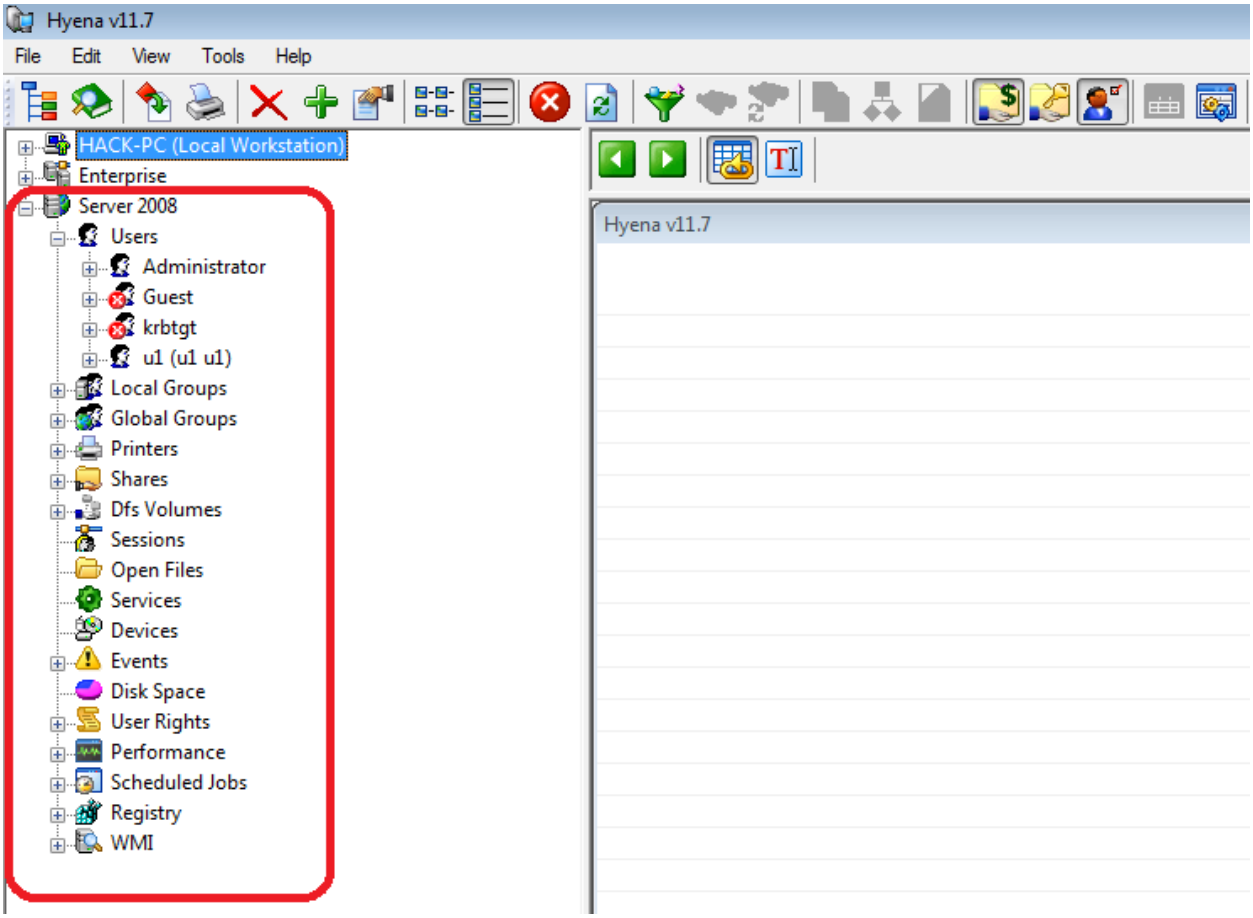
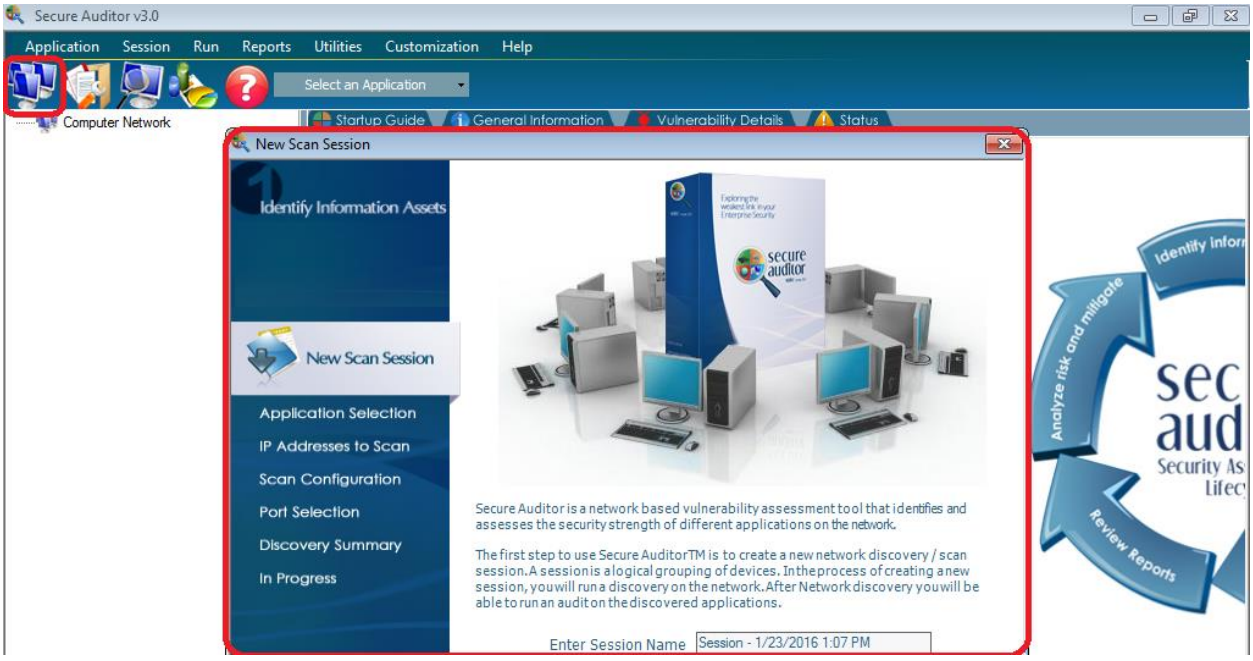
@Javangrpchannel



