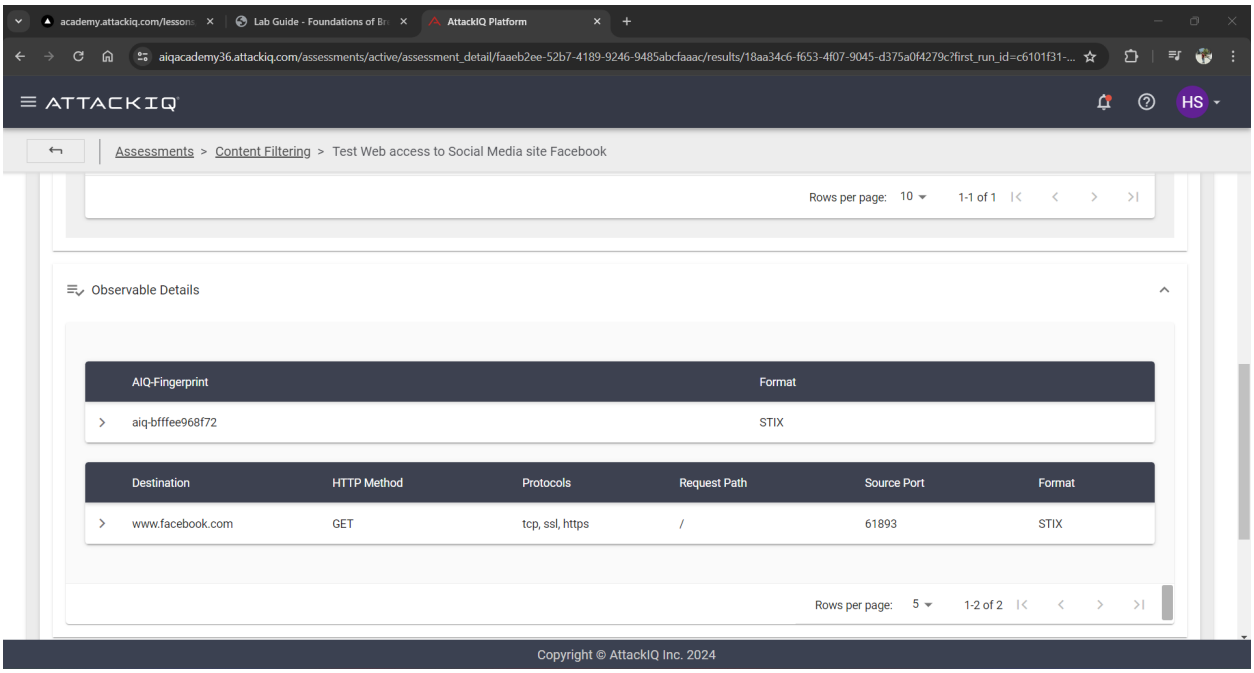

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac?section=findings&sub_section=scenario_results
ATTACKIQ
HS
Assessments > Content Filtering (Results)
Setup
On Demand
Scheduled OFF
Results
Summary
History
MITRE ATT&CK
Mitigations
Reports
Team
Showing 24 of 24 results
EXPORT CSV
no filters selected
REFRESH
FILTER
04/23/2024 10:15 pm | Social Media sites | Test Web access to Social Media site Facebook | SYSTEM | acad3141-un | Prevented | Not Detected | View (0)
04/23/2024 10:15 pm | Social Media sites | Test Web access to Social Media site Facebook | SYSTEM | acad5790-prot | Prevented | Not Detected | View (0)
04/23/2024 10:15 pm | Social Media sites | Test Web access to Social Media site Instagram | SYSTEM | acad3141-un | Not Prevented | Not Detected | View (0)
04/23/2024 10:15 pm | Social Media sites | Test Web access to Social Media site Instagram | SYSTEM | acad5790-prot | Not Prevented | Not Detected | View (0)
Copyright © AttackIQ Inc. 2024

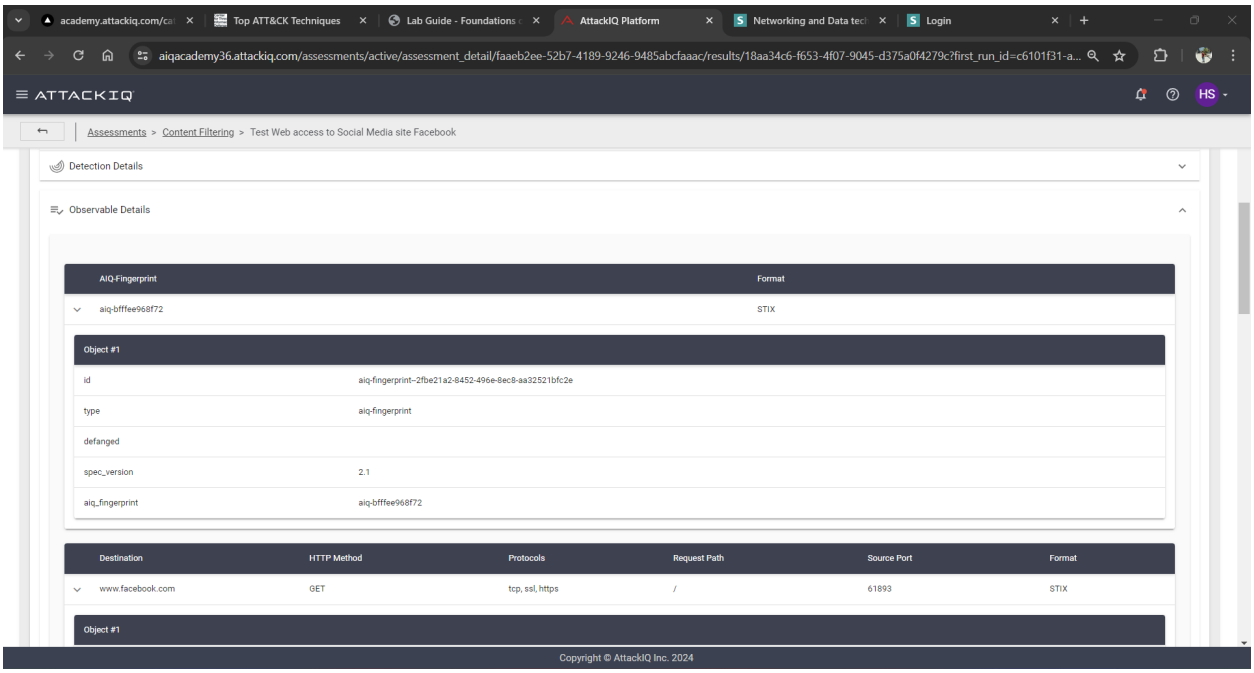

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-...
ATTACKIQ
HS
Assessments > Content Filtering > Test Web access to Social Media site Facebook
Test Web access to Social Media site Facebook
Assessment: Content Filtering
04/23/2024 - 10:17 pm
Prevented
Not Detected
Web Request Response
HTTP Proxy Configuration
Showing result 14 of 24
Prevention | Detection | User Privileges | Hostname | Installed Technologies | IP Address | Operating System
Prevented | Not Detected | SYSTEM | acad5790-prot | 172.16.14.154 | Microsoft Windows 10 Pro N
Phases
Name | Critical Phase | Prevention | Detection | Start Time | End Time
Send Web Request | Critical | Prevented | Not Detected | 04/23/2024 10:17:11 pm | 04/23/2024 10:17:11 pm
Activity Details
Copyright © AttackIQ Inc. 2024

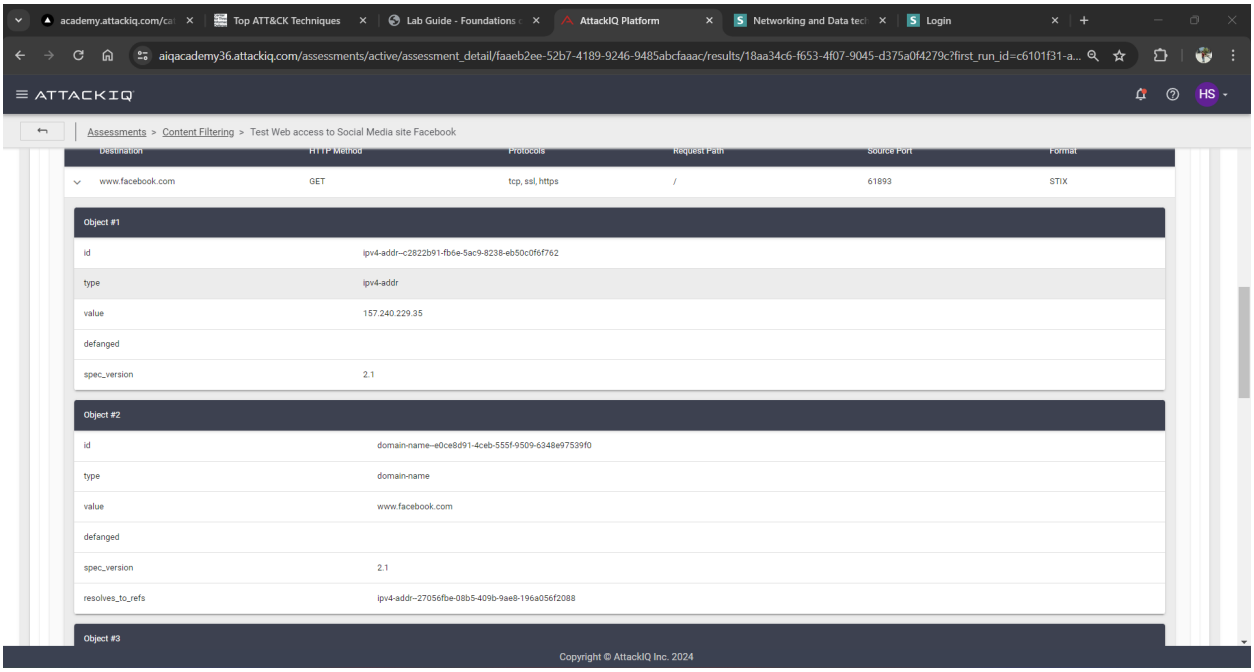

academy.attackiq.com/les
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-...
ATTACKIQ
HS
Assessments > Content Filtering > Test Web access to Social Media site Facebook
Prevention
Detection
User Privileges
Hostname
Installed Technologies
IP Address
Operating System
Prevented
Not Detected
SYSTEM
acad5790-prot
172.16.14.154
Microsoft Windows 10 Pro N
Phases
Name
Critical Phase
Prevention
Detection
Start Time
End Time
Send Web Request
Critical
Prevented
Not Detected
04/23/2024 10:17:11 pm
04/23/2024 10:17:11 pm
Activity Details
Detection Details
Observable Details
Integration Expected Observables
Mitigations
Copyright © AttackIQ Inc. 2024

