Part 1: Windows Server Attack

Question 1

What mitigations would you recommend to protect each user account?

Install a firewall on the login server.

Require users to submit their home/office IP address and configure firewall to permit access to the login from those IP addresses.

How would you protect the whole company from a "bad login" attack?

Configure and deploy VPN access for employees and put the login server inside the firewall.

Question 2

What sort of mitigation would you use to protect against “bad logins” lock out?

Monitor for multiple login attempts from a single IP address and create a firewall rule which denies access when the count exceeds 5 in an hour.

Question 3

How would you learn more about windows security logs? What is going on with all the create/delete/modify of users?

The website ultimatewindowssecurity.com has a free online book called "The Windows Security Log Revealed" that looks quite thourough.

Question 4

How are EventCode, signature and signature\_id related? Why can a given signature contain more than one EventCode when they appear to contridict each other. Does the fact that messages in the first burst of activity don't contain EventCodes indicate a logging falure as a result of the high rate of requests? Does the re-appearance of the EventCodes field after a short period of time indicate a load-balancer picking up the slack?

Part 2: Apache Webserver Attack

Question 1

What geographic firewall rule would you recommend to mitigate this attack? (english and screen shot)

Block all incomming HTTP traffic to the VSI\_Account\_logon page where the source IP traffic does not come from one of the cities where we have offices.



during the attack



Question 2

What other rules (2) can you create to protect from this kind of attack which is not based on static IP addresses?

monitor clientip access rate to login page

blacklist clientip based on rate of

404 errors (5/hr)  
 login page visits (4/hr)

Question 3

How would you learn more about how to track website login attempts and if the answer varies depending the on the authentication method used by the server, the configuration of the webapp, the use of https or something else?

Apache uses .htaccess and .htpasswd files to configure and manage authentication. Why the POSTS to the website do not show which user is attempting to login is not clear to me.

If your authentication is managed by a framework other than Apache, say Google OAUTH in a react app, I suspect your app framework would be responsible for logging that. Then the question becomes, write to disk or ship directly to the SIEM.