SQL Filtering Operators

Operator	Description	Example Query	Example Query Description
=	Equal to 'string' or number	SELECT uid FROM user_groups WHERE gid = 80;	Show me the user id field from the user groups table where the group id is 80 (admin group on MacOS)
<>	Not equal	SELECT username,shell FROM users WHERE shell <> '/usr/bin/false';	Show me the username and shell fields from the users table where the shell /usr/bin/false was not used.
<	Less Than	SELECT username,uid FROM users WHERE uid < 500;	Show me the username and uid fields from the users table where the user id is less than 500.
<=	Less Than or Equal		
>	Greater Than	SELECT username,uid FROM users WHERE uid >= 500;	Show me the username and uid fields from the users table where the user id equal to or greater than 500.
>=	Greater Than or Equal		
BETWEEN	Between an inclusive range	SELECT username FROM users WHERE uid BETWEEN 100 AND 500;	Show me the username and uid fields from the users table where the user id is between 100 – 500, including 100 & 500.
LIKE	Pattern search with wildcards		
%	Zero, one, or multiple characters	SELECT username, uid FROM users WHERE username LIKE '%admin%';	Show me the username and uid fields from the users table where the username contains the string 'admin'.
_	One character	SELECT username, uid FROM users WHERE username LIKE '_uest';	Show me the username and uid fields from the users table where the username is 5 characters long and ends with 'uest'.

Filtering out unneeded / known-good data is a key component to security operations – this handout guides you through the use of the most common SQL filtering operators that you can use with osquery.

Feedback? Josh@DefensiveDepth.com

LearnOsquery.com

NetworkDefense.io