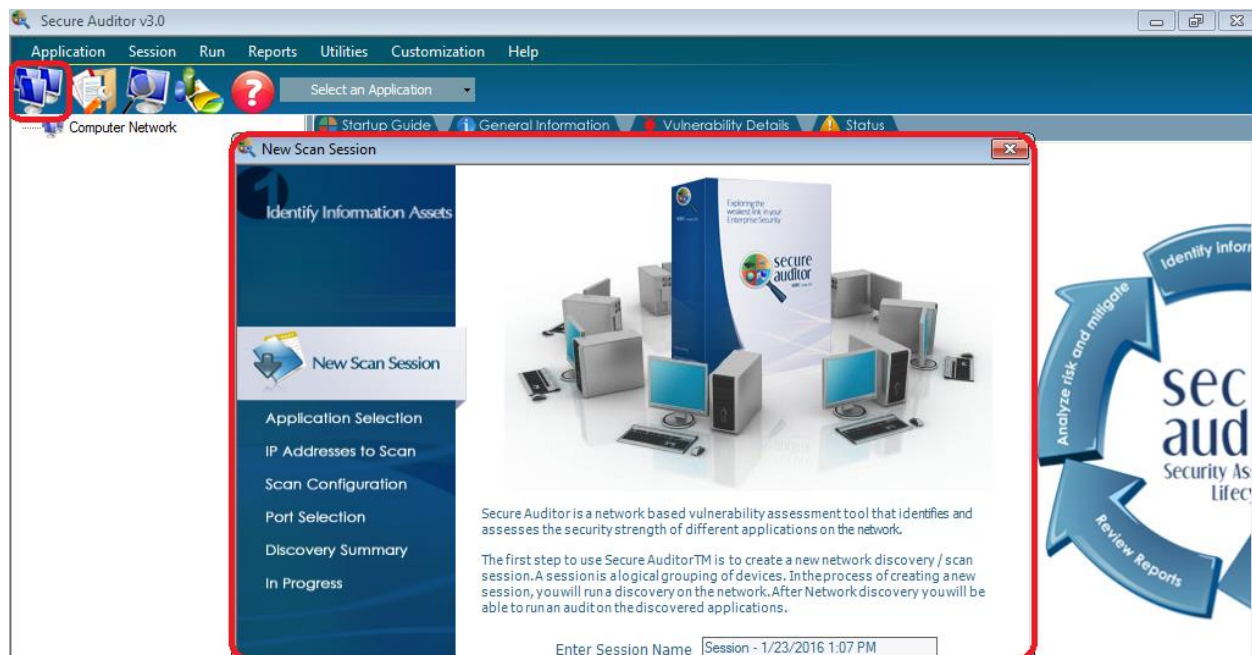


یکی دیگر از ابزارهایی که برای Enumeration استفاده می شود ابزاری است به نام Secure Auditor که به صورت زیر عمل می کند.





