

Lab 3

Accounting and Audit

Question 1: As shown in the screenshot below, the source IP of the attacker is 195.21.15.9. You can tell they failed to log in because the description message states “A user attempted to logon however the username or password was invalid”.

The screenshot shows a security log interface with three entries for failed logon attempts on Jan 20, 2017, at 11:15:59.677, 11:15:55.451, and 11:15:54.103. Each entry includes the user, log name, security source, computer, date, time, source IP (195.24.15.9), and a detailed description stating that the user attempted to logon but the username or password was invalid. The logon event ID for each attempt is 4614.

Question 1 of 7

What is the source IP address of the failed login attempts?

Correct

Question 2 of 7

What is the computer name the attacker is attempting to access?

Correct

Question 2: As from the q1 screenshot above, the attacker is attempting to access SERVER5.

Question 3: As shown from the screenshots below, the attacker tried 9 usernames: dataadmin, defaultadmin, enterpriseadmin, localadmin, root, manager, domainadmin, administrator, and admin.

The screenshot shows a security log interface with nine entries for failed logon attempts on Jan 20, 2017, at various times between 11:15:59.677 and 11:15:54.103. Each entry includes the user, log name, security source, computer, date, time, source IP (195.24.15.9), and a detailed description stating that the user attempted to logon but the username or password was invalid. The logon event ID for each attempt is 4614.

Question 3 of 7

How many different usernames did the attacker try?

Correct

Question 4 of 7

Did the attacker successfully log in?

Yes

> Jan 20, 2017 @ 11:15:38.491	User: localadmin Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:38.491 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:15:38.491 Task Category: Attempted Logon Event ID: 4614 _id: neW5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:15:34.349	User: alice01 Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:34.349 Source IP: 14.124.115.31 Description: A user successfully logged on. @timestamp: Jan 20, 2017 @ 11:15:34.349 Task Category: Successful Logon Event ID: 4610 _id: n0W5JXQBo61UnPLeIw7 _type: _doc _index: accaud _score: -
> Jan 20, 2017 @ 11:15:28.293	User: root Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:28.293 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:15:28.293 Task Category: Attempted Logon Event ID: 4614 _id: m-W5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:15:11.123	User: manager Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:11.123 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:15:11.123 Task Category: Attempted Logon Event ID: 4614 _id: muW5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:15:02.010	User: domainadmin Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:02.010 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:15:02.010 Task Category: Attempted Logon Event ID: 4614 _id: meW5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:14:57.031	User: administrator Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:14:57.031 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:14:57.031 Task Category: Attempted Logon Event ID: 4614 _id: l-W5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:14:54.878	User: admin Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:14:54.878 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:14:54.878 Task Category: Attempted Logon Event ID: 4614 _id: 1-W5JXQBo61UnPLeIw7 _type: _doc _index: accaud

Question 4: From the attempts above, all prompted a “A user attempted to logon however the username or password was invalid” message because they did not match the username(s) with access, such as admin_domain, alice01, or \$admin_domain, etc.

> Jan 20, 2017 @ 11:14:54.878	User: admin Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:14:54.878 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:14:54.878 Task Category: Attempted Logon Event ID: 4614 _id: 1-W5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:14:54.456	User: \$admin_domain Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:14:54.456 Source IP: 14.124.115.31 Description: Security Updates installed successfully. @timestamp: Jan 20, 2017 @ 11:14:54.456 Task Category: Security Updates Event ID: 2351 _id: luW5JXQBo61UnPLeIw7 _type: _doc _index: accaud

Question 5: As shown in the screenshot below, between the attacks from q3, user alice01 successfully logged on.