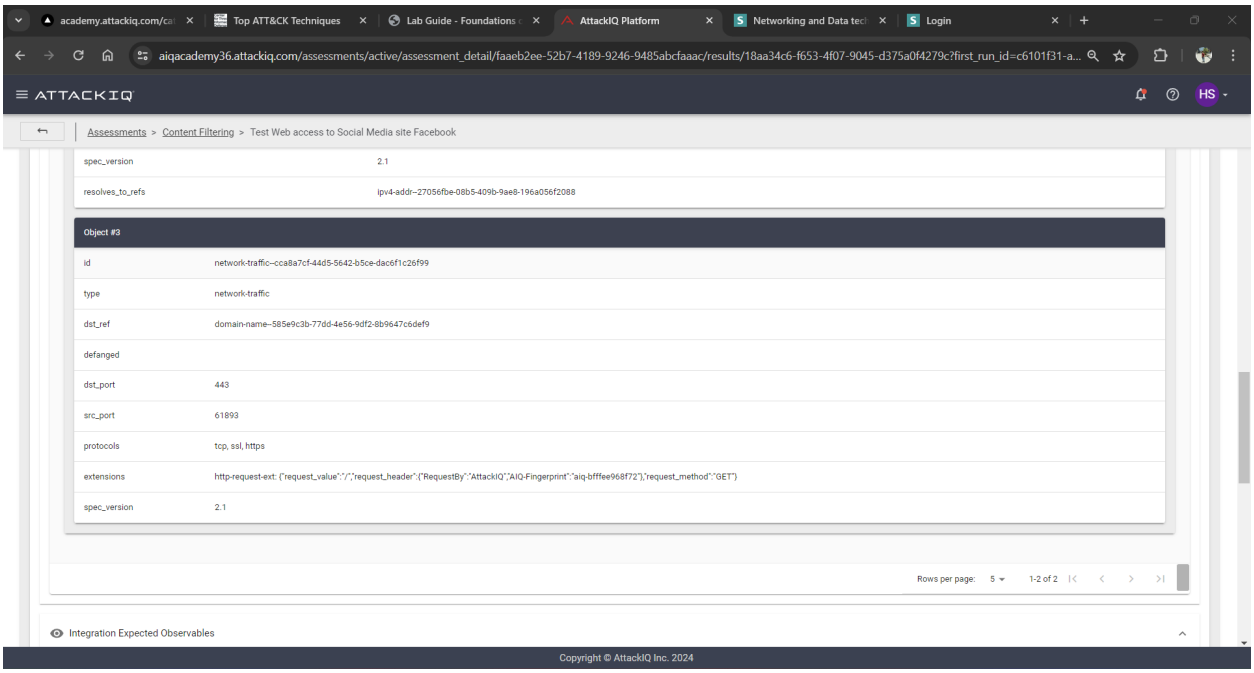

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-...
ATTACKIQ
HS
Assessments
Test Web access to Social Media site Facebook
Scenario Ver. 1.0.211 - Last Updated 03/07/2022
OVERVIEW
PARAMETERS
MITIGATIONS
MITRE ATT&CK
NOTES
CAPABILITIES TESTED
NGFW
Network IDS/IPS
+2
TECHNOLOGIES EXERCISED
PRESENT IN
1 Assessments
USED BY
0 Adversaries
Scenario Description
Scenario Template: Web Request Communication
This scenario tests your network security controls detection and prevention mechanisms against a web request to one of the most popular social media sites.
Communication will be considered successful if the scenario receives a 200 OK response from the request sent to https://www.facebook.com.
SUPPORTED PLATFORMS
DOWNLOAD SOURCE CODE
SCENARIO TAGS
Global Variable: HTTP Proxy Configuration
Global Variable: Web Request Response
CLOSE
Copyright © AttackIQ Inc. 2024


academy.attackiq.com/les
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-...
ATTACKIQ
HS
Assessments > Content Filtering > Test Web access to Social Media site Facebook
Activity Details
Info
Warning
Error
Advanced
(04/23/2024 10:17:11 pm) Sending request to https://www.facebook.com/
(04/23/2024 10:17:11 pm) AIQ-Fingerprint headers set to: 'aiq-bfffee968f72'
(04/23/2024 10:17:11 pm) Request sent to https://www.facebook.com/
(04/23/2024 10:17:11 pm) Response status code does not match the expected one (302 not in [200])
(04/23/2024 10:17:11 pm) Server response does not match with the expected. Attack was Protected.
(04/23/2024 10:17:11 pm) The request failed given the parameters
Detection Details
Observable Details
Copyright © AttackIQ Inc. 2024

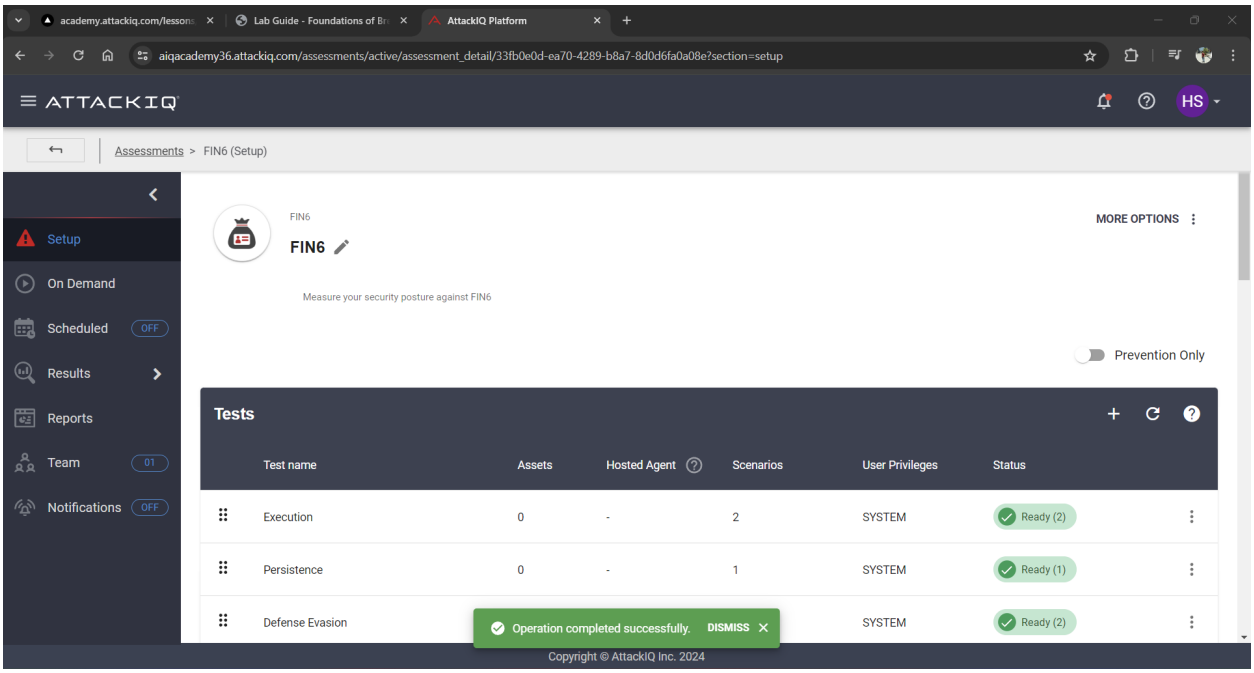

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-...
ATTACKIQ
HS
Assessments > Content Filtering > Test Web access to Social Media site Facebook
Rows per page: 10
1-1 of 1
Observable Details
AIQ-Fingerprint
Format
aiq-bfffee968f72
STIX
Destination
HTTP Method
Protocols
Request Path
Source Port
Format
www.facebook.com
GET
tcp, ssl, https
/
61893
STIX
Rows per page: 5
1-2 of 2
Copyright © AttackIQ Inc. 2024

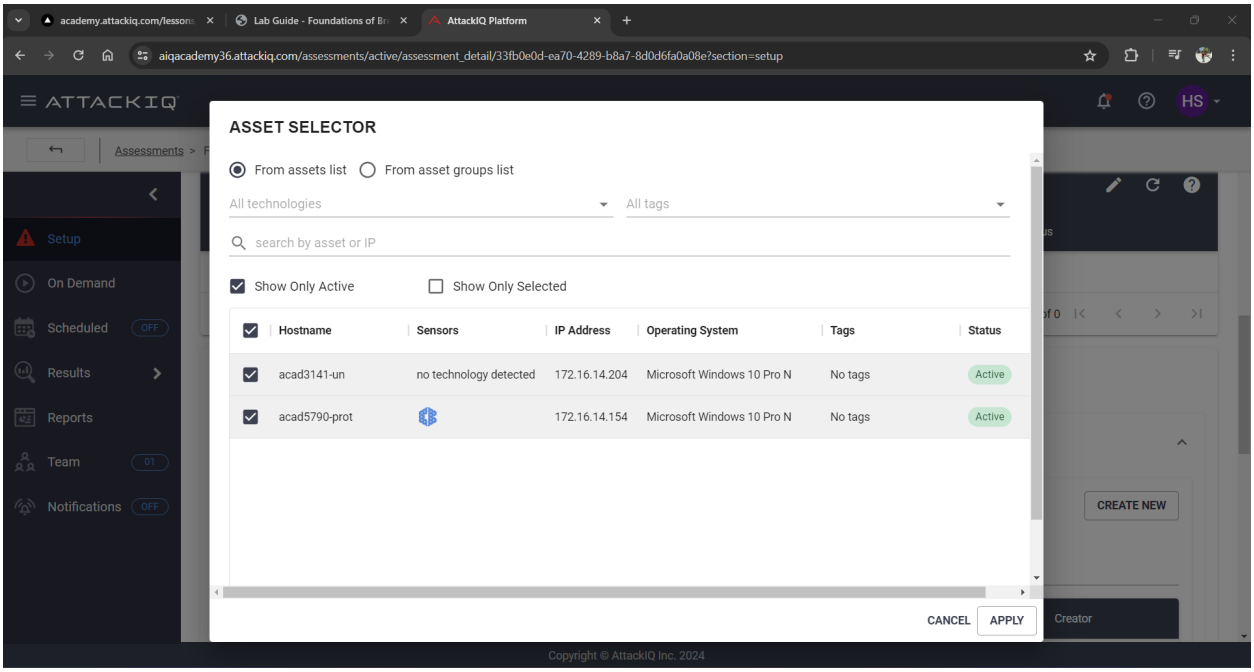

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-a...
ATTACKIQ
HS
Assessments > Content Filtering > Test Web access to Social Media site Facebook
Detection Details
Observable Details
AIQ-Fingerprint
Format
aiq-bfffee968f72
STIX
Object #1
id
aiq-fingerprint--2fbe21a2-8452-496e-8ec8-aa32521bfc2e
type
aiq-fingerprint
defanged
spec_version
2.1
aiq_fingerprint
aiq-bfffee968f72
Destination
HTTP Method
Protocols
Request Path
Source Port
Format
www.facebook.com
GET
tcp, ssl, https
/
61893
STIX
Object #1
Copyright © AttackIQ Inc. 2024

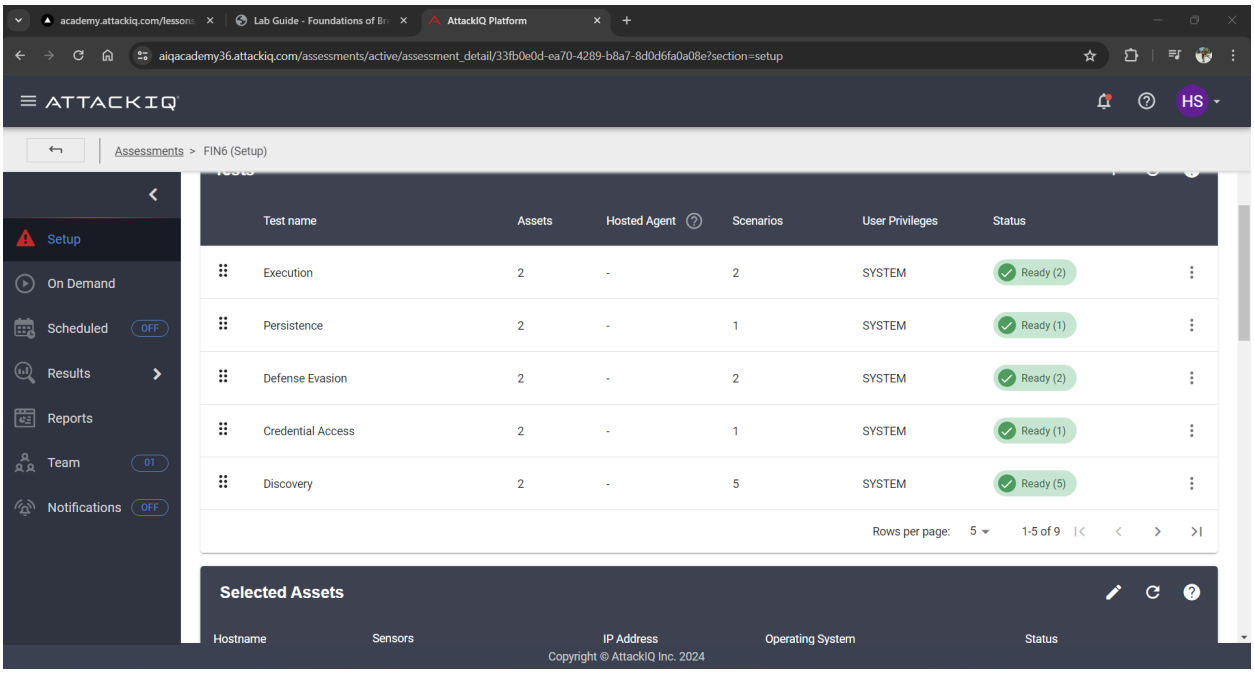

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/faaeb2ee-52b7-4189-9246-9485abcfaaac/results/18aa34c6-f653-4f07-9045-d375a0f4279c?first_run_id=c6101f31-a...
ATTACKIQ
HS
Assessments > Content Filtering > Test Web access to Social Media site Facebook
Destination
HTTP Method
Protocols
Request Path
Source Port
Format
www.facebook.com
GET
tcp, ssl, https
/
61893
STIX
Object #1
id
ipv4-addr--c2822b91-fb6e-5ac9-8238-eb50c0f6f762
type
ipv4-addr
value
157.240.229.35
defanged
spec_version
2.1
Object #2
id
domain-name--e0ce8d91-4ceb-555f-9509-6348e97539f0
type
domain-name
value
www.facebook.com
defanged
spec_version
2.1
resolves_to_refs
ipv4-addr--27056fbe-08b5-409b-9ae8-196a056f2088
Object #3
Copyright © AttackIQ Inc. 2024