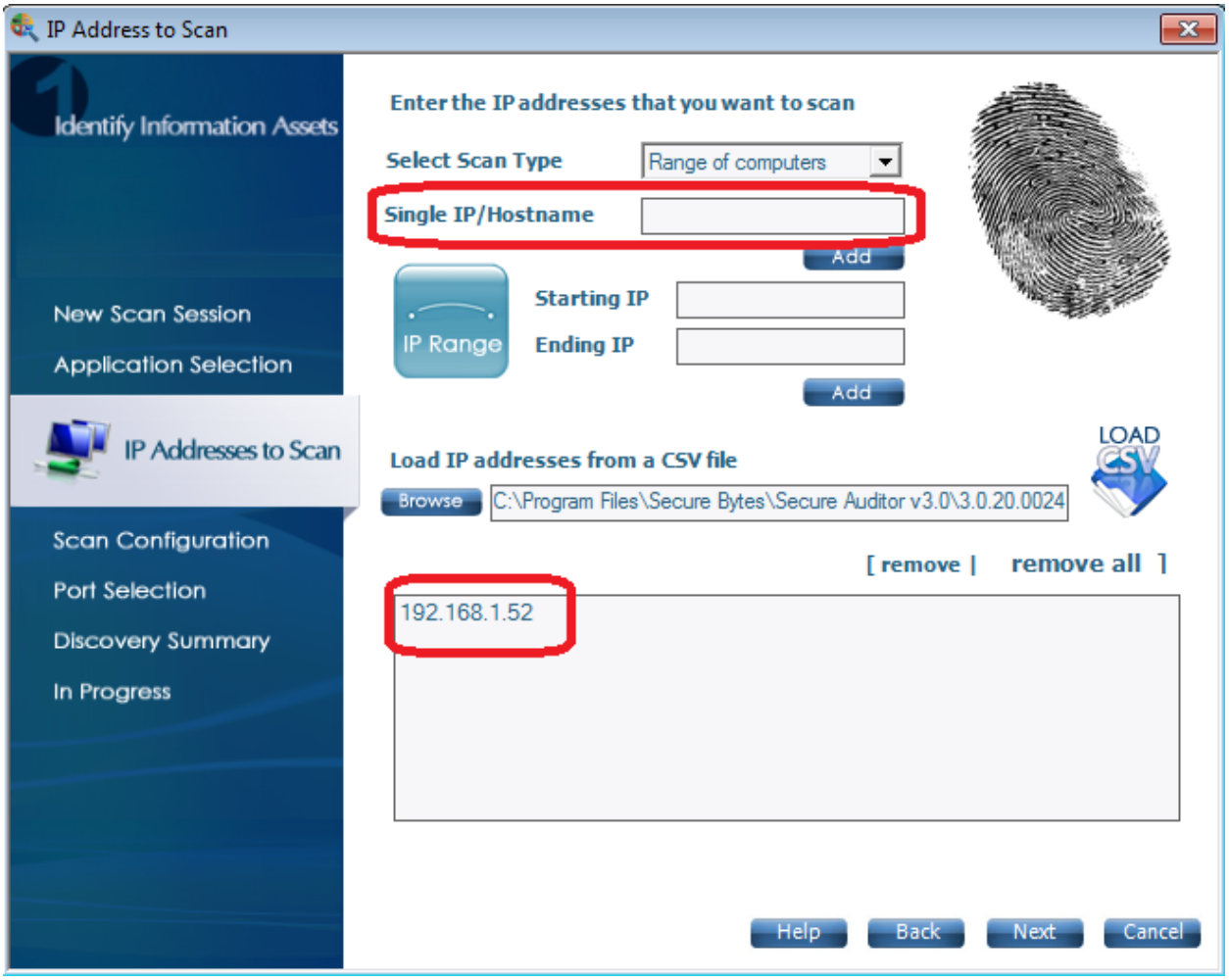
@Javangrpchannel

یکی دیگر از ابزارهایی که برای **Enumeration** استفاده می شود ابزاری است به نام **Secure Auditor** که به صورت زیر عمل می کند.

