E-Security

Cheat Sheet

Windows Commands 1

By Ehsan Nikavar

http://esecurity.ir

هدف

آشنایی با دستورات کاربردی در محیط CMD سیستم عامل ویندوز

این Cheat Sheet برای دوره های **PWK**، **CEH**، **ECSA** و **SEC 504** طراحی شده است.

ابزارها

در این بخش با موارد زیر آشنا می شوید:

آشنایی با دستورات

WMIC

WMIC

WMIC مخفف Windows Management Instrumentation Command می باشد و برای جمع آوری اطلاعات و تجزیه وتحلیل سیستم می توان از آن استفاده نمود.

شما می توانید از دستورات alias برای wmic استفاده کنید که برای کسب اطلاعات از سیستم عامل مورد استفاده قرار می گیرند و همچنین قابلیت شرط گذاری و مدیریت خروجی را هم شامل می شوند.

wmic [alias] [where clauses] [verb clauses]

alias های کاربردی که می توان از آن ها استفاده نمود:

Process، Share، Service، Useraccount، Startup، Nicconfig، Bios، OS، qfe و .....

دستور برای استخراج اطلاعات سیستم عامل

wmic os get > os.txt

دستور فوق تمامی فیلد های اطلاعاتی مربوط به OS را برای شما استخراج می کند. برای مشاهده فیلدهای اطلاعاتی برای دستور OS از دستور زیر استفاده نمایید

wmic os get /?

ساختار بالا برای کلیه alias ها جهت مشاهده جزئیات آن ها، قابل دسترس می باشد. به عنوان مثال دیگر:

wmic statup get /?

دستور فوق جزئیات فیلدهای مربوط به Startup را به شما نمایش می دهد.

WMIC

نکته: شما با قرار دادن عبارت "/?" می توانید به دستورات محیطی بخش مورد نظر دسترسی داشته باشید.

علاوه بر عبارت get که برای استخراج اطلاعات از آن استفاده می شود عبارات دیگری مانند Call، Create، Delete، List و ... نیز وجود دارد که می توان از آن ها نیز استفاده نمود. به عنوان مثال برای call جهت فراخوانی مورد استفاده قرار می گیرد.

WMIC PROCESS CALL Create "calc.exe"

در مثال فوق برنامه calc فراخوانی می شود.

برای استفاده از شرط ها می توان از where استفاده کرد.

WMIC PROCESS WHERE Name="calc.exe" CALL Terminate

دستور فوق، اگر برنامه calc فراخوانی شده باشد، آن را اصطلاحا Terminate یا حذف می کند.
نکته: شما می توانید در صورت ذخیره خروجی در یک فایل مانند text، فیلدهای خروجی را سفارشی نموده و موارد خاصی از آن را استخراج کنید:

wmic process get caption,executablepath > proc.txt

دستور فوق، فقط دو فیلد از کلیه فیلد های مربوط به process را در فایل proc.txt ذخیره می کند. در ادامه نمونه دیگری از این دستور را مشاهده می فرمایید:

wmic useraccount get caption,domain,name > b.txt