> Jan 20, 2017 @ 11:15:38.491	User: localadmin Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:38.491 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:15:38.491 Task Category: Attempted Logon Event ID: 4614 _id: neW5JXQBo61UnPLeIw7 _type: _doc _index: accaud
> Jan 20, 2017 @ 11:15:34.349	User: alice01 Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:34.349 Source IP: 14.124.115.31 Description: A user successfully logged on. @timestamp: Jan 20, 2017 @ 11:15:34.349 Task Category: Successful Logon Event ID: 4610 _id: n0W5JXQBo61UnPLeIw7 _type: _doc _index: accaud _score: -
> Jan 20, 2017 @ 11:15:28.293	User: root Log Name: Security Source: Computer Event Log Computer: SERVER5 Date: Jan 20, 2017 @ 11:15:28.293 Source IP: 195.24.15.9 Description: A user attempted to logon however the username or password was invalid. @timestamp: Jan 20, 2017 @ 11:15:28.293 Task Category: Attempted Logon Event ID: 4614 _id: m-W5JXQBo61UnPLeIw7 _type: _doc _index: accaud

Question 6: As shown in the screenshot below, admin_domain is the administrative account, they can change passwords, such as shown below.

Question 3 of 7

How many different usernames did the attacker try?

Correct

Question 4 of 7

Did the attacker successfully log in?

Question 3 of 7

How many different usernames did the attacker try?

Correct

Question 4 of 7

Did the attacker successfully log in?

Question 3 of 7

How many different usernames did the attacker try?

Question 4 of 7

Did the attacker successfully log in?

Correct

Question 5 of 7

Which standard user logged in during the attack?

Correct

Question 6 of 7

What is the username of the legitimate administrative user account?

Event ID: 2351 _id: puW5JXQBo61uNPeI1W/_type: _doc _index: accaud

```
> Jan 20, 2017 @ 11:16:47.437 User: admin_domain Log Name: Security Source: Computer Event Log
Computer: SERVER5 Date: Jan 20, 2017 @ 11:16:47.437 Source IP: 14.124.115.31 Description: Password reset successfully for alice01.
@timestamp: Jan 20, 2017 @ 11:16:47.437 Task Category: Password Reset for standard user Event ID: 4268 _id: o-W5JXQBo61uNPeI1W7 _type: _doc

> Jan 20, 2017 @ 11:16:32.001 User: admin_domain Log Name: Security Source: Computer Event Log
Computer: SERVER5 Date: Jan 20, 2017 @ 11:16:32.001 Source IP: 14.124.115.31 Description: Password changed successfully. @timestamp: Jan 20, 2017 @ 11:16:32.001 Task Category: Password Change Event ID: 4627 _id: ouW5JXQBo61uNPeI1W7 _type: _doc _index: accaud _score: -

> Jan 20, 2017 @ 11:16:11.329 User: admin_domain Log Name: Security Source: Computer Event Log
Computer: SERVER5 Date: Jan 20, 2017 @ 11:16:11.329 Source IP: 14.124.115.31 Description: A user successfully logged on. @timestamp: Jan 20, 2017 @ 11:16:11.329 Task Category: Successful Logon Event ID: 4610 _id: oeW5JXQBo61uNPeI1W7 _type: _doc _index: accaud _score: -

> Jan 20, 2017 @ 11:15:59.677 User: dataadmin Log Name: Security Source: Computer Event Log
```