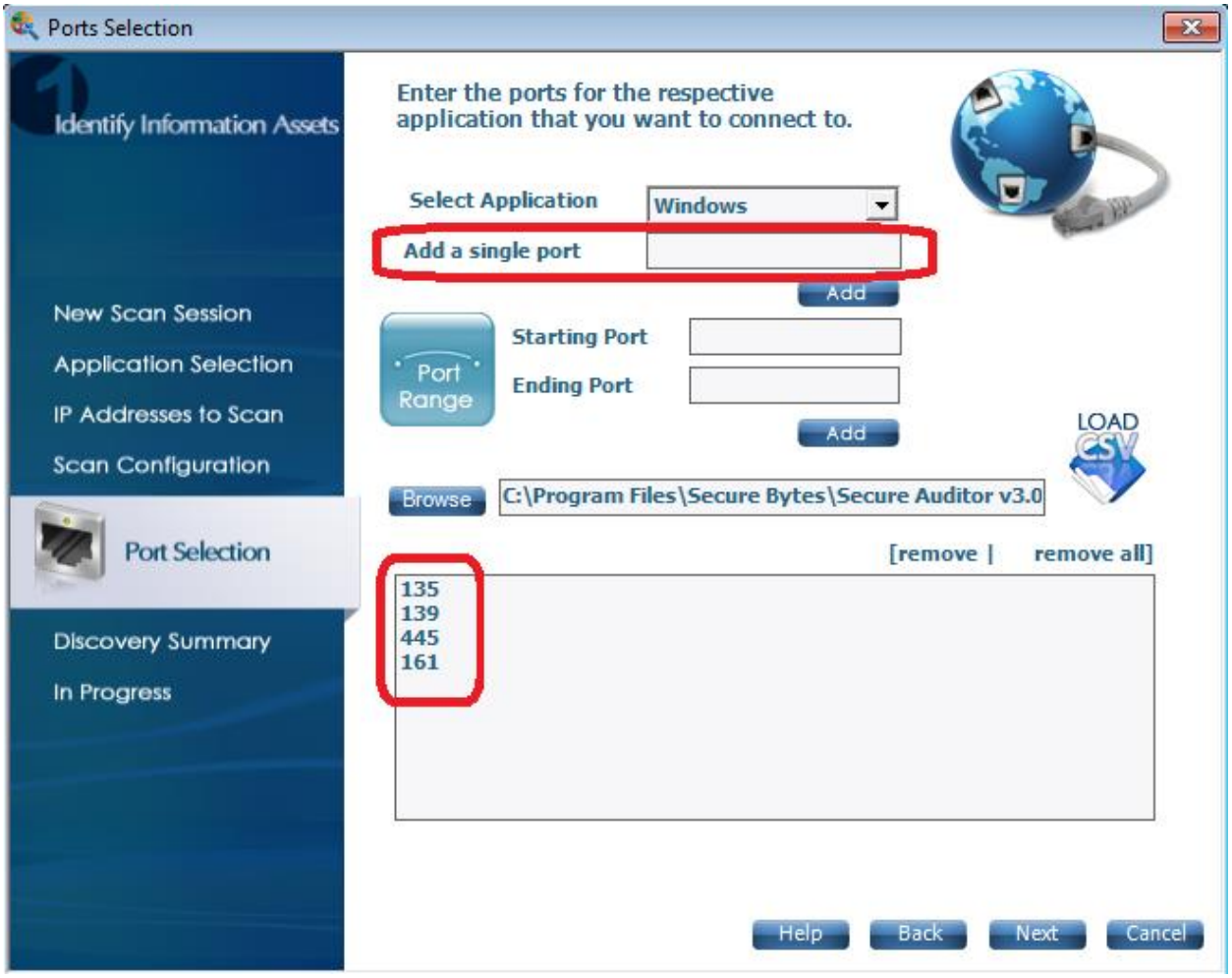


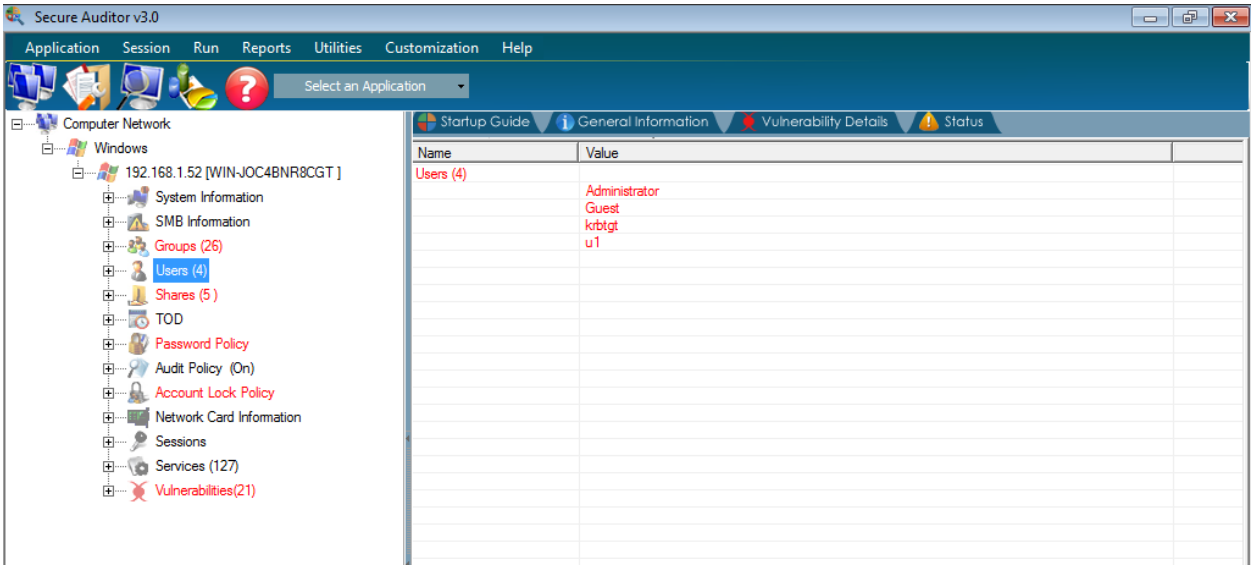
@Javangrpchannel

@Javangrpchannel



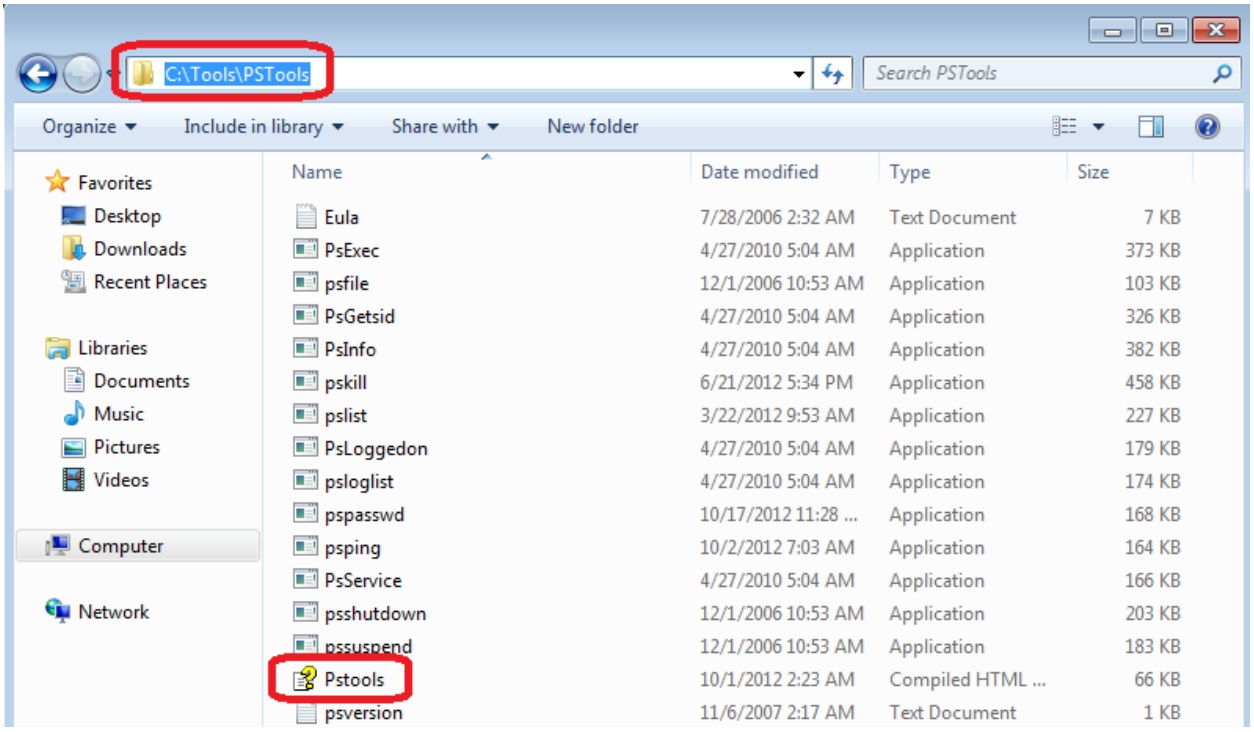
@techjob @Javangrpchannel

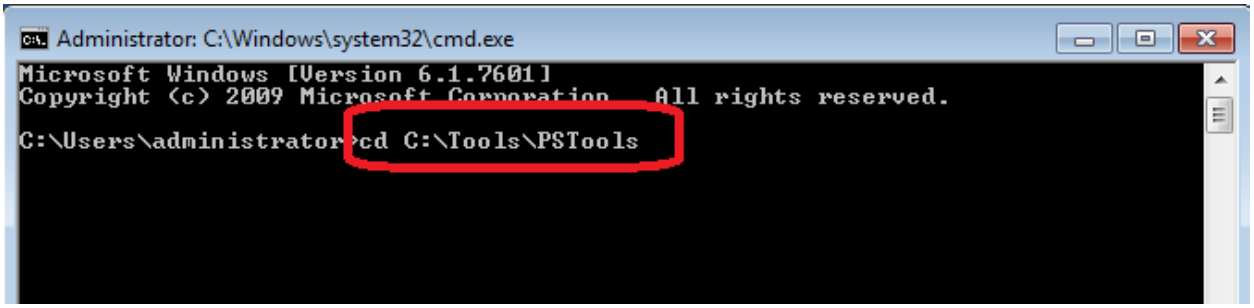

Ports Selection
Identify Information Assets
New Scan Session
Application Selection
IP Addresses to Scan
Scan Configuration
Port Selection
Discovery Summary
In Progress
Enter the ports for the respective application that you want to connect to.
Select Application
Windows
Add a single port
Add
Port Range
Starting Port
Ending Port
Add
LOAD CSV
Browse
C:\Program Files\Secure Bytes\Secure Auditor v3.0
[remove | remove all]
135
139
445
161