IP Address to Scan

1 Identify Information Assets

New Scan Session
Application Selection

IP Addresses to Scan

Scan Configuration
Port Selection
Discovery Summary
In Progress

Enter the IP addresses that you want to scan

Select Scan Type Range of computers

Single IP/Hostname

Add

IP Range

Starting IP

Ending IP

Add

Load IP addresses from a CSV file

Browse

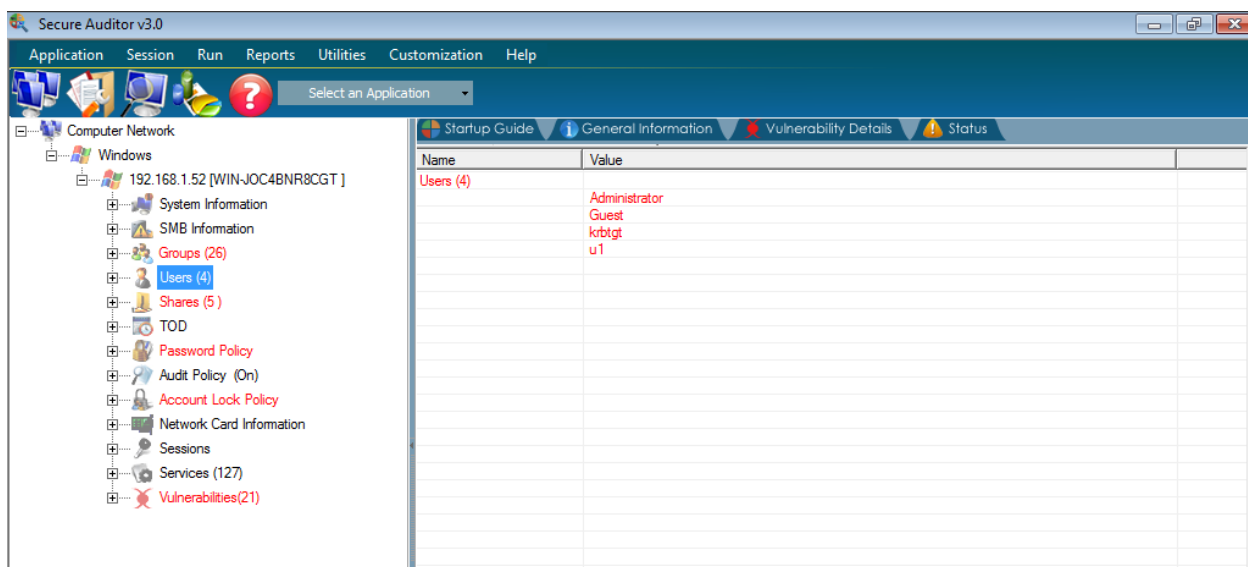
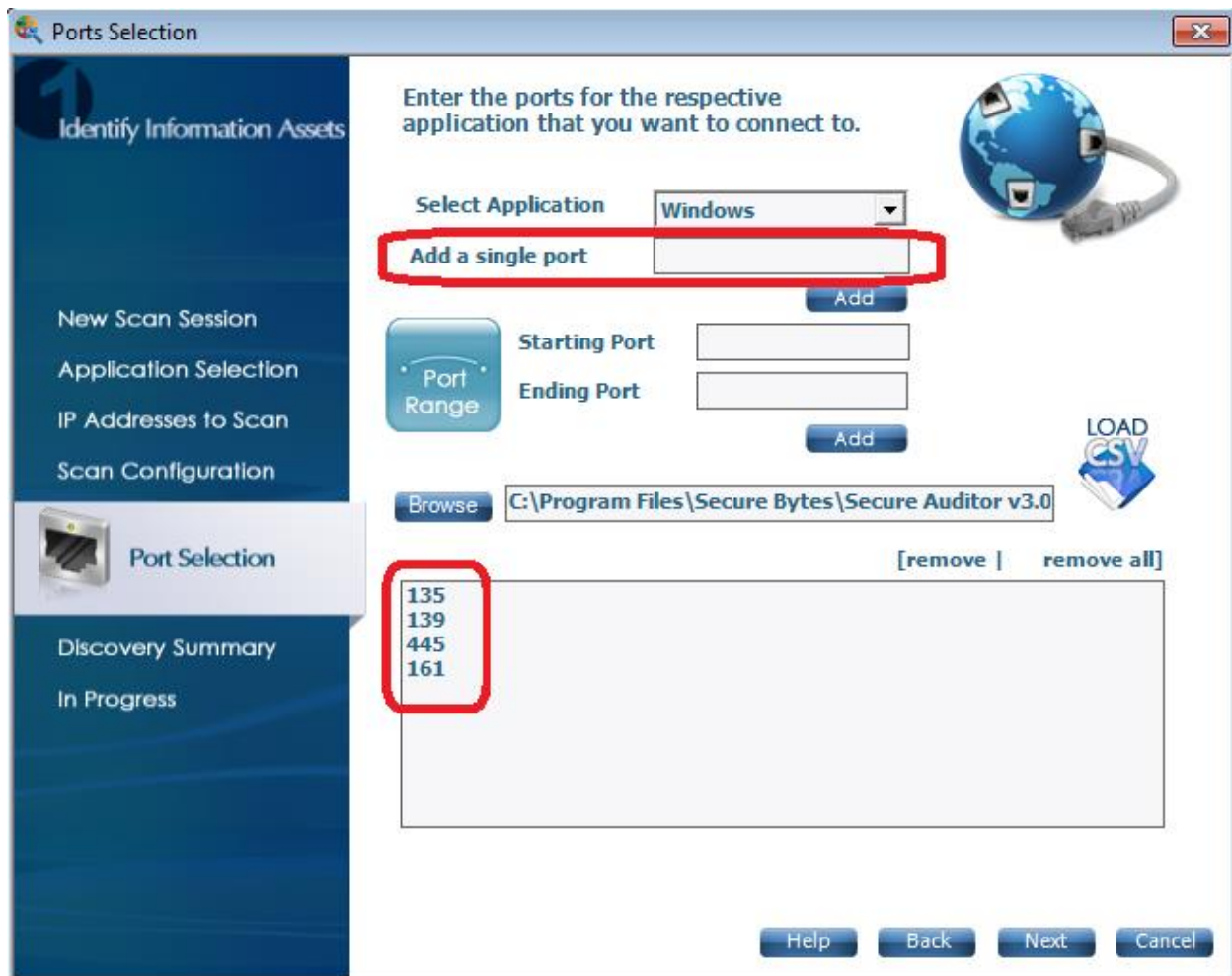
LOAD CSV