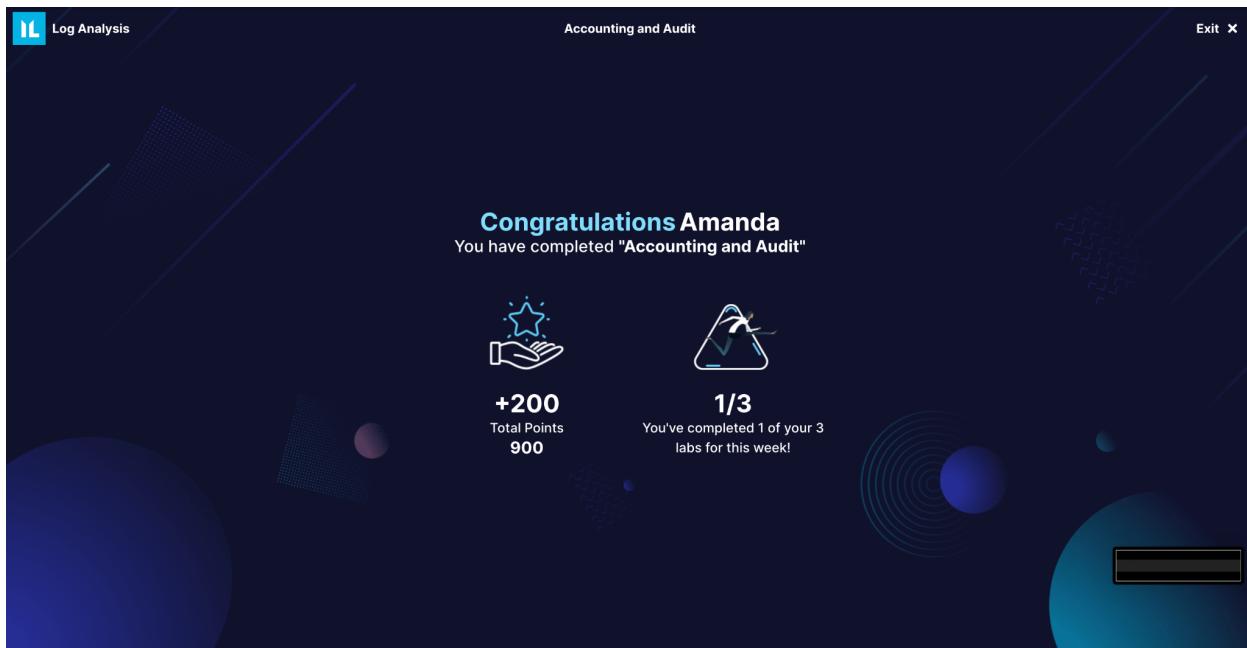
Question 7: As shown in screenshot below, the description states “Password reset successfully for alice01” from the user admin_domain, at 11:16:47.437.

Event ID: 2351 _id: puW5JXQBo61uNPeI1W/_type: _doc _index: accaud

```
> Jan 20, 2017 @ 11:16:47.437 User: admin_domain Log Name: Security Source: Computer Event Log
Computer: SERVER5 Date: Jan 20, 2017 @ 11:16:47.437 Source IP: 14.124.115.31 Description: Password reset successfully for alice01.
@timestamp: Jan 20, 2017 @ 11:16:47.437 Task Category: Password Reset for standard user Event ID: 4268 _id: o-W5JXQBo61uNPeI1W7 _type: _doc

> Jan 20, 2017 @ 11:16:32.001 User: admin_domain Log Name: Security Source: Computer Event Log
Computer: SERVER5 Date: Jan 20, 2017 @ 11:16:32.001 Source IP: 14.124.115.31 Description: Password changed successfully. @timestamp: Jan 20, 2017 @ 11:16:32.001 Task Category: Password Change Event ID: 4627 _id: ouW5JXQBo61uNPeI1W7 _type: _doc _index: accaud _score: -
```

Results:



Snort Rules Ep.1

Question 1: As shown in screenshot below, the snort rule used to alert on traffic to port 443 was `alert tcp any any -> any 443 (msg: "Testing Alert"; sid: 1000001)` this means that we are accepting from all sources and ports to all destinations that are on port 443. We get the token `d68b28` as a result.

Snort Rule

```
alert tcp any any -> any 443 (msg: "Testing Alert"; sid:1000001)
```

Question Number

1

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: `d68b28`

This table shows `152` packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-07T11:19:52.694783	172.16.169.132:49451	2.21.189.133:443	TCP	Testing Alert

Question 1 of 5

Create a Snort rule that will alert on traffic using TCP with a destination port of 443. Validate the rule in the PCAP scanner and enter the token.

```
d68b28
```

Correct

Question 2 of 5

What is the name of the content modifier that can be used to alert on HTTP Status Codes?