Help
Back
Next
Cancel

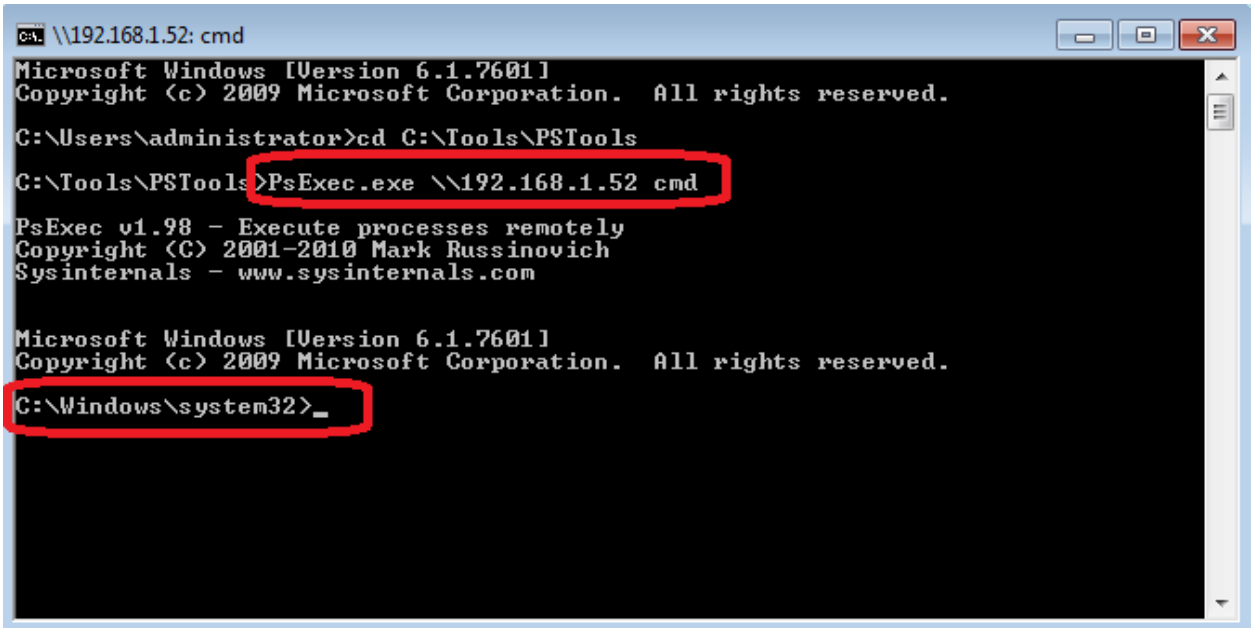

Secure Auditor v3.0
Application
Session
Run
Reports
Utilities
Customization
Help
Select an Application
Computer Network
Windows
192.168.1.52 [WIN-JOC4BNR8CGT]
System Information
SMB Information
Groups (26)
Users (4)
Shares (5)
TOD
Password Policy
Audit Policy (On)
Account Lock Policy
Network Card Information
Sessions
Services (127)
Vulnerabilities(21)
Startup Guide
General Information
Vulnerability Details
Status
Name
Value
Users (4)
Administrator
Guest
krbtgt
u1

@Javangrpchannel

یکی دیگر از ابزارهایی که برای **Enumeration** استفاده می شود ابزاری است به نام **PS Tools** که به صورت زیر عمل می کند.