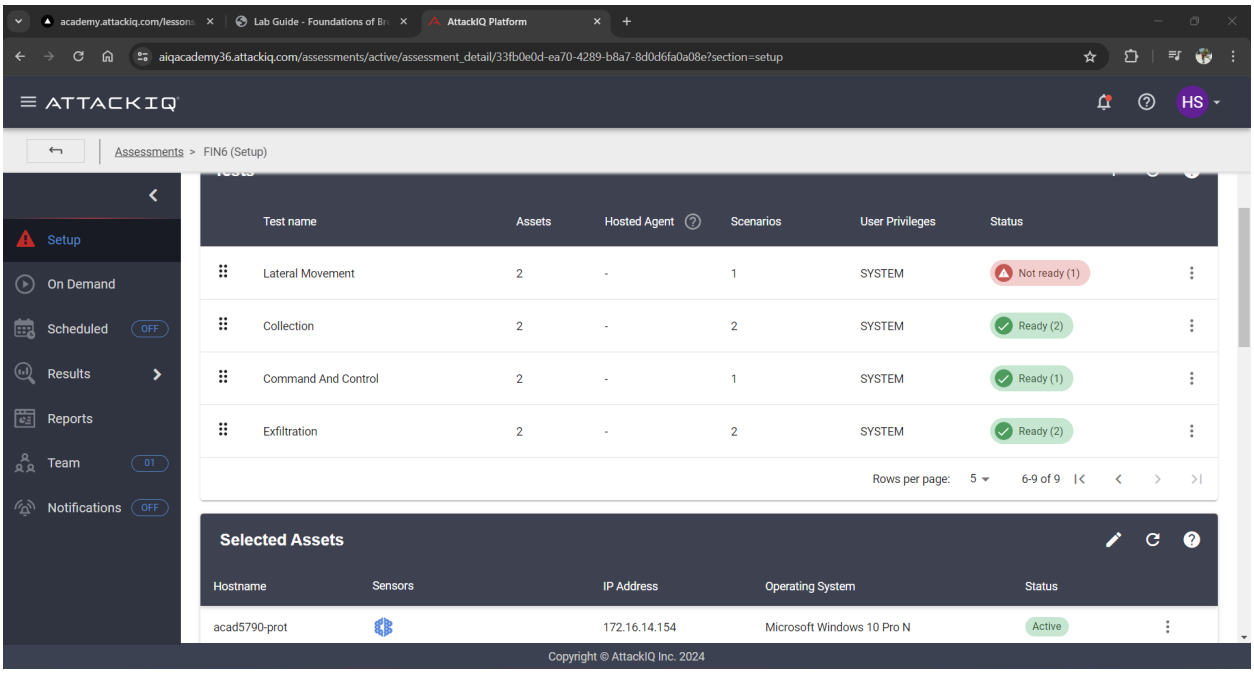


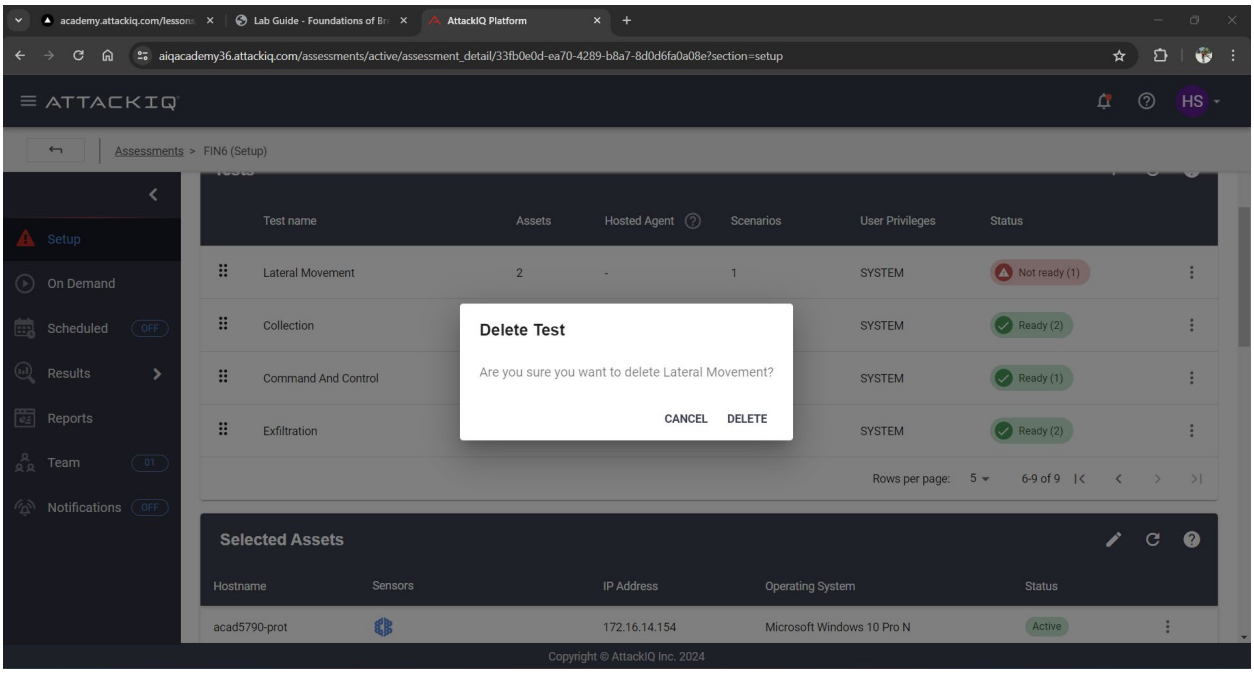
Exercise 3: FIN6 Emulation 1. Click on the three horizontal lines in the top left-hand corner of the screen to open the main menu. 2. Click on ASSESSMENT in the main menu. 11 3. Click on the CREATE NEW ASSESSMENT button 4. Click CHOOSE TEMPLATE. 5. On the Assessment Templates page, click the dropdown under Select template type, and choose Threat Emulation.. 12 6. Find the FIN6 assessment template on the page, and click it. 7. Click Create New 8. Add both assets to the Assessment. a. Click the Manage Assets button b. Click the checkboxes of BOTH assets listed. c. Click Apply 13 9. Under the assets, where it lists the tests configured, click on the three dots under the ACTION column for the test name Lateral Movement. 10. Click DELETE TEST. 11. Click OK 12. Click the Continue button in the bottom right-hand corner of the page. 13. Click the Run Now button

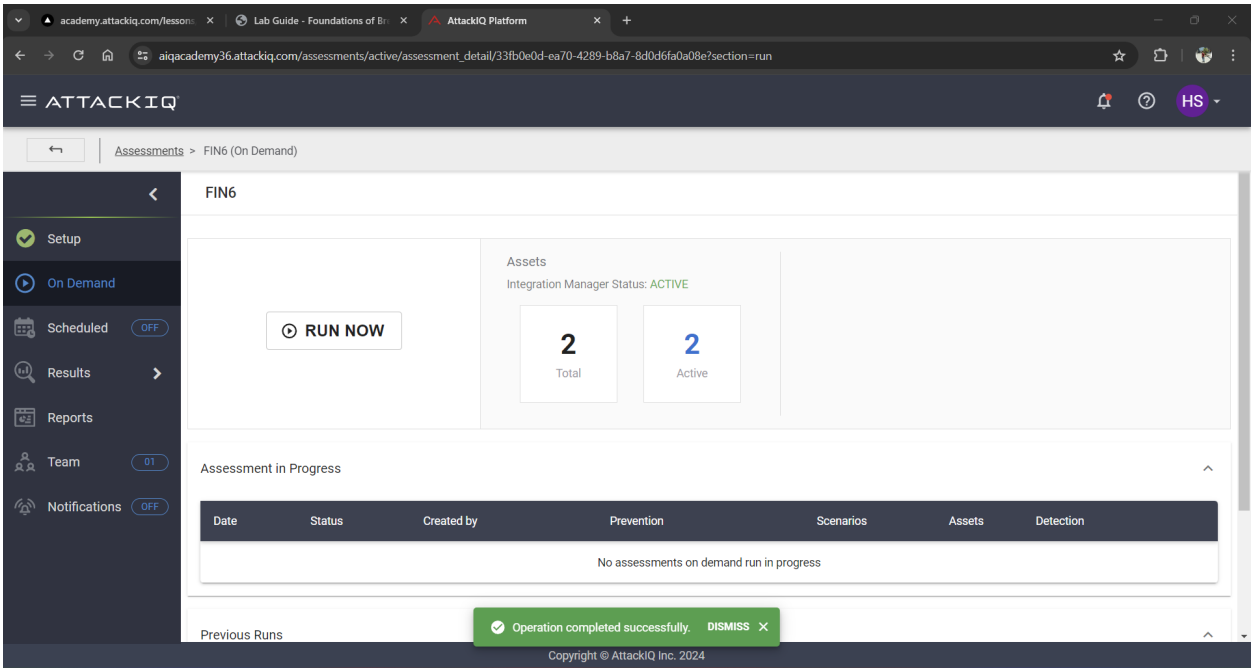

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=setup
ATTACKIQ
HS
Assessments > FIN6 (Setup)
Setup
On Demand
Scheduled
OFF
Results
Reports
Team
01
Notifications
OFF
FIN6
FIN6
Measure your security posture against FIN6
MORE OPTIONS
Prevention Only
Tests
Test name
Assets
Hosted Agent
Scenarios
User Privileges
Status
Execution
0
-
2
SYSTEM
Ready (2)
Persistence
0
-
1
SYSTEM
Ready (1)
Defense Evasion
SYSTEM
Ready (2)
Operation completed successfully.
DISMISS
Copyright © AttackIQ Inc. 2024

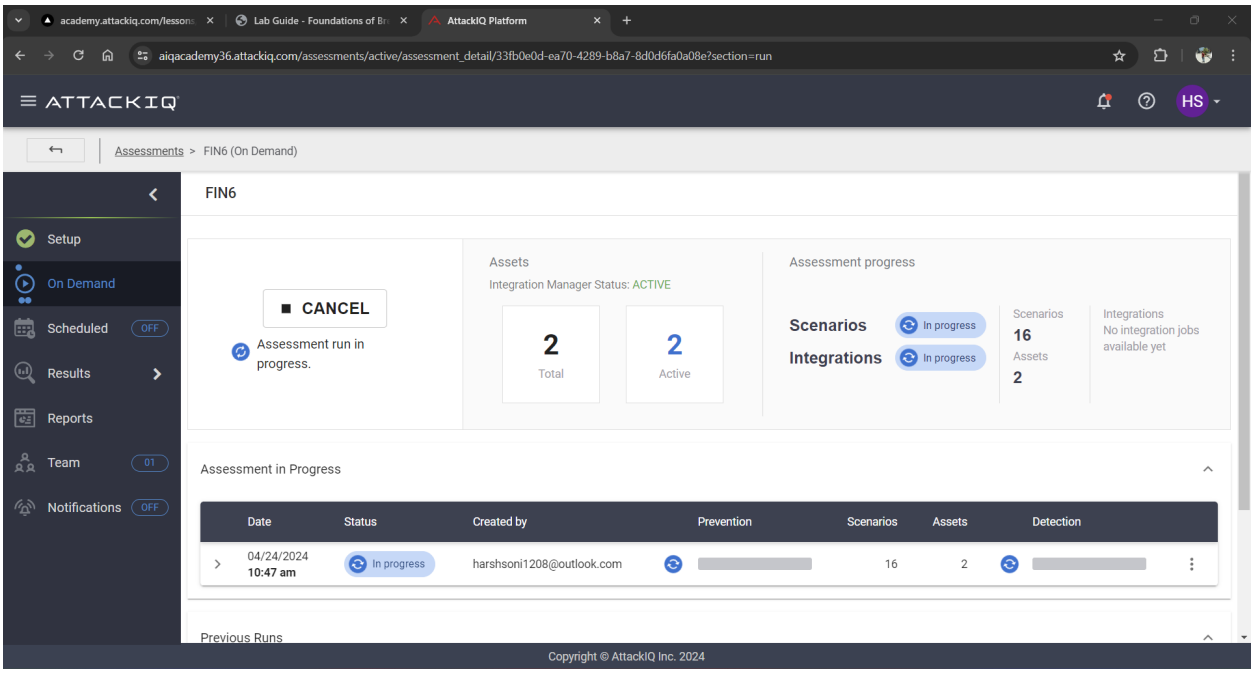

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=setup
ATTACKIQ
HS
ASSET SELECTOR
From assets list
From asset groups list
All technologies
All tags
search by asset or IP
Show Only Active
Show Only Selected
Hostname
Sensors
IP Address
Operating System
Tags
Status
acad3141-un
no technology detected
172.16.14.204
Microsoft Windows 10 Pro N
No tags
Active
acad5790-prot
172.16.14.154
Microsoft Windows 10 Pro N
No tags
Active
CANCEL
APPLY
CREATE NEW
Creator
Copyright © AttackIQ Inc. 2024


academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=setup
ATTACKIQ
HS
Assessments > FIN6 (Setup)
Setup
On Demand
Scheduled OFF
Results
Reports
Team 01
Notifications OFF
Test name
Assets
Hosted Agent
Scenarios
User Privileges
Status
Execution 2 - 2 SYSTEM Ready (2)
Persistence 2 - 1 SYSTEM Ready (1)
Defense Evasion 2 - 2 SYSTEM Ready (2)
Credential Access 2 - 1 SYSTEM Ready (1)
Discovery 2 - 5 SYSTEM Ready (5)
Rows per page: 5
1-5 of 9
Selected Assets
Hostname
Sensors
IP Address
Operating System
Status
Copyright © AttackIQ Inc. 2024

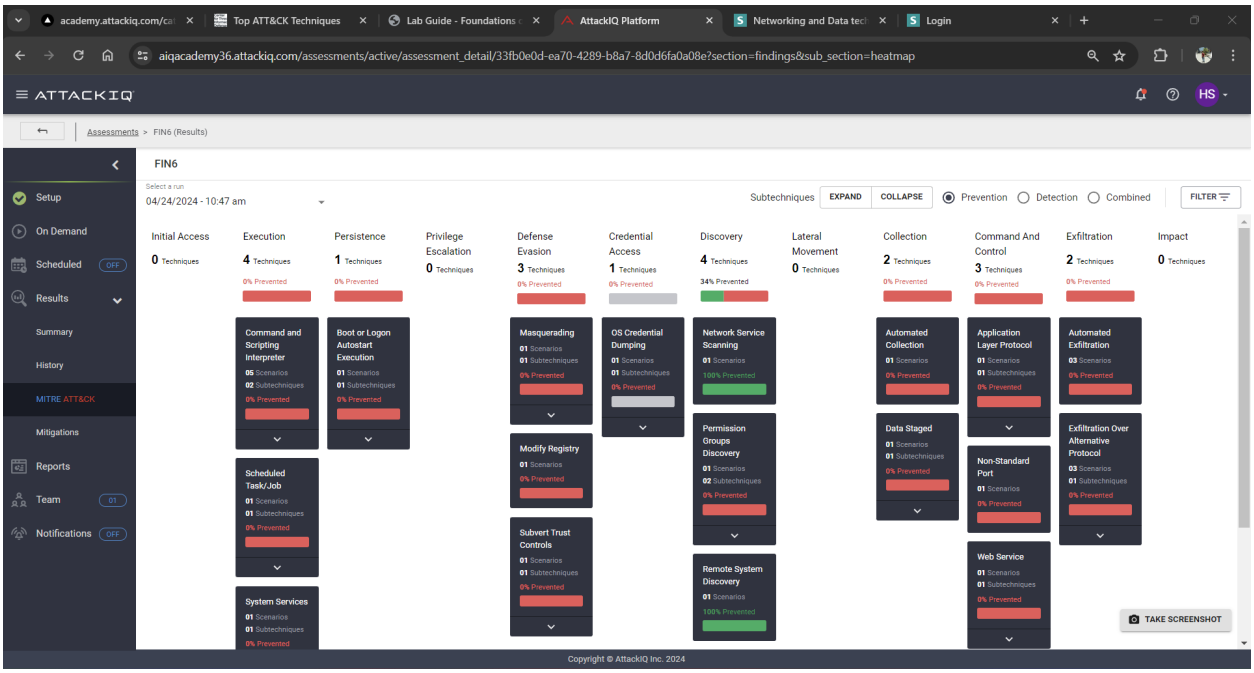

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=setup
ATTACKIQ
HS
Assessments > FIN6 (Setup)
Setup
On Demand
Scheduled OFF
Results
Reports
Team 01
Notifications OFF
Test name
Assets
Hosted Agent
Scenarios
User Privileges
Status
Lateral Movement 2 - 1 SYSTEM Not ready (1)
Collection 2 - 2 SYSTEM Ready (2)
Command And Control 2 - 1 SYSTEM Ready (1)
Exfiltration 2 - 2 SYSTEM Ready (2)
Rows per page: 5
6-9 of 9
Selected Assets
Hostname
Sensors
IP Address
Operating System
Status
acad5790-prot 172.16.14.154 Microsoft Windows 10 Pro N Active
Copyright © AttackIQ Inc. 2024

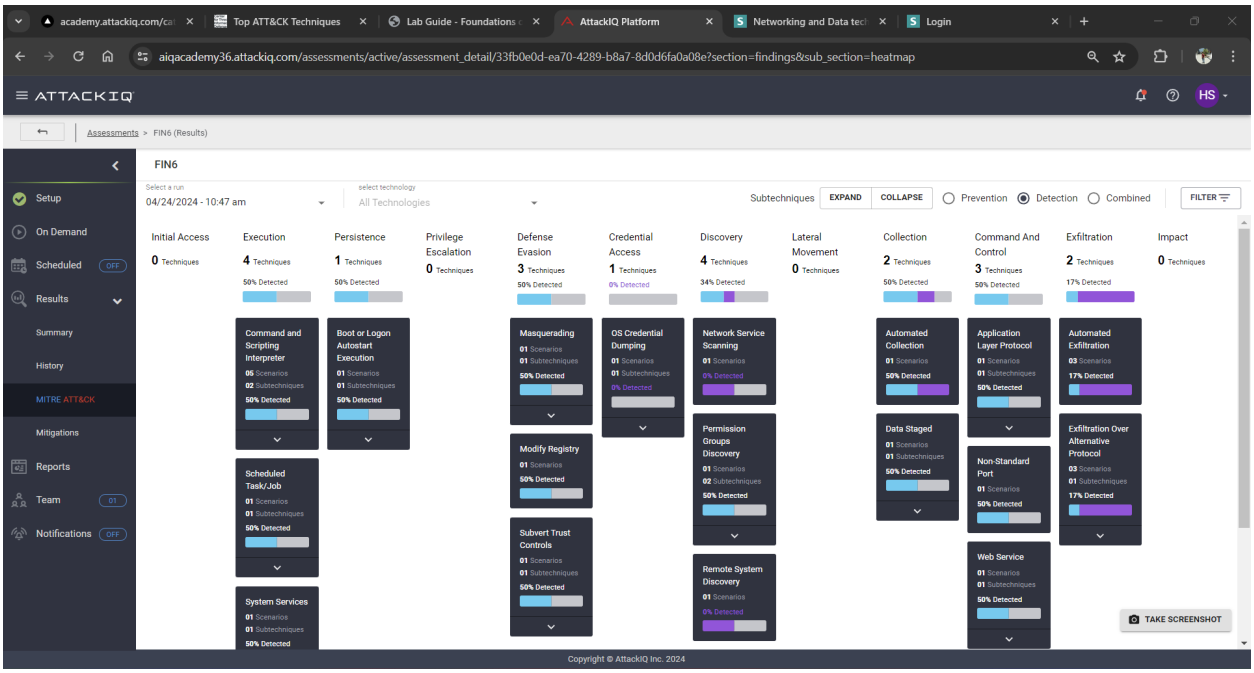

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=setup
ATTACKIQ
HS
Assessments > FIN6 (Setup)
Setup
On Demand
Scheduled
OFF
Results
Reports
Team
01
Notifications
OFF
Test name
Assets
Hosted Agent
Scenarios
User Privileges
Status
Lateral Movement
2
-
1
SYSTEM
Not ready (1)
Collection
SYSTEM
Ready (2)
Command And Control
SYSTEM
Ready (1)
Exfiltration
SYSTEM
Ready (2)
Delete Test
Are you sure you want to delete Lateral Movement?
CANCEL
DELETE
Rows per page: 5
6-9 of 9
Selected Assets
Hostname
Sensors
IP Address
Operating System
Status
acad5790-prot
172.16.14.154
Microsoft Windows 10 Pro N
Active
Copyright © AttackIQ Inc. 2024

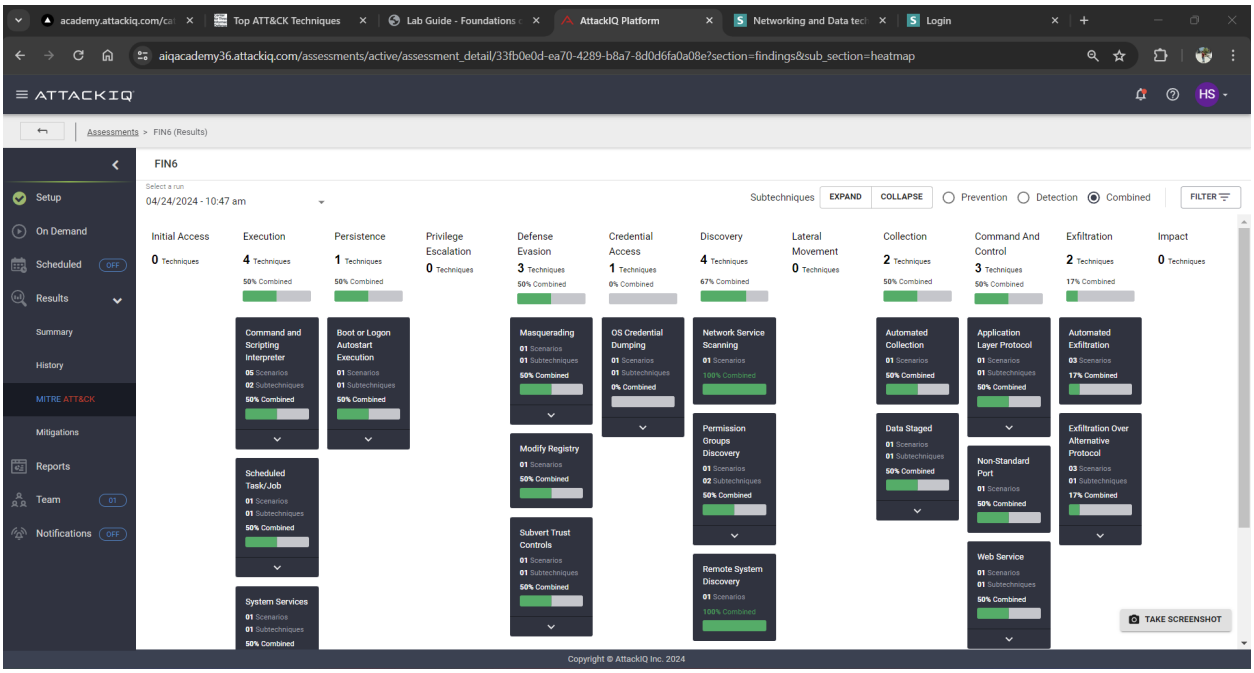

academy.attackiq.com/lessons
Lab Guide - Foundations of Br
AttackIQ Platform
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=run
ATTACKIQ
HS
Assessments > FIN6 (On Demand)
FIN6
Setup
On Demand
Scheduled
OFF
Results
Reports
Team
01
Notifications
OFF
RUN NOW
Assets
Integration Manager Status: ACTIVE
2
Total
2
Active
Assessment in Progress
Date
Status
Created by
Prevention
Scenarios
Assets
Detection
No assessments on demand run in progress
Previous Runs
Operation completed successfully.
DISMISS
Copyright © AttackIQ Inc. 2024