Question 3 of 5

Question 2: As shown in the screenshots below, the modifier `http_stat_code` is used to alert on http.

`http_stat_code`

This modifier restricts the search to the extracted Status Code field from an HTTP server response.

Question 2 of 5

What is the name of the content modifier that can be used to alert on HTTP Status Codes?

```
http_stat_code
```

Correct

Question 3: As shown in the screenshot below, the snort rule, `alert tcp any any -> any [443,447]` (`msg: "Testing Alert"; sid: 1000001`) alerts traffic from any sources to any destinations on port 443 or 447 only. The resulting token is 403bb9.

Snort Rule

```
alert tcp any any -> any [443,447] (msg: "Testing Alert" ; sid:1000001)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: **403bb9**

This table shows **622** packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-	172.16.169.132:49451	2.21.189.133:443	TCP	Testing

Question 3 of 5

What is the token generated when you create a Snort rule that will detect outbound traffic using TCP to ports 443 and 447?

403bb9

Correct

Question 4 of 5

What is the token generated when you create a Snort rule that will detect all ICMP traffic?

Question 4: As shown below, to detect all ICMP traffic, the snort rule, `alert icmp any any -> any any` (`msg: "Testing Alert"; sid: 1000001`). All ICMP packets from all sources to all destinations are alerted. The result token is 8e14ef.

Snort Rule

```
alert icmp any any -> any any (msg: "Testing Alert" ; sid:1000001)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: **8e14ef**

This table shows **2** packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-	172.16.169.132	172.16.169.2	ICMP	Testing

Correct

Question 4 of 5

What is the token generated when you create a Snort rule that will detect all ICMP traffic?

8e14ef

Correct

Question 5 of 5

Modify this rule, so that it only alerts if the content matches in the first three bytes: `'alert tcp any any -> any any (msg:"Immersive Labs Question 5"; content:"[37 e1 a4]"; sid:1000001;)'`, then enter the token that is generated.

Question 5: As shown below, I modified the original message, `alert tcp any any -> any any (msg: "Immersive Labs Question 5"; content: "[37 e1 a4]"; sid: 1000001;)` to include a depth of 3 to specify matches in the first 3 bytes only as: `alert tcp any any -> any any (msg: "Immersive Labs Question 5"; content: "[37 e1 a4]"; depth: 3; sid: 1000001;)`. The generated token was 31e9ba.