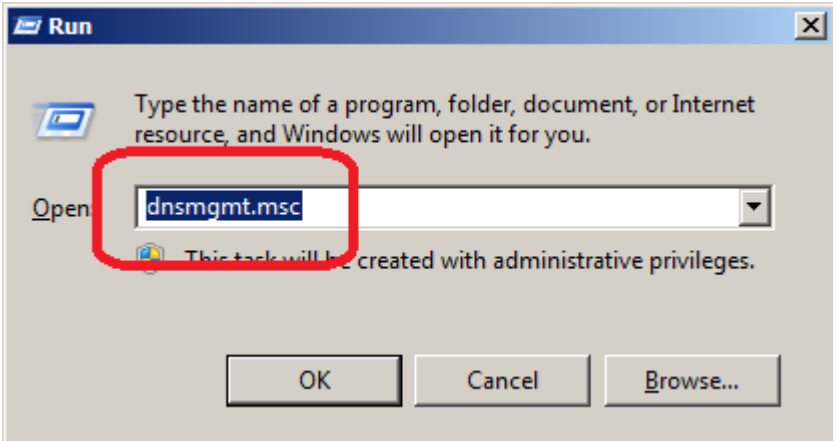




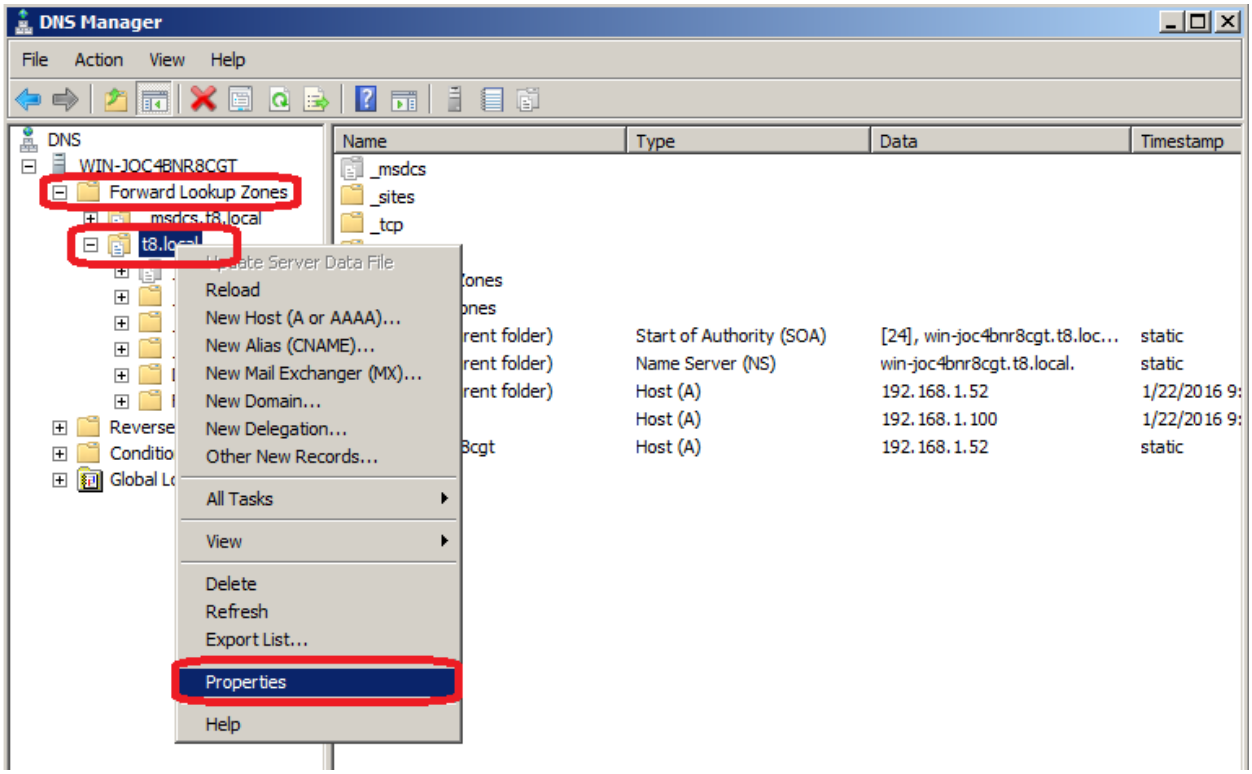
یکی دیگر از متدهای **Enumeration** استفاده از **DNS Zone Transfer Enumeration** می باشد اگر **DNS Zone Transfer** برروی سرور های ویندوزی فعال باشد شما می توانید با استفاده از ابزار **Nslookup** یک کپی از تمامی رکوردهای مربوط به آن **zone** را برروی سیستم خود دانلود کنید.

روش کار به صورت زیر می باشد:

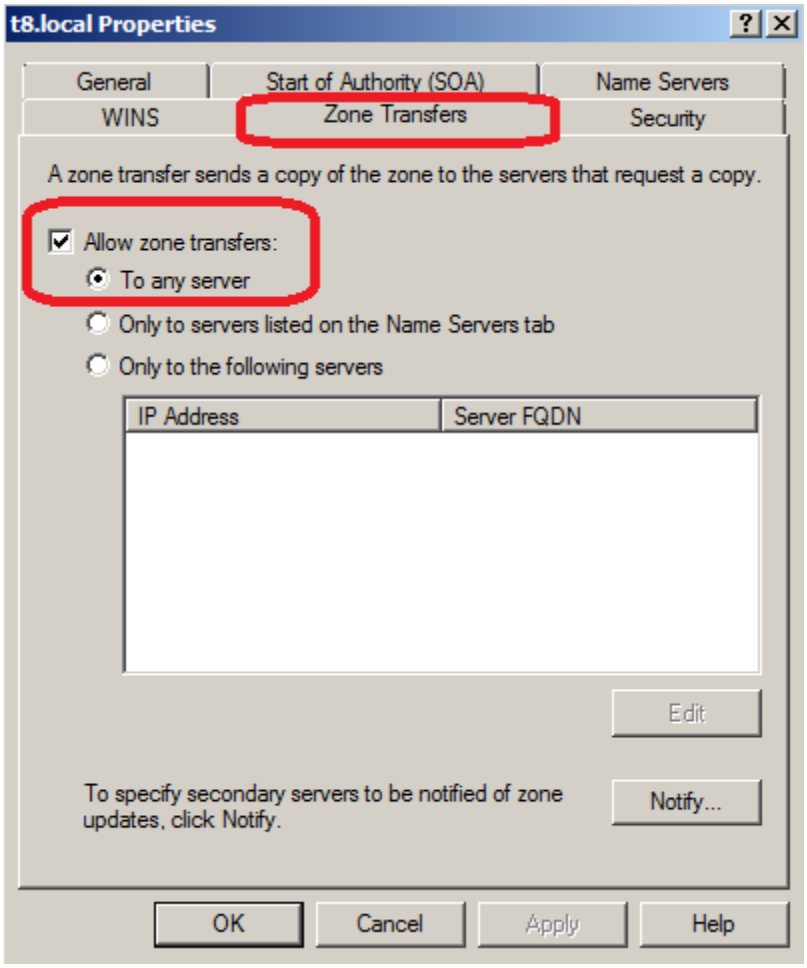
برای مشاهده تنظیمات مربوط به **DNS Zone Transfer** برروی سرور به صورت زیر عمل کنید:



