پویش آسیب پذیری: پس از پیدا شدن آسیب پذیری های سیستم هدف، با انتخاب یک حمله متناسب با آسیب پذیری ها می توان به سیستم نفوذ کرد.

** یکی از ابزار های پرکاربرد و قوی در این زمینه ابزار Acunetix است که روی پویش آسیب پذیری تارنما ها متمرکز است.
**علاوه بر ابزار Acunetix می توانید از ابزار های متنوعی مانند : Nagios، Nessus،Retina نیز استفاده کنید .

فاز ۳: ایجاد و حفظ دسترسی (حمله)

پس از اینکه هکر از طریق ابزار های پویش، نقاط آسیب پذیر یک سیستم را تشخیص داد، حمله واقعی خود را آغاز می کند. پس از دسترسی به سیستم هدف، باید برای اجرای حملات بعدی، دسترسی خود را حفظ کرد.برای این کار از Backdoor ها استفاده میشود .

** برای جلوگیری از این حمله باید از ابزار های امنیتی کامل و جامع استفاده کرد و از نصب برنامه های ناشناخته جلوگیری کرد.

حملات DoS و DDoS

در حملات DoS هدف هکر ایجاد اختلال و یا قطع سرویس دهی سرور به کاربران است. هکر می تواند شروع به ارسال ترافیک با حجم بالا به سمت سرور کند و به قدری سرور را درگیر جواب دادن به این ترافیک کند که سرور توان پاسخ دادن به کاربران مجاز را نداشته باشد!

DDoS : در این حالت هکر به جای ارسال ترافیک تنها از یک سیستم، از چندین و شاید چندین هزار سیستم شروع به ارسال هم زمان ترافیک می کند. در این حالت اصطلاحا سرور Crash میکند و از سرویس خارج میشود .

** ابزار LOIC یکی از ابزار های حمله DoS است .

در برنامه LOIC در کجا نوع و پارامترهای حمله را تعیین میکنیم ؟ در کادر Attack Options

وظیفه کادر Threads چیست ؟ تعداد جریان های ارتباطی با هدف را مشخص میکند . هرچه این عدد بزرگ تر باشد، سیستم هدف بیشتر درگیر خواهد شد و زودتر از پا در می آید.

برای مشاهده ترافیک ورودی بعد از شروع حمله از چه ابزاری استفاده میکنید ؟ Wireshark

فاز ٤: پاک کردن ردپا ها

یکی از معمول ترین روش ها، پاک کردن پرونده های Log در سرویس Event Viewer ویندوز است.