Snort Rule

```
alert tcp any any -> any any (msg: "Immersive Labs Question 5"; content:"|37 e1 a4|"; depth:3; sid:1000001;)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: **31e9ba**

This table shows 1 packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-	202.169.44.149:80	172.16.169.132:49448	TCP	Immersive

Question 4 of 5

What is the token generated when you create a Snort rule that will detect all ICMP traffic?

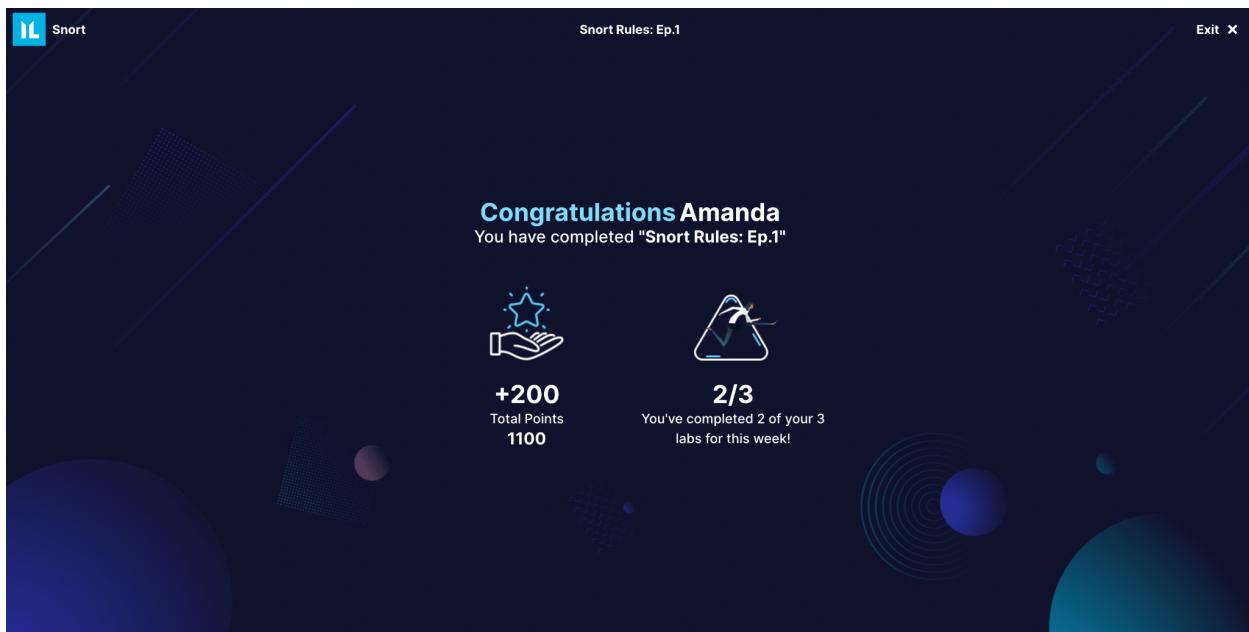
Correct

Question 5 of 5

Modify this rule, so that it only alerts if the content matches in the first three bytes: 'alert tcp any any -> any any (msg:"Immersive Labs Question 5"; content:"|37 e1 a4|"; sid:1000001;)', then enter the token that is generated.

Correct

Result:



Snort Rules Ep.2 DNS

Question 1: As shown in the screenshot, the snort rule, `alert udp any any <> any 53`, captures bidirectional traffic on port 53 for udp which is DNS traffic. The resulting token is 8eb202.

Snort Rule

```
alert udp any any <> any 53 (msg: "Testing Alert" ; sid:1000001)
```

Question Number

1

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: [8eb202](#)

This table shows 56 packets that matched your current rule

Question 1 of 4

Create a Snort rule to detect all DNS Traffic, then test the rule with the scanner and submit the token.

```
8eb202
```

Correct

Question 2 of 4

Question 2: As shown below, the snort rule, `alert udp any any -> any 53 (msg: "Testing Alert"; content: "|69 63 61 6E 68 61 7A 69 70|"; sid: 1000001)`, captures udp traffic from any source to port 53 (dns) to the domain 'icanhazip', which matches the content's hex value '69 63 61 6E 68 61 7A 69 70'. The resulting token is da4c73.

Snort Rule

```
alert udp any any -> any 53 (msg: "Testing Alert" ; content: "|69 63 61 6E 68 61 7A 69 70|"; sid:1000001)
```

Question Number

2

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: [da4c73](#)

This table shows 1 packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-07T11:20:23.068188	172.16.169.132:61348	172.16.169.2:53	UDP	Testing Alert

Question 2 of 4

Create a rule to detect DNS requests to 'icanhazip', then test the rule with the scanner and submit the token.

```
da4c73
```

Correct

Question 3 of 4

Create a rule to detect DNS requests to 'interbanx', then test the rule with the scanner and submit the token.

Question 3: As shown below, the snort rule, `alert udp any any -> any 53 (msg: "Testing Alert"; content: "|69 6E 74 65 72 62 61 6E 78|"; sid: 1000001)`, captures udp traffic from any source to port 53 (dns) to the domain 'icanhazip', which matches the content's hex value '69 6E 74 65 72 62 61 6E 78'. The resulting token is 97497f.

Snort Rule

```
alert udp any any -> any 53 (msg: "Testing Alert" ; content: "|69 6E 74 65 72 62 61 6E 78|"; sid:1000001)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: [97497f](#)

This table shows 1 packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-07T11:19:02.626785	172.16.169.132:53804	172.16.169.2:53	UDP	Testing Alert

Question 4: As shown below, the exceptions to DNS using UDP are when the response is bigger than 512 bytes, zone transfers, or DNS settings set by the operator. These circumstances will use TCP port 53 instead.