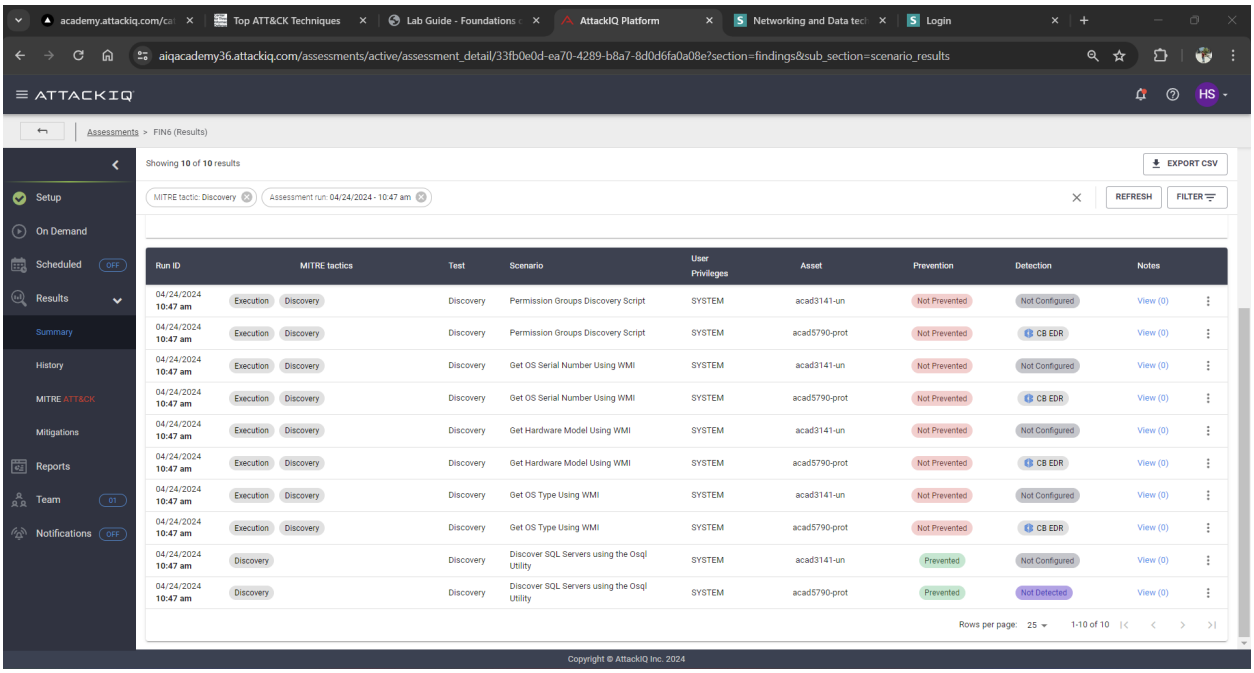


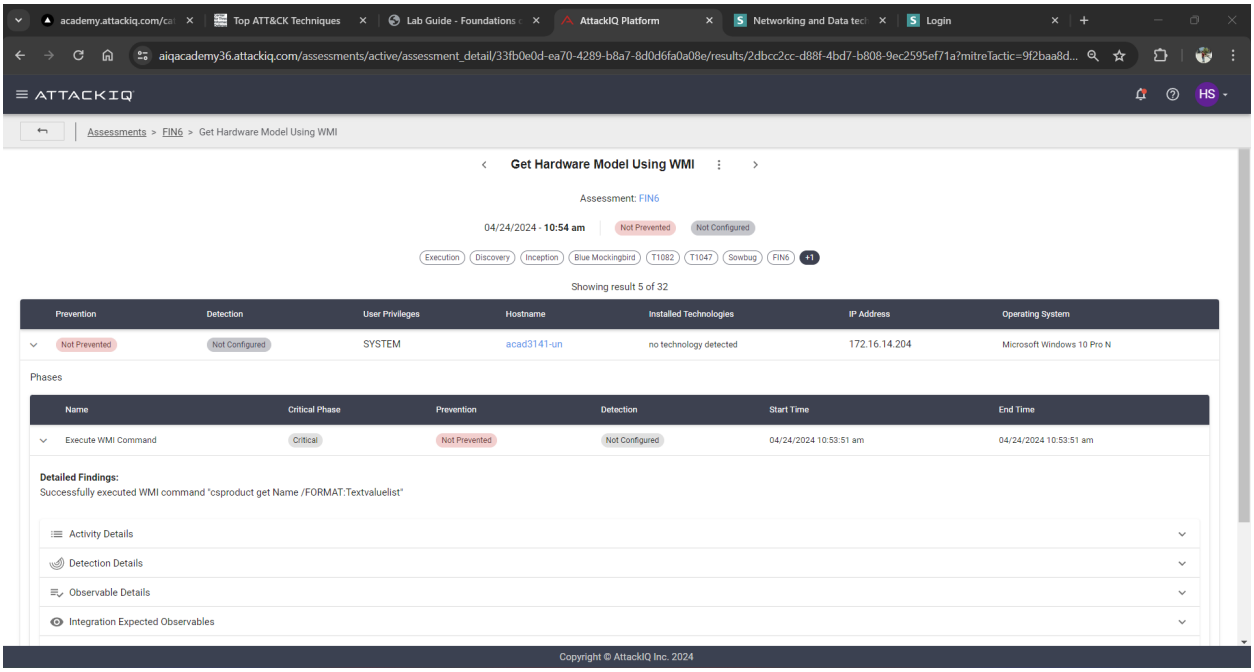
Exercise 4: MITRE ATT&CK Mapping 1. In the left-hand menu, under Results, click on MITRE ATT&CK 2. Review the results for Prevention. 3. Click on the Detection radio button to toggle the view to detection results. 4. Click the Combined radio button to toggle the view to combined detection and prevention results. 5. Click on the Discover tactic column heading. 6. On the Results page you will see a listing of results that have been filtered to display scenarios from the FIN6 assessment that fall under the ATT&CK tactic of Discovery. 15 7. Click on the line item for Get Hardware Model Using WMI (either one is okay). 8. Click the ? icon next to the scenario title and read the scenario description to get a better understanding of what this scenario is trying to accomplish. 9. Make a note of the WMI command used to obtain the hardware model, you will need this information for your final exam. 16 10. Review the Activity Details to see the output or error code for the scenario. 11. Review the Indicators of Compromise (IOCs) Details

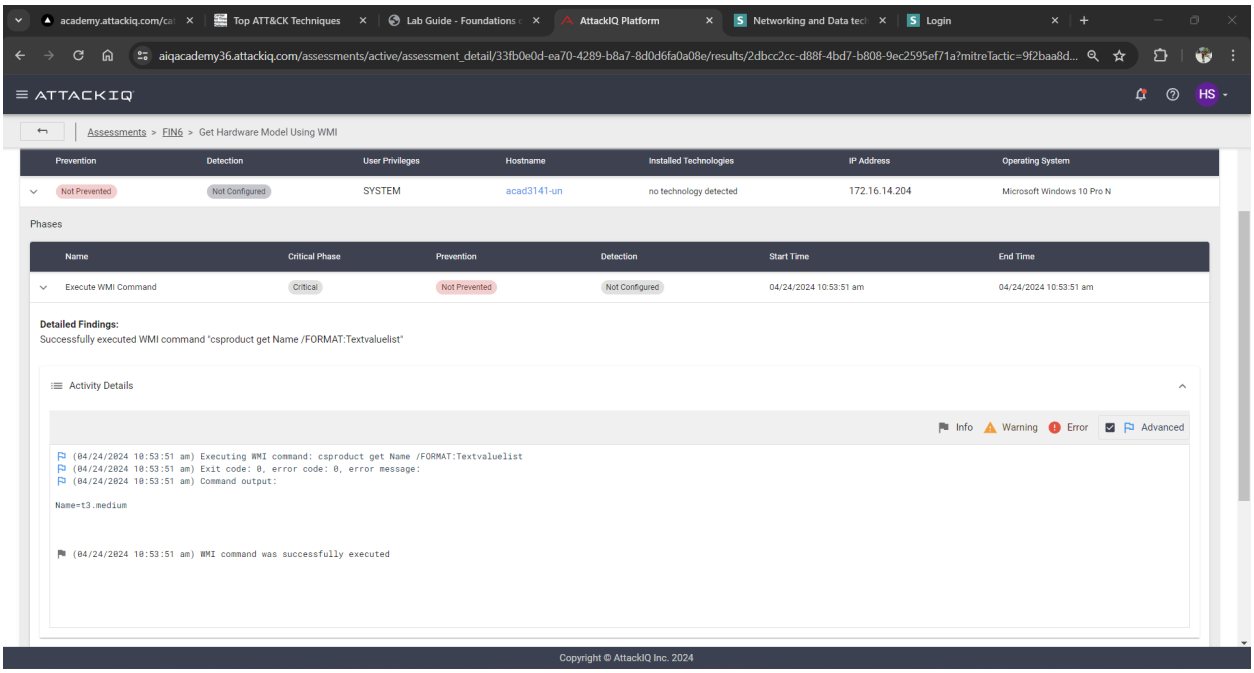

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=findings&sub_section=heatmap
ATTACKIQ
HS
Assessments > FIN6 (Results)
FIN6
Setup
On Demand
Scheduled
Results
Summary
History
MITRE ATT&CK
Mitigations
Reports
Team
Notifications
Select a run
04/24/2024 - 10:47 am
Subtechniques
EXPAND
COLLAPSE
Prevention
Detection
Combined
FILTER
Initial Access
0 Techniques
Execution
4 Techniques
0% Prevented
Persistence
1 Techniques
0% Prevented
Privilege Escalation
0 Techniques
Defense Evasion
3 Techniques
0% Prevented
Credential Access
1 Techniques
0% Prevented
Discovery
4 Techniques
34% Prevented
Lateral Movement
0 Techniques
Collection
2 Techniques
0% Prevented
Command And Control
3 Techniques
0% Prevented
Exfiltration
2 Techniques
0% Prevented
Impact
0 Techniques
Command and Scripting Interpreter
05 Scenarios
02 Subtechniques
0% Prevented
Boot or Logon Autostart Execution
01 Scenarios
01 Subtechniques
0% Prevented
Scheduled Task/Job
01 Scenarios
01 Subtechniques
0% Prevented
System Services
01 Scenarios
01 Subtechniques
0% Prevented
Masquerading
01 Scenarios
01 Subtechniques
0% Prevented
Modify Registry
01 Scenarios
0% Prevented
Subvert Trust Controls
01 Scenarios
01 Subtechniques
0% Prevented
OS Credential Dumping
01 Scenarios
01 Subtechniques
0% Prevented
Network Service Scanning
01 Scenarios
100% Prevented
Permission Groups Discovery
01 Scenarios
02 Subtechniques
0% Prevented
Remote System Discovery
01 Scenarios
100% Prevented
Automated Collection
01 Scenarios
0% Prevented
Data Staged
01 Scenarios
01 Subtechniques
0% Prevented
Application Layer Protocol
01 Scenarios
01 Subtechniques
0% Prevented
Non-Standard Port
01 Scenarios
0% Prevented
Web Service
01 Scenarios
01 Subtechniques
0% Prevented
Automated Exfiltration
03 Scenarios
0% Prevented
Exfiltration Over Alternative Protocol
03 Scenarios
01 Subtechniques
0% Prevented
TAKE SCREENSHOT
Copyright © AttackIQ Inc. 2024