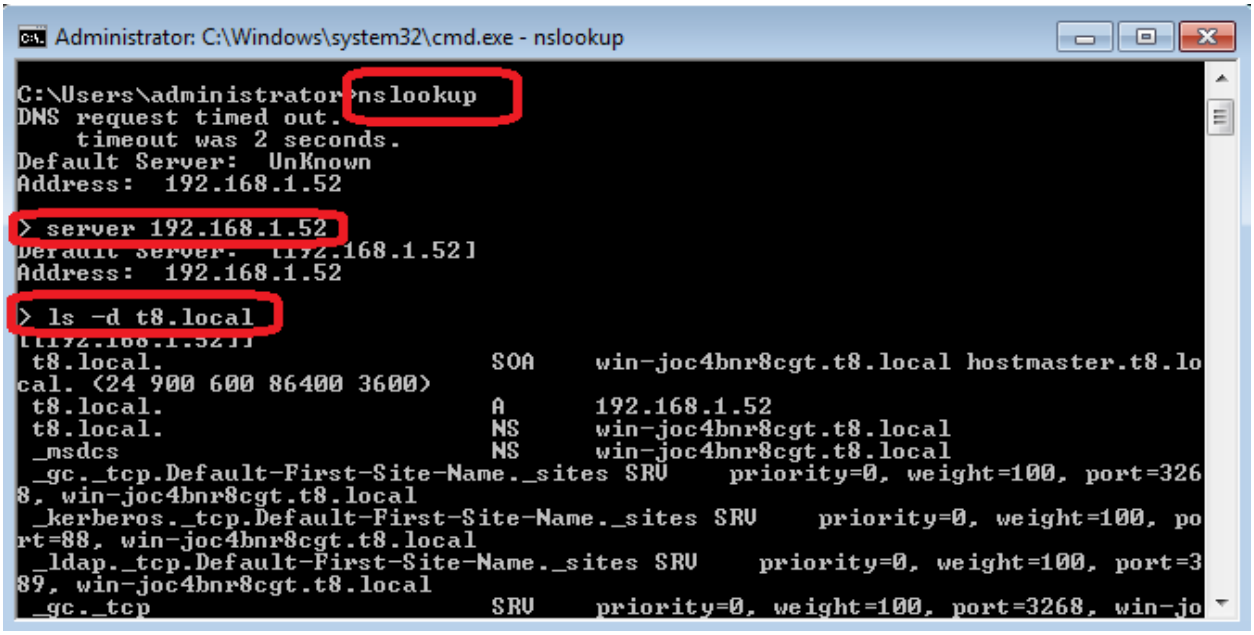
@Javangrpchannel



@Javangrpchannel
@techjob



برای گرفتن یک کپی از تمامی رکورد های سرور با استفاده از NSLookup به صورت زیر عمل کنید:


Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\Users\administrator>nslookup
DNS request timed out.
timeout was 2 seconds.
Default Server: UnKnown
Address: 192.168.1.52
> server 192.168.1.52
Address: 192.168.1.52
> ls -d t8.local
t8.local. SOA win-joc4bnr8cgt.t8.local hostmaster.t8.local. (24 900 600 86400 3600)
t8.local. A 192.168.1.52
t8.local. NS win-joc4bnr8cgt.t8.local
_msdcs NS win-joc4bnr8cgt.t8.local
_gc._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=3268, win-joc4bnr8cgt.t8.local
_kerberos._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=88, win-joc4bnr8cgt.t8.local
_ldap._tcp.Default-First-Site-Name._sites SRV priority=0, weight=100, port=389, win-joc4bnr8cgt.t8.local
_gc._tcp SRV priority=0, weight=100, port=3268, win-jo

@Javangrpchannel

Module 05 System Hacking

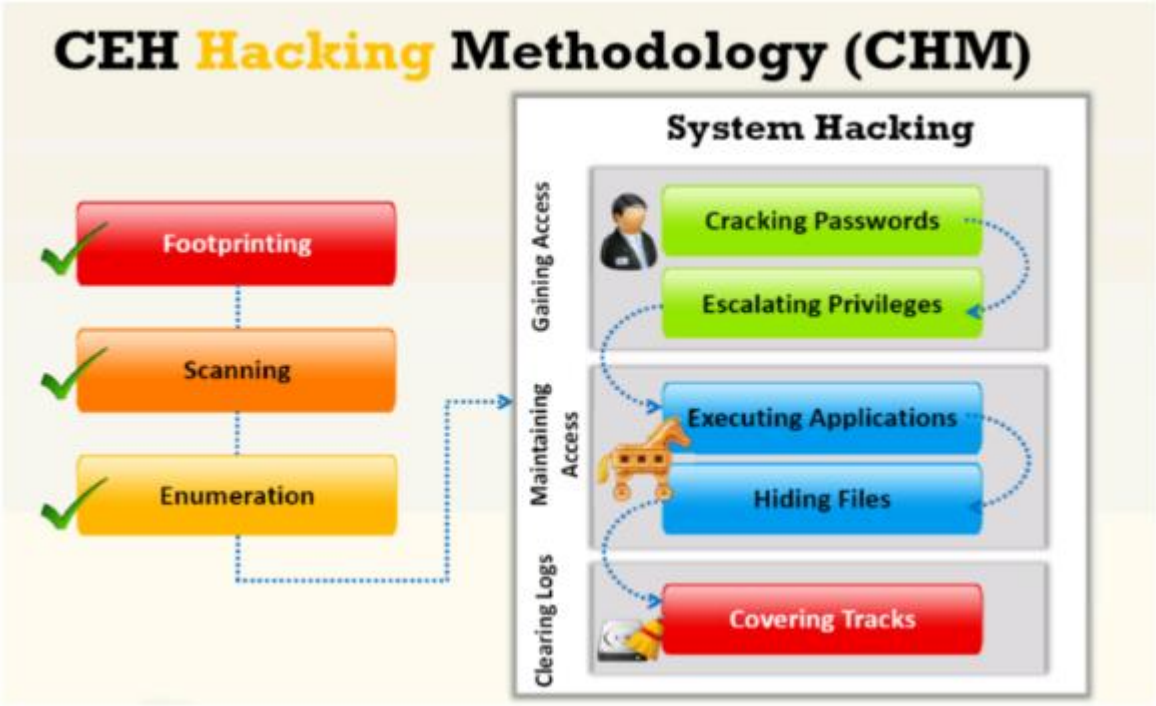
@Javangrpchannel

System Hacking: Goals

	Hacking-Stage	Goal	Technique/Exploit Used
	Gaining Access	To collect enough information to gain access	Password eavesdropping, brute forcing
	Escalating Privileges	To create a privileged user account if the user level is obtained	Password cracking, known exploits
	Executing Applications	To create and maintain backdoor access	Trojans
	Hiding Files	To hide malicious files	Rootkits
	Covering Tracks	To hide the presence of compromise	Clearing logs