[remove | remove all]

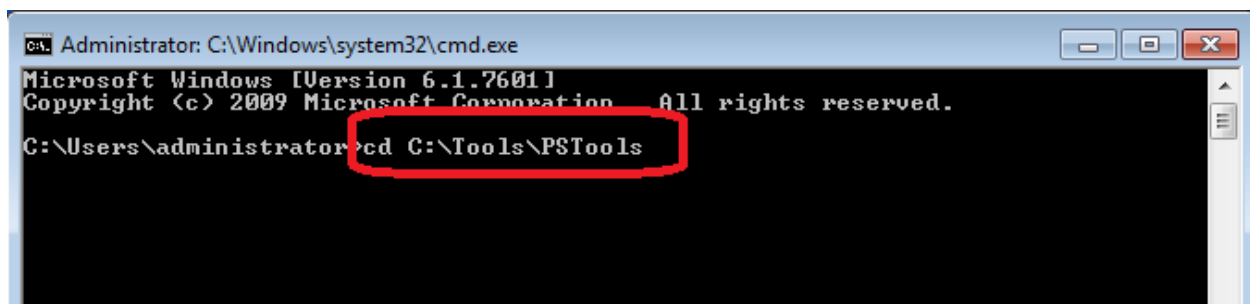
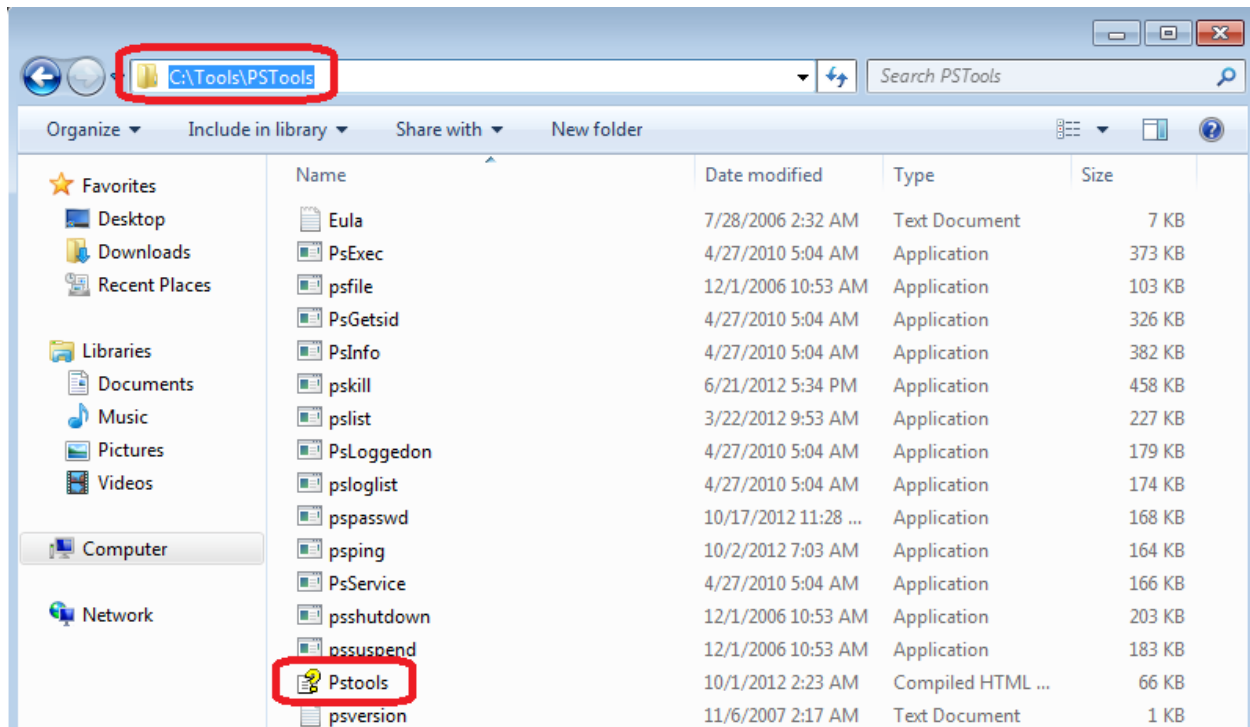
192.168.1.52