There are a few exceptions when the DNS will instead use TCP port 53:

- If the response is greater than 512 bytes
- Tasks like zone transfers
- Explicitly set by the DNS operator

Question 4 of 4

Which of the following would cause DNS to use TCP instead of UDP?

- If the response is greater than 512 bytes
- Tasks like zone transfers
- Explicitly set by the DNS operator
- All of them

Correct

Result:

Question 3 of 4

Create a rule to detect DNS requests to 'interbanx', then test the rule with the scanner and submit the token.

Correct

Question 4 of 4

Which of the following would cause DNS to use TCP instead of UDP?

- If the response is greater than 512 bytes
- Tasks like zone transfers



Next Lab
Snort Rules: Ep.3 – HTTP >

Snort Rules Ep.3 HTTP

Question 1: As shown in the screenshot below, the snort rule, `alert tcp any any -> any any (msg: "Testing Alert"; content: "msn.com"; http_cookie; sid: 1000001)`, looks for the content 'msn.com' in the cookie value from all tcp traffic. The resulting token is 35094e.

Snort Rule

```
alert tcp any any -> any any (msg: "Testing Alert" ; content:"msn.com"; http_cookie;  
sid:1000001)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: 35094e

This table shows 1 packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-07T11:19:52.311866	204.79.197.203:80	172.16.169.132:49449	TCP	Testing Alert

Question 2: As shown below, to look for content 'GET' and 'gif' in the url, i used the snort rule, `alert tcp any any -> any any (msg: "Testing Alert"; content: "GET"; content: "gif"; http_uri; sid: 1000001)`. The resulting token was 945a38.

Snort Rule

```
alert tcp any any -> any any (msg: "Testing Alert" ; content: "GET"; content: "gif"; http_uri;  
sid:1000001)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: 945a38

This table shows 2 packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-07T11:19:52.843478	172.16.169.132:49454	104.40.210.32:80	TCP	Testing Alert

Question 3: As shown below, the snort rule, `alert tcp any any -> any any (msg: "Testing Alert"; file_data; content: "MZ"; depth: 2; sid: 1000001)`, specifies the content of 'MZ' in file_data, which must be before the content. The depth of 2 is for the first two characters only. The resulting token is 7f5cbc.

Question 1 of 4

Create a Snort rule that looks for 'msn.com' in an HTTP cookie value. Test the rule and enter the token.

Correct

Question 2 of 4

Create a Snort rule that looks for an HTTP method 'GET' and contains 'gif' in the URL. Test the rule and enter the token.

Question 2 of 4

Create a Snort rule that looks for an HTTP method 'GET' and contains 'gif' in the URL. Test the rule and enter the token.

Correct

Question 3 of 4

Create a rule that will alert when 'MZ' are first two characters in the HTTP body. Test the rule and enter the token.

Snort Rule

```
alert tcp any any -> any any (msg: "Testing Alert"; file_data; content: "MZ"; depth: 2; sid:1000001)
```

Question Number

Scan

The scan results for your snort rule will be displayed below.

You created a valid rule that produced no false positives in our dataset. Your token is: **7f5cbc**

This table shows **1** packets that matched your current rule

TimeStamp	Source	Destination	Protocol	Message
2018-04-07T11:19:03.727229	202.169.44.149:80	172.16.169.132:49448	TCP	Testing Alert

Question 3 of 4

Create a rule that will alert when 'MZ' are first two characters in the HTTP body. Test the rule and enter the token.