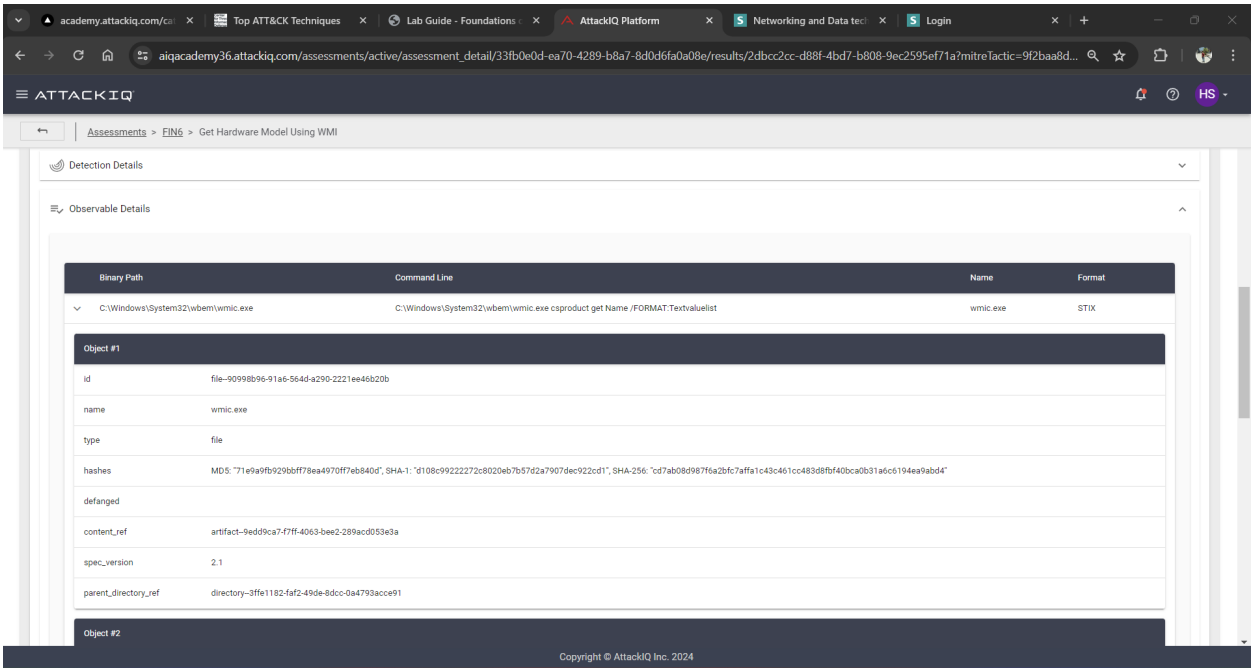

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=findings&sub_section=heatmap
ATTACKIQ
HS
Assessments > FIN6 (Results)
FIN6
Setup
On Demand
Scheduled
Results
Summary
History
MITRE ATT&CK
Mitigations
Reports
Team
Notifications
Select a run
04/24/2024 - 10:47 am
select technology
All Technologies
Subtechniques
EXPAND
COLLAPSE
Prevention
Detection
Combined
FILTER
Initial Access
0 Techniques
Execution
4 Techniques
50% Detected
Persistence
1 Techniques
50% Detected
Privilege Escalation
0 Techniques
Defense Evasion
3 Techniques
50% Detected
Credential Access
1 Techniques
0% Detected
Discovery
4 Techniques
34% Detected
Lateral Movement
0 Techniques
Collection
2 Techniques
50% Detected
Command And Control
3 Techniques
50% Detected
Exfiltration
2 Techniques
17% Detected
Impact
0 Techniques
Command and Scripting Interpreter
05 Scenarios
02 Subtechniques
50% Detected
Boot or Logon Autostart Execution
01 Scenarios
01 Subtechniques
50% Detected
Scheduled Task/Job
01 Scenarios
01 Subtechniques
50% Detected
System Services
01 Scenarios
01 Subtechniques
50% Detected
Masquerading
01 Scenarios
01 Subtechniques
50% Detected
Modify Registry
01 Scenarios
50% Detected
Subvert Trust Controls
01 Scenarios
01 Subtechniques
50% Detected
OS Credential Dumping
01 Scenarios
01 Subtechniques
0% Detected
Network Service Scanning
01 Scenarios
0% Detected
Permission Groups Discovery
01 Scenarios
02 Subtechniques
50% Detected
Remote System Discovery
01 Scenarios
0% Detected
Automated Collection
01 Scenarios
50% Detected
Data Staged
01 Scenarios
01 Subtechniques
50% Detected
Application Layer Protocol
01 Scenarios
01 Subtechniques
50% Detected
Non-Standard Port
01 Scenarios
50% Detected
Web Service
01 Scenarios
01 Subtechniques
50% Detected
Automated Exfiltration
03 Scenarios
17% Detected
Exfiltration Over Alternative Protocol
03 Scenarios
01 Subtechniques
17% Detected
TAKE SCREENSHOT
Copyright © AttackIQ Inc. 2024

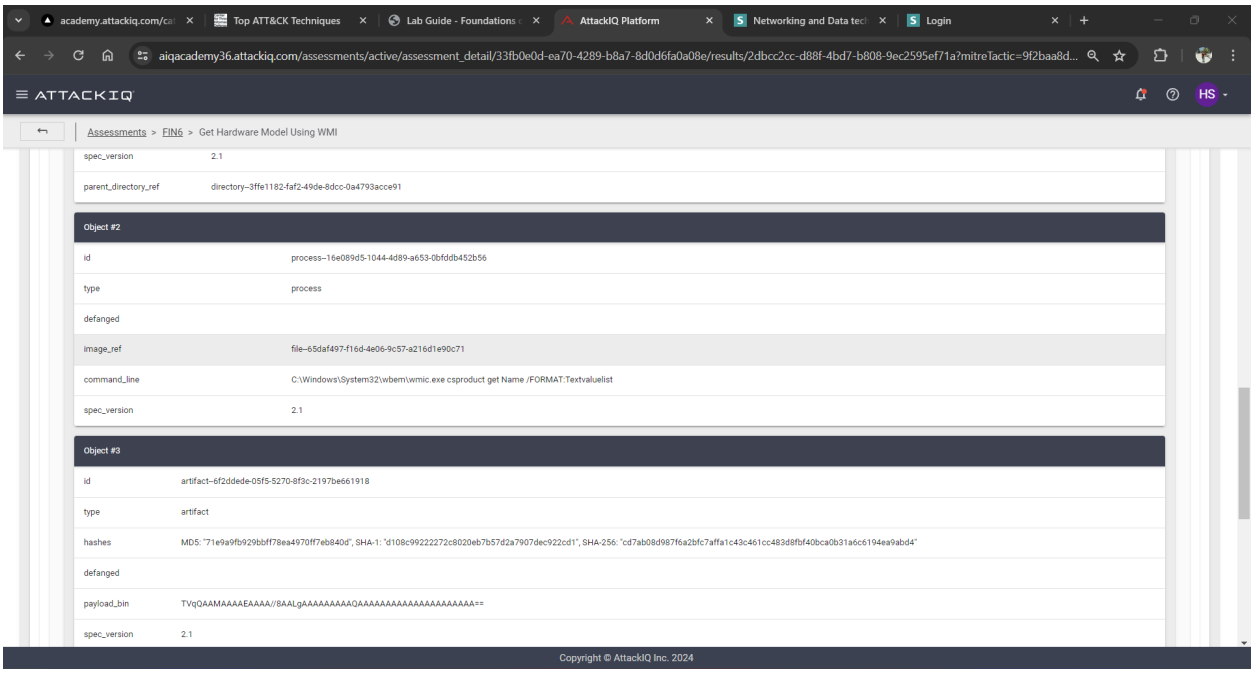

Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=findings&sub_section=heatmap
ATTACKIQ
HS
Assessments > FIN6 (Results)
FIN6
Select a run
04/24/2024 - 10:47 am
Subtechniques
EXPAND
COLLAPSE
Prevention
Detection
Combined
FILTER
Setup
On Demand
Scheduled
OFF
Results
Summary
History
MITRE ATT&CK
Mitigations
Reports
Team
01
Notifications
OFF
Initial Access
0 Techniques
Execution
4 Techniques
50% Combined
Command and Scripting Interpreter
05 Scenarios
02 Subtechniques
50% Combined
Scheduled Task/Job
01 Scenarios
01 Subtechniques
50% Combined
System Services
01 Scenarios
01 Subtechniques
50% Combined
Persistence
1 Techniques
50% Combined
Boot or Logon Autostart Execution
01 Scenarios
01 Subtechniques
50% Combined
Privilege Escalation
0 Techniques
Defense Evasion
3 Techniques
50% Combined
Masquerading
01 Scenarios
01 Subtechniques
50% Combined
Modify Registry
01 Scenarios
50% Combined
Subvert Trust Controls
01 Scenarios
01 Subtechniques
50% Combined
Credential Access
1 Techniques
0% Combined
OS Credential Dumping
01 Scenarios
01 Subtechniques
0% Combined
Discovery
4 Techniques
67% Combined
Network Service Scanning
01 Scenarios
100% Combined
Permission Groups Discovery
01 Scenarios
02 Subtechniques
50% Combined
Remote System Discovery
01 Scenarios
100% Combined
Lateral Movement
0 Techniques
Collection
2 Techniques
50% Combined
Automated Collection
01 Scenarios
50% Combined
Data Staged
01 Scenarios
01 Subtechniques
50% Combined
Command And Control
3 Techniques
50% Combined
Application Layer Protocol
01 Scenarios
01 Subtechniques
50% Combined
Non-Standard Port
01 Scenarios
50% Combined
Web Service
01 Scenarios
01 Subtechniques
50% Combined
Exfiltration
2 Techniques
17% Combined
Automated Exfiltration
03 Scenarios
17% Combined
Exfiltration Over Alternative Protocol
03 Scenarios
01 Subtechniques
17% Combined
Impact
0 Techniques
TAKE SCREENSHOT
Copyright © AttackIQ Inc. 2024

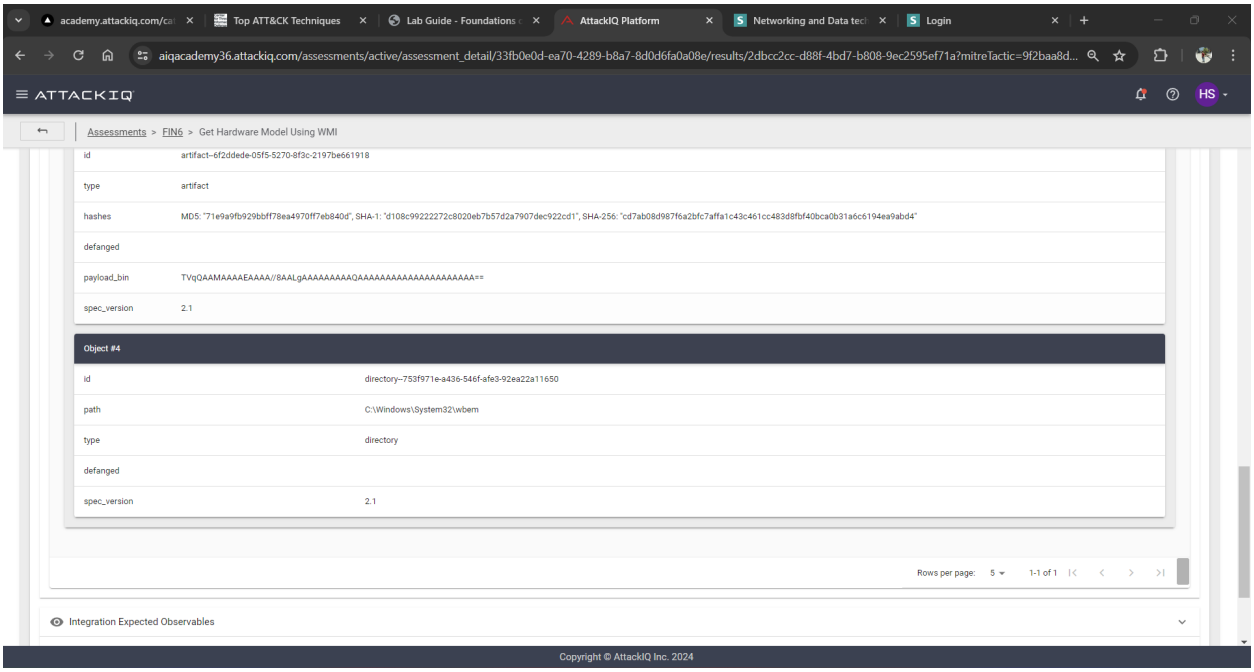

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=findings&sub_section=scenario_results
ATTACKIQ
HS
Assessments > FIN6 (Results)
Setup
On Demand
Scheduled
Results
Summary
History
MITRE ATT&CK
Mitigations
Reports
Team
Notifications
Showing 10 of 10 results
EXPORT CSV
MITRE tactic: Discovery
Assessment run: 04/24/2024 - 10:47 am
REFRESH
FILTER
Run ID
MITRE tactics
Test
Scenario
User Privileges
Asset
Prevention
Detection
Notes
04/24/2024 10:47 am
Execution
Discovery
Discovery
Permission Groups Discovery Script
SYSTEM
acad3141-un
Not Prevented
Not Configured
View (0)
acad5790-prot
CB EDR
Get OS Serial Number Using WMI
Get Hardware Model Using WMI
Get OS Type Using WMI
Discover SQL Servers using the Osql Utility
Prevented
Not Detected
Rows per page: 25
1-10 of 10
Copyright © AttackIQ Inc. 2024


academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e/results/2dbcc2cc-d88f-4bd7-b808-9ec2595ef71a?mitreTactic=9f2baa8d...
ATTACKIQ
HS
Assessments > FIN6 > Get Hardware Model Using WMI
Get Hardware Model Using WMI
Assessment: FIN6
04/24/2024 - 10:54 am
Not Prevented
Not Configured
Execution
Discovery
Inception
Blue Mockingbird
T1082
T1047
Sowbug
FIN6
+1
Showing result 5 of 32
Prevention
Detection
User Privileges
Hostname
Installed Technologies
IP Address
Operating System
Not Prevented
Not Configured
SYSTEM
acad3141-un
no technology detected
172.16.14.204
Microsoft Windows 10 Pro N
Phases
Name
Critical Phase
Prevention
Detection
Start Time
End Time
Execute WMI Command
Critical
Not Prevented
Not Configured
04/24/2024 10:53:51 am
04/24/2024 10:53:51 am
Detailed Findings:
Successfully executed WMI command "csproduct get Name /FORMAT:Textvaluelist"
Activity Details
Detection Details
Observable Details
Integration Expected Observables
Copyright © AttackIQ Inc. 2024