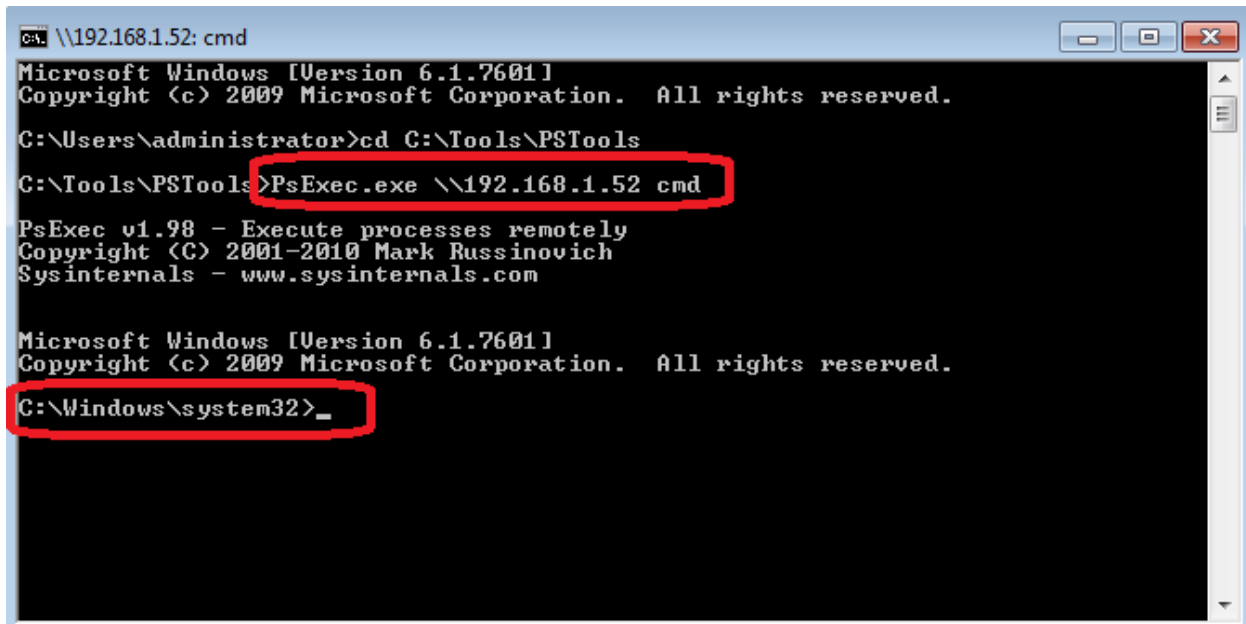
Help Back Next Cancel





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





A screenshot of a Windows command prompt window titled "\\192.168.1.52: cmd". The window shows the execution of PsExec to run a command remotely. The first prompt is "C:\Users\administrator>cd C:\Tools\PSTools". The second prompt is "C:\Tools\PSTools>PsExec.exe \\192.168.1.52 cmd", which is highlighted with a red box. The output shows "PsExec v1.98 - Execute processes remotely" and "Copyright (C) 2001-2010 Mark Russinovich". The next prompt is "Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved." followed by "C:\Windows\system32>_", which is also highlighted with a red box.

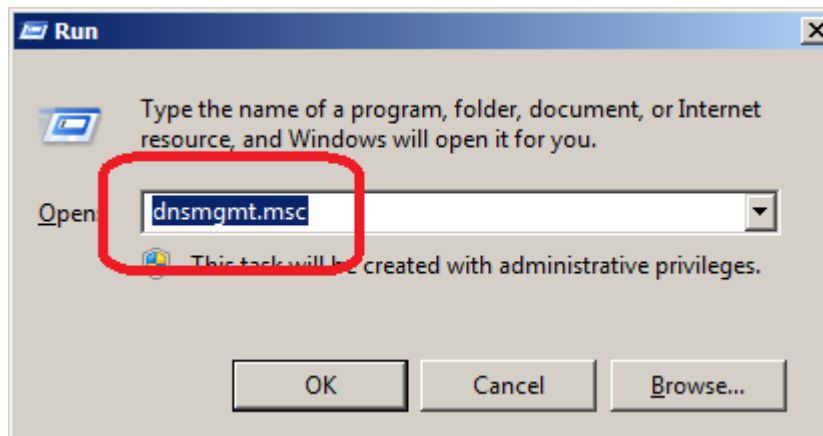
```
C:\Users\administrator>cd C:\Tools\PSTools
C:\Tools\PSTools>PsExec.exe \\192.168.1.52 cmd
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