Correct

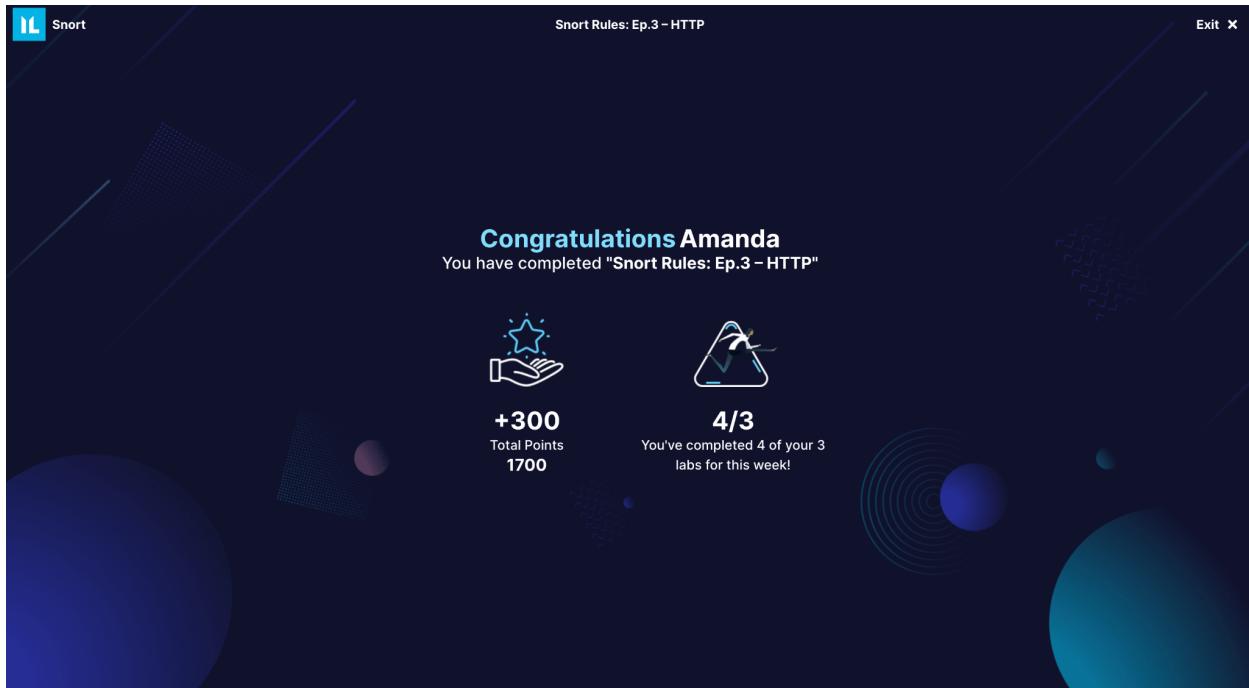
Question 4 of 4

If you wanted a rule to match on a URI string that has been URI decoded, which modifier would you use?

Correct

Question 4: As shown in the screenshot above from q3, the modifier http_uri is used to match a decoded URI to a URI string, as opposed to http_raw_uri.

Result:



Write-Up

The first part of the lab was auditing data from log files; we did this with Kibana, which allowed us to see features like connections and access attempts. In this, we were able to see attempts from an attacker to log in using incorrect credentials. The UI allowed us to see messages alerting us of the invalid username logon, and the details associated with the person doing so, such as their IP, and which computer they were targeting. Further, we saw examples of a valid user log on and valid administrator that had the privilege to change passwords. This tool could be extremely useful to monitor networks and firewalls to prevent unauthorized access.

The latter part of the lab focused on snort rules to create rules for specific packet information. Alerts can be generated for specific packets on protocols like tcp, udp, and icmp, which we focused on. Some specific information we alerted on was content on specific ports. For http, snort rules had more modifiers and components to hone in on uri, cookie, or body information. This tool can be used to build very specific protections against known attacker techniques.