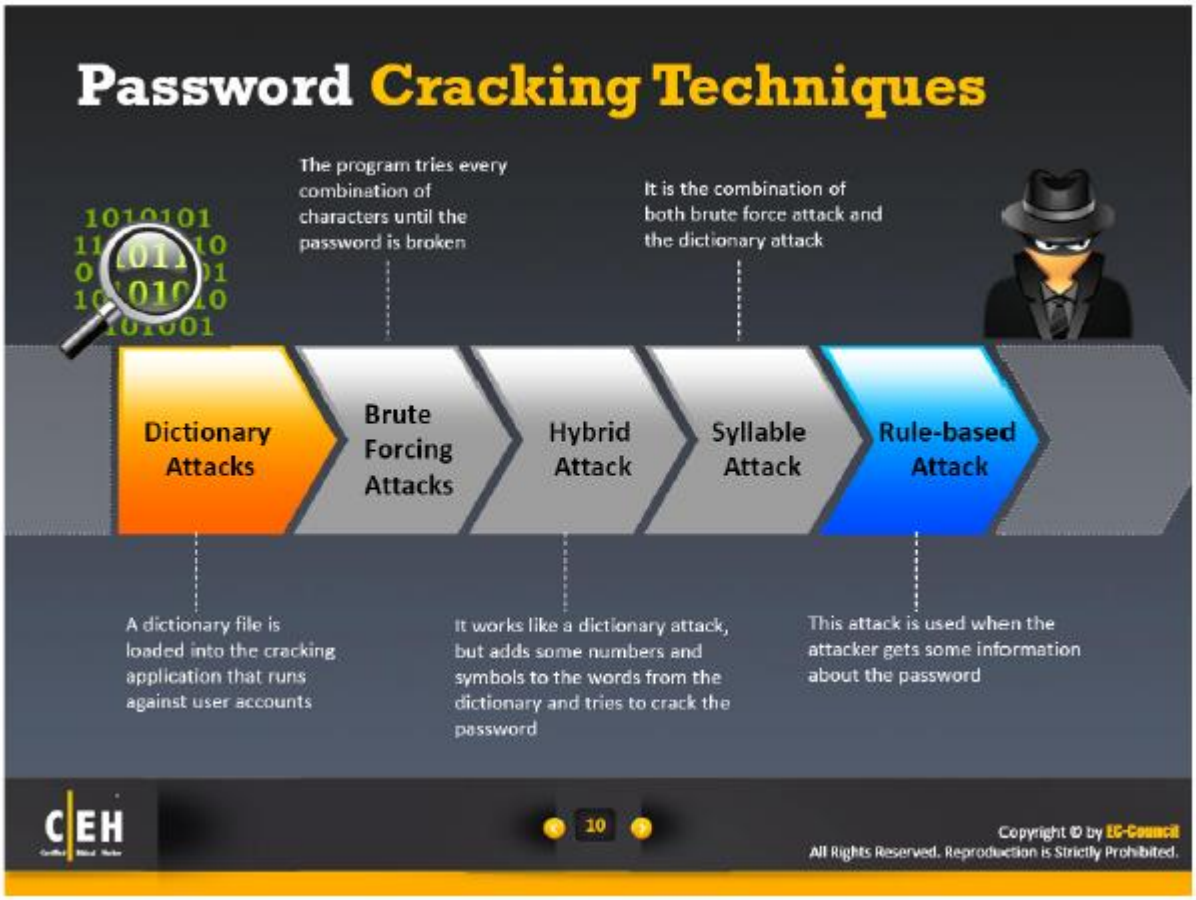
@Javangrpchannel

اولین مرحله ایی که در **System Hacking** وجود دارد **Cracking Password** می باشد.



@Javangrpchannel

@techjob

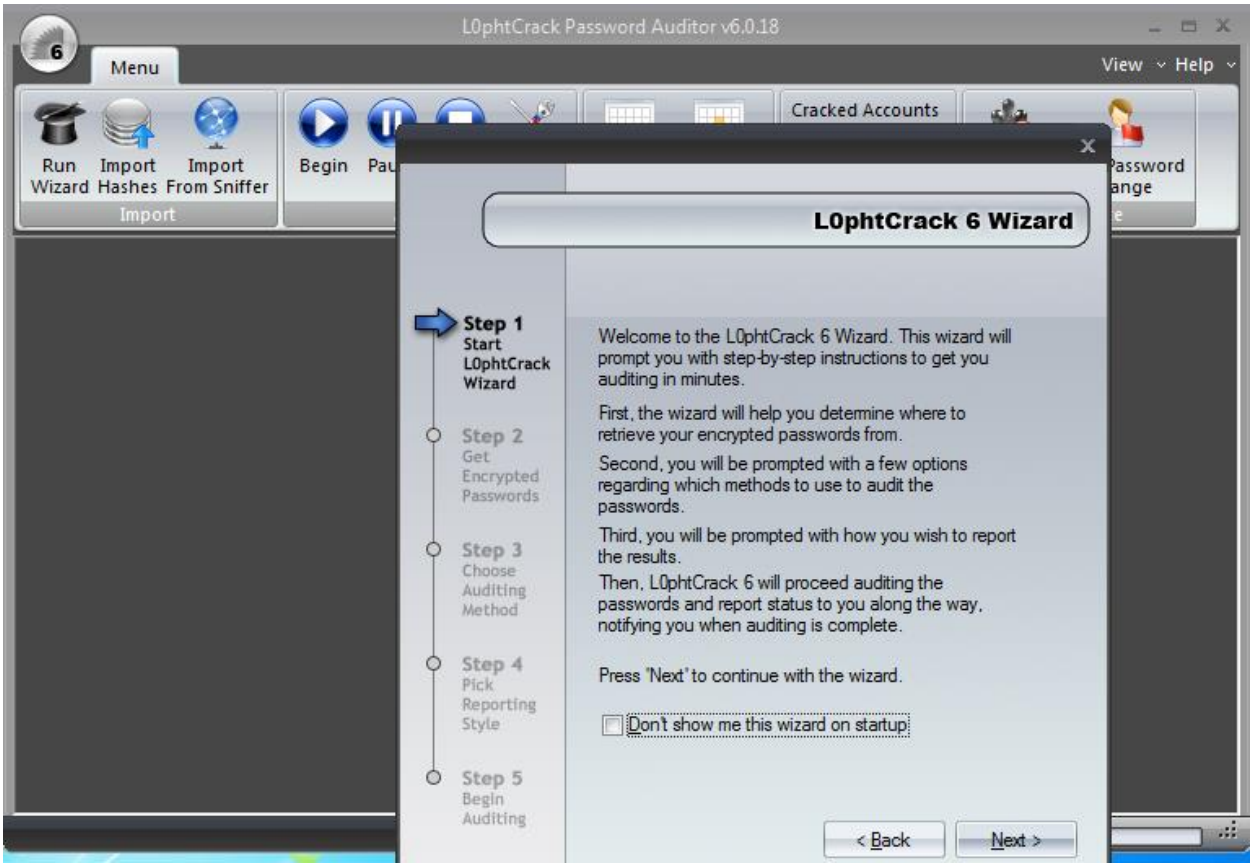


یکی از ابزارهایی که برای Crack Password استفاده می شود L0pht Crack می باشد که هم به صورت Local و هم به صورت Remote کار می کند با اجرای این برنامه برروی یک سیستم می توانید کلیه پسورد های یک سیستم را بدست آورید.

