ENPM685 – Security Tools for Information Security

Section: 0101

Homework – 6

Name: Syed Mohammad Ibrahim

UID: *iamibi*

UID Number: 118428369

Email – *iamibi@umd.edu*

SNORT Rules

To detect Union based SQL injection:

alert tcp any any -> any any (msg: "SQL Injection attempt using UNION"; content: "union"; nocase; sid:10412345;)

To detect sqlmap usage:

alert tcp any any -> any any (msg: "sqlmap usage detected"; content: "sqlmap"; nocase; sid:10412346;)

Recommendations

The existing rule should be updated with the following new rules to detect a generic SQL injection attack:

alert tcp any any -> any any (msg: " SQL injection discovered!"; content: "%27"; sid: 100002;)

alert tcp any any -> any any (msg: " SQL injection discovered!"; content: "%22"; sid: 100003;)

The above rules make sure that if an additional single quote (‘) or double quote (“) is passed as part of the URL, it will raise an alert. The quotes are usually encoded when being passed as part of the URL, thus, their encoded versions %27 and %22 respectively are added as part of the rule to detect them. A corner case, where a legitimate query parameter may contain a quote can raise a false positive. However, those can probably be filtered out from the logs.