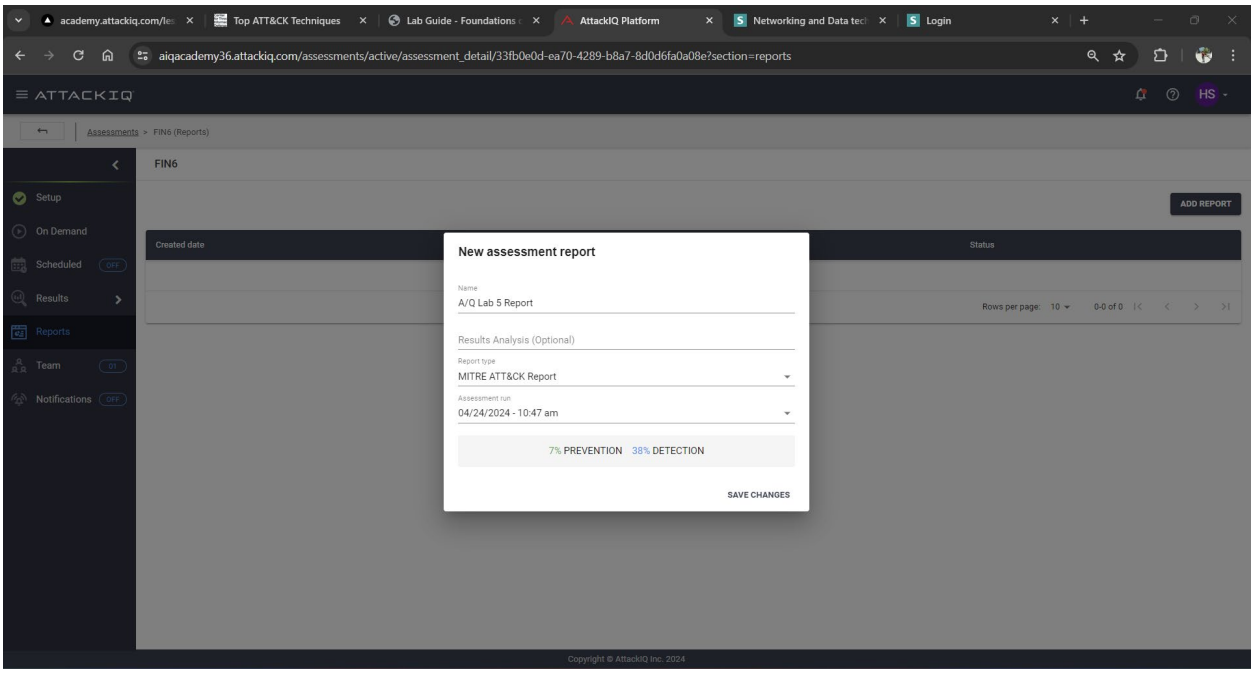

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e/results/2dbcc2cc-d88f-4bd7-b808-9ec2595ef71a?mitreTactic=9f2baa8d...
ATTACKIQ
HS
Assessments > FIN6 > Get Hardware Model Using WMI
Prevention
Detection
User Privileges
Hostname
Installed Technologies
IP Address
Operating System
Not Prevented
Not Configured
SYSTEM
acad3141-un
no technology detected
172.16.14.204
Microsoft Windows 10 Pro N
Phases
Name
Critical Phase
Prevention
Detection
Start Time
End Time
Execute WMI Command
Critical
Not Prevented
Not Configured
04/24/2024 10:53:51 am
04/24/2024 10:53:51 am
Detailed Findings:
Successfully executed WMI command "csproduct get Name /FORMAT:Textvaluelist"
Activity Details
Info
Warning
Error
Advanced
(04/24/2024 10:53:51 am) Executing WMI command: csproduct get Name /FORMAT:Textvaluelist
(04/24/2024 10:53:51 am) Exit code: 0, error code: 0, error message:
(04/24/2024 10:53:51 am) Command output:
Name=t3.medium
(04/24/2024 10:53:51 am) WMI command was successfully executed
Copyright © AttackIQ Inc. 2024

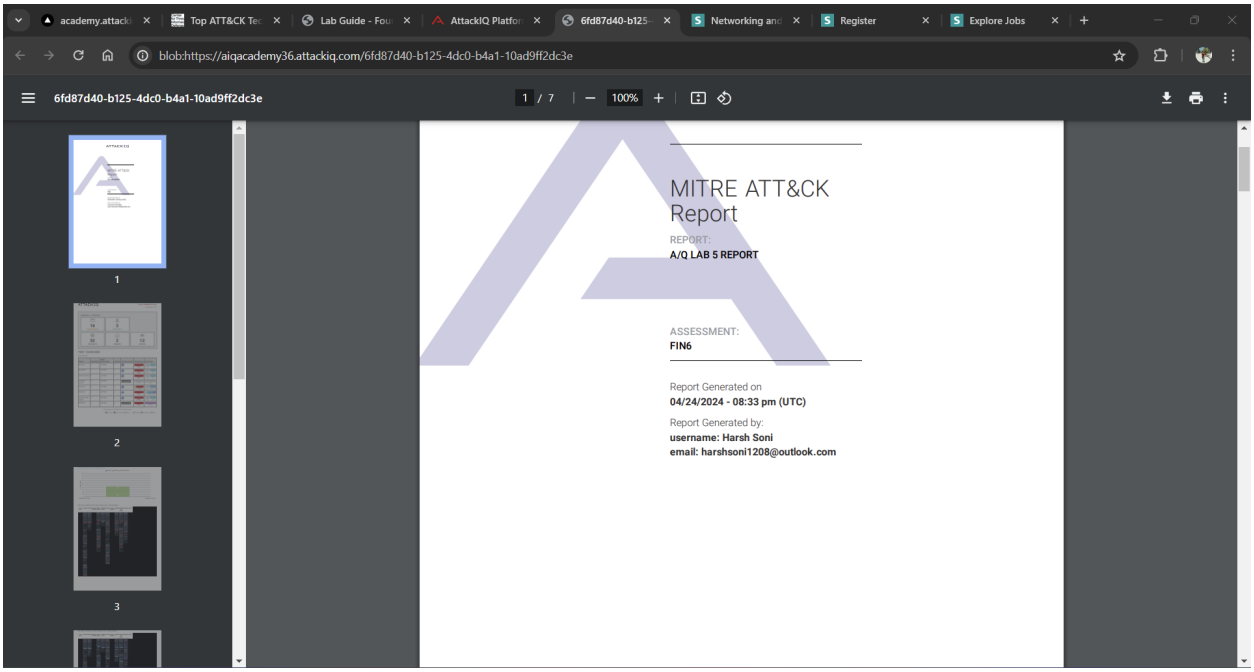

academy.attackiq.com/ca
Top ATT&CK Techniques
Lab Guide - Foundations
AttackIQ Platform
Networking and Data tec
Login
aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e/results/2dbcc2cc-d88f-4bd7-b808-9ec2595ef71a?mitreTactic=9f2baa8d...
ATTACKIQ
HS
Assessments > FIN6 > Get Hardware Model Using WMI
Detection Details
Observable Details
Binary Path
Command Line
Name
Format
C:\Windows\System32\wbem\wmic.exe
C:\Windows\System32\wbem\wmic.exe csproduct get Name /FORMAT:Textvaluelist
wmic.exe
STIX
Object #1
id
file--90998b96-91a6-564d-a290-2221ee46b20b
name
wmic.exe
type
file
hashes
MD5: "71e9a9fb929bbff78ea4970ff7eb840d", SHA-1: "d108c99222272c8020eb7b57d2a7907dec922cd1", SHA-256: "cd7ab08d987f6a2bfc7affa1c43c461cc483d8fbf40bca0b31a6c6194ea9abd4"
defanged
content_ref
artifact--9edd9ca7-f7ff-4063-bee2-289acd053e3a
spec_version
2.1
parent_directory_ref
directory--3ffe1182-faf2-49de-8dcc-0a4793acce91
Object #2
Copyright © AttackIQ Inc. 2024