برای Crack Password به صورت Remote نیاز به Session باز یا Agent L0pht Crack می باشد.

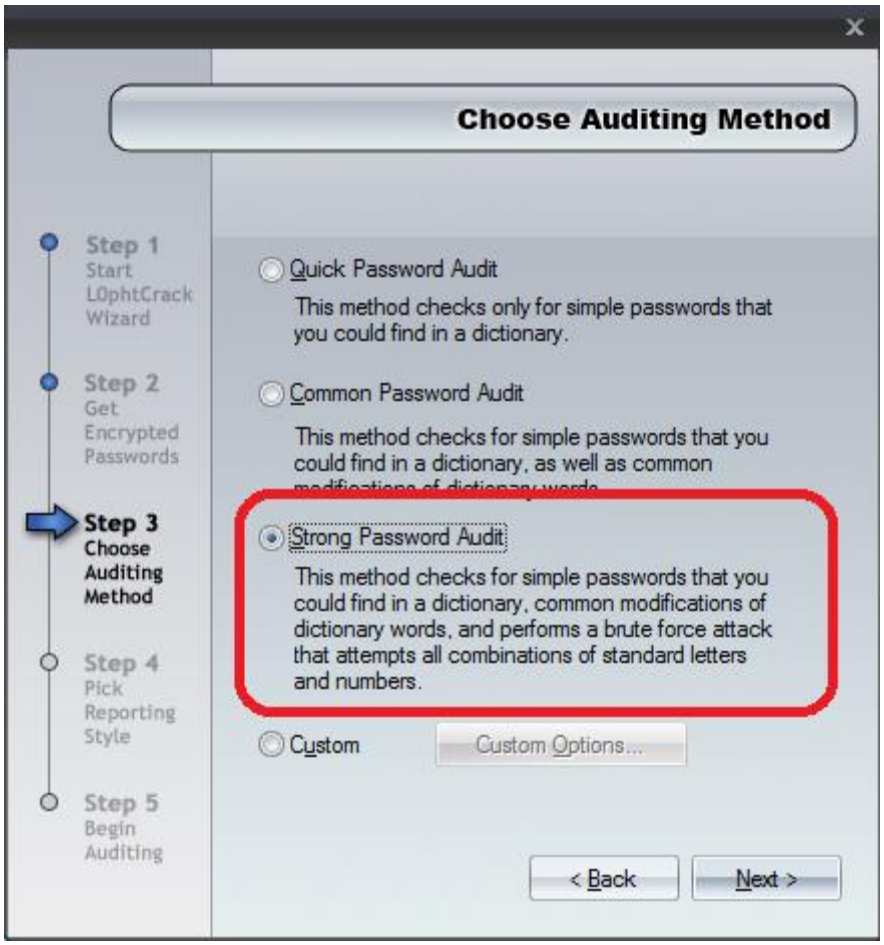
@Javangrpchannel

روش کار این ابزار به صورت زیر می باشد:

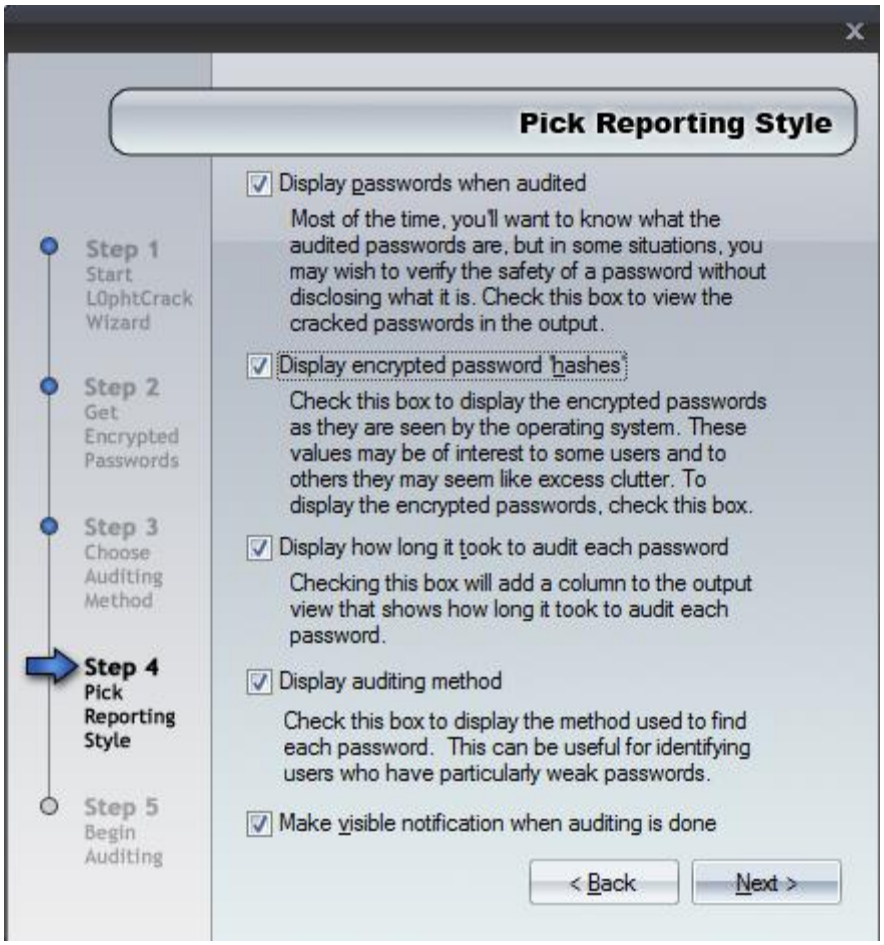


@Javangrpchannel

@Javangrpchannel



@Javangrpchannel



@Javangrpchannel

@techjob