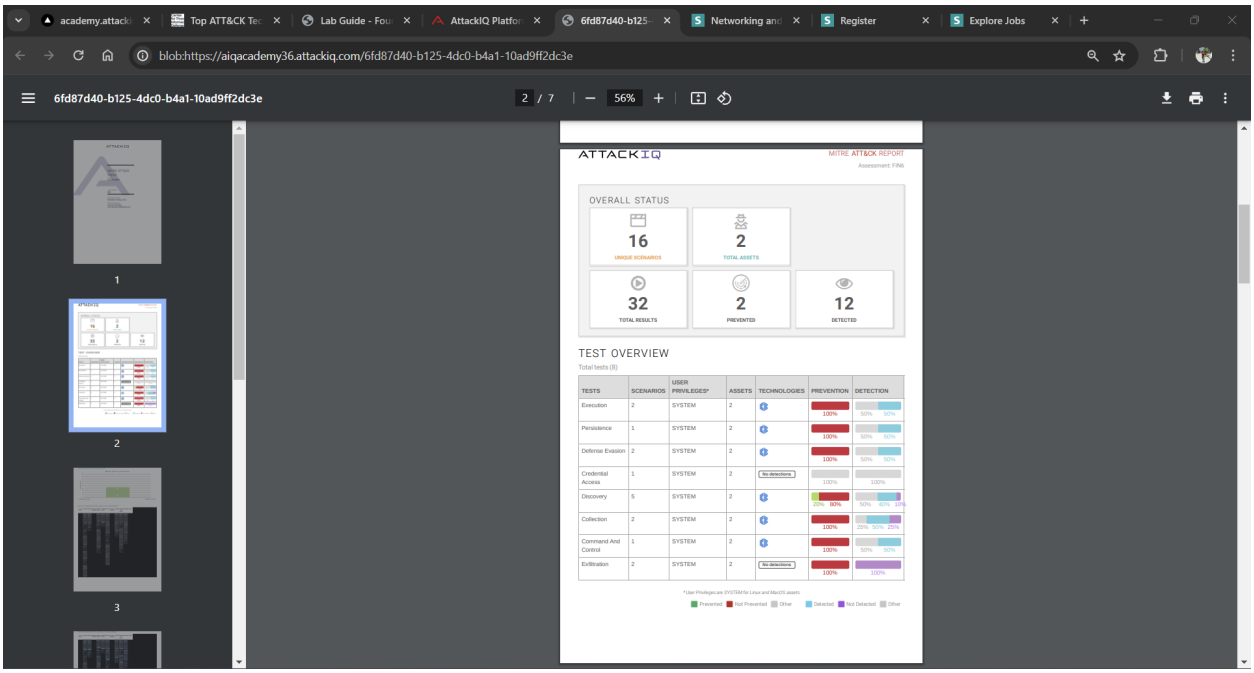


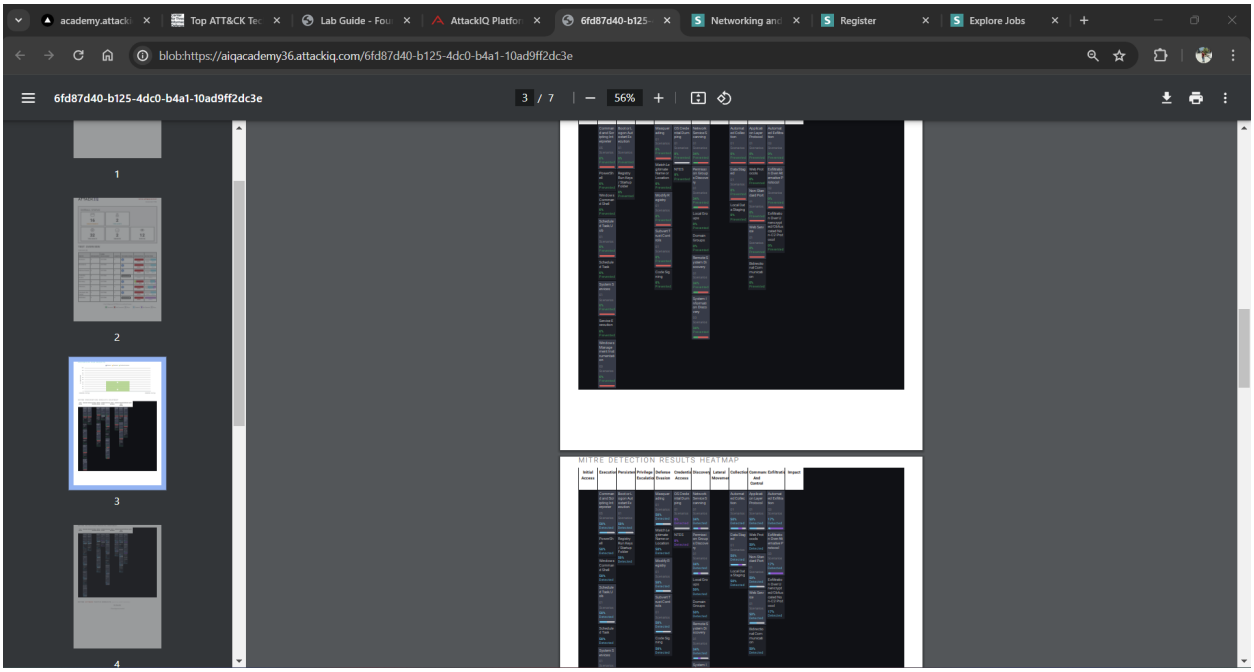


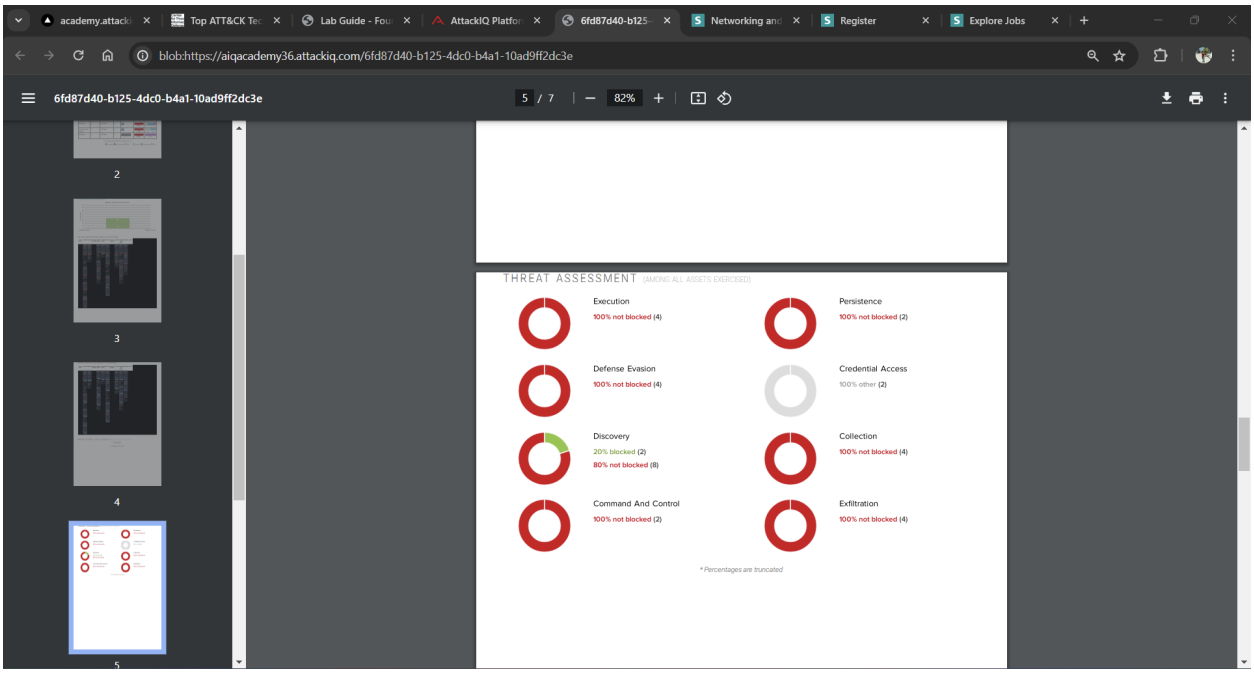
Exercise 5: Reporting 1. Click on FIN6 (Results) in the breadcrumb navigation at the top of the page. 2. Click on Reports in the left-hand menu. 3. Click the ADD Report button. 4. Give your report a name, select MITRE ATT&CK Report as the report type, and chose the assessment you ran in previous exercises. 18 5. Click SAVE CHANGES. 6. Click on the three vertical dots at the end of the row for the report you just created. 7. Click VIEW. 8. Review the report to get a better understanding of how the lab environment responded to different MITRE ATT&CK techniques.

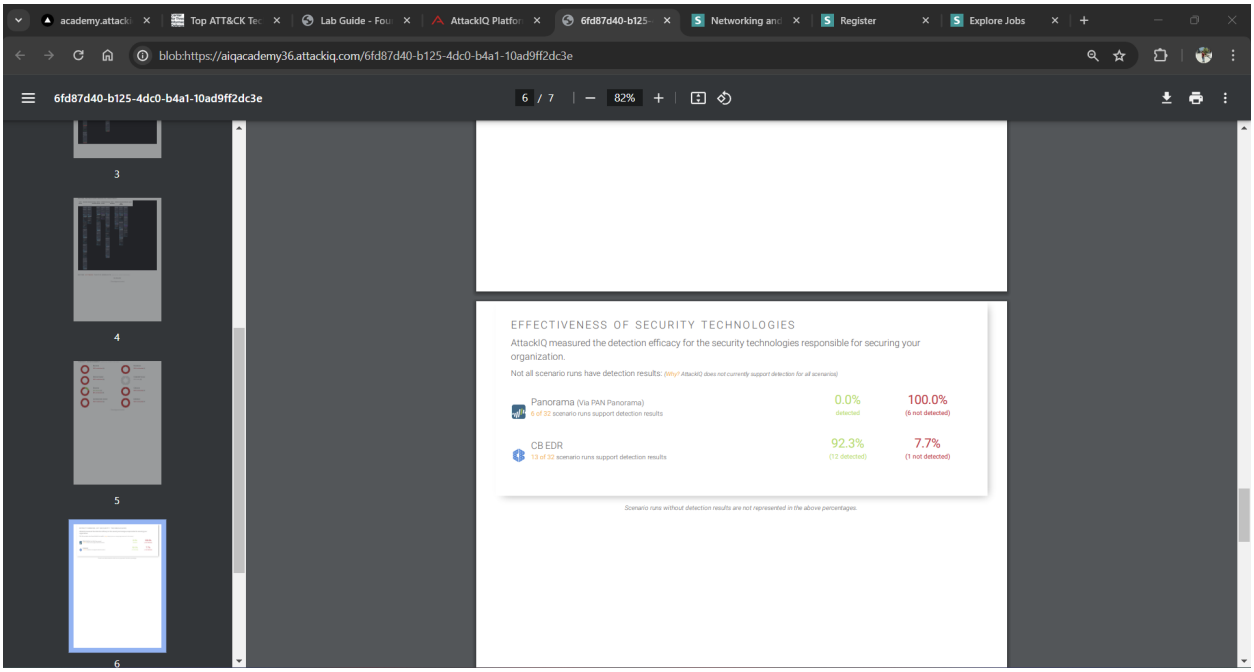

aiqacademy36.attackiq.com/assessments/active/assessment_detail/33fb0e0d-ea70-4289-b8a7-8d0d6fa0a08e?section=reports
ATTACKIQ
Assessments > FIN6 (Reports)
FIN6
Setup
On Demand
Scheduled
Results
Reports
Team
Notifications
ADD REPORT
Created date
Status
New assessment report
Name
A/Q Lab 5 Report
Results Analysis (Optional)
Report type
MITRE ATT&CK Report
Assessment run
04/24/2024 - 10:47 am
7% PREVENTION 38% DETECTION
SAVE CHANGES
Copyright © AttackIQ Inc. 2024


blob:https://aiqacademy36.attackiq.com/6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
1 / 7
100%
MITRE ATT&CK Report
REPORT:
A/Q LAB 5 REPORT
ASSESSMENT:
FIN6
Report Generated on
04/24/2024 - 08:33 pm (UTC)
Report Generated by:
username: Harsh Soni
email: harshsoni1208@outlook.com


academy.attack
Top ATT&CK Tec
Lab Guide - Fou
AttackIQ Platfor
6fd87d40-b125-
Networking and
Register
Explore Jobs
blob:https://aiqacademy36.attackiq.com/6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
2 / 7
56%
ATTACKIQ
MITRE ATT&CK REPORT
OVERALL STATUS
16
UNIQUE SCENARIOS
2
TOTAL ASSETS
32
TOTAL RESULTS
2
PREVENTED
12
DETECTED
TEST OVERVIEW
TESTS
SCENARIOS
USER PRIVILEGES*
ASSETS
TECHNOLOGIES
PREVENTION
DETECTION
Execution
Persistence
Defense Evasion
Credential Access
Discovery
Collection
Command And Control
Exfiltration
SYSTEM
No detections
Prevented
Not Prevented
Other
Detected
Not Detected


academy.attack
Top ATT&CK Tec
Lab Guide - Fou
AttackIQ Platfor
6fd87d40-b125-
Networking and
Register
Explore Jobs
blob:https://aiqacademy36.attackiq.com/6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
3 / 7
56%
MITRE DETECTION RESULTS HEATMAP
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command And Control
Exfiltration
Impact


academy.attack
Top ATT&CK Tec
Lab Guide - Fou
AttackIQ Platfor
6fd87d40-b125-
Networking and
Register
Explore Jobs
blob:https://aiqacademy36.attackiq.com/6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
5 / 7
82%
2
3
4
5
THREAT ASSESSMENT (AMONG ALL ASSETS EXERCISED)
Execution
100% not blocked (4)
Persistence
100% not blocked (2)
Defense Evasion
100% not blocked (4)
Credential Access
100% other (2)
Discovery
20% blocked (2)
80% not blocked (8)
Collection
100% not blocked (4)
Command And Control
100% not blocked (2)
Exfiltration
100% not blocked (4)
* Percentages are truncated


academy.attack
Top ATT&CK Tec
Lab Guide - Fou
AttackIQ Platfor
6fd87d40-b125-
Networking and
Register
Explore Jobs
blob:https://aiqacademy36.attackiq.com/6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
6fd87d40-b125-4dc0-b4a1-10ad9ff2dc3e
6 / 7
82%
3
4
5
6
EFFECTIVENESS OF SECURITY TECHNOLOGIES
AttackIQ measured the detection efficacy for the security technologies responsible for securing your organization.
Not all scenario runs have detection results: (Why? AttackIQ does not currently support detection for all scenarios)
Panorama (Via PAN Panorama)
6 of 32 scenario runs support detection results
0.0%
detected
100.0%
(6 not detected)
CB EDR
13 of 32 scenario runs support detection results
92.3%
(12 detected)
7.7%
(1 not detected)
Scenario runs without detection results are not represented in the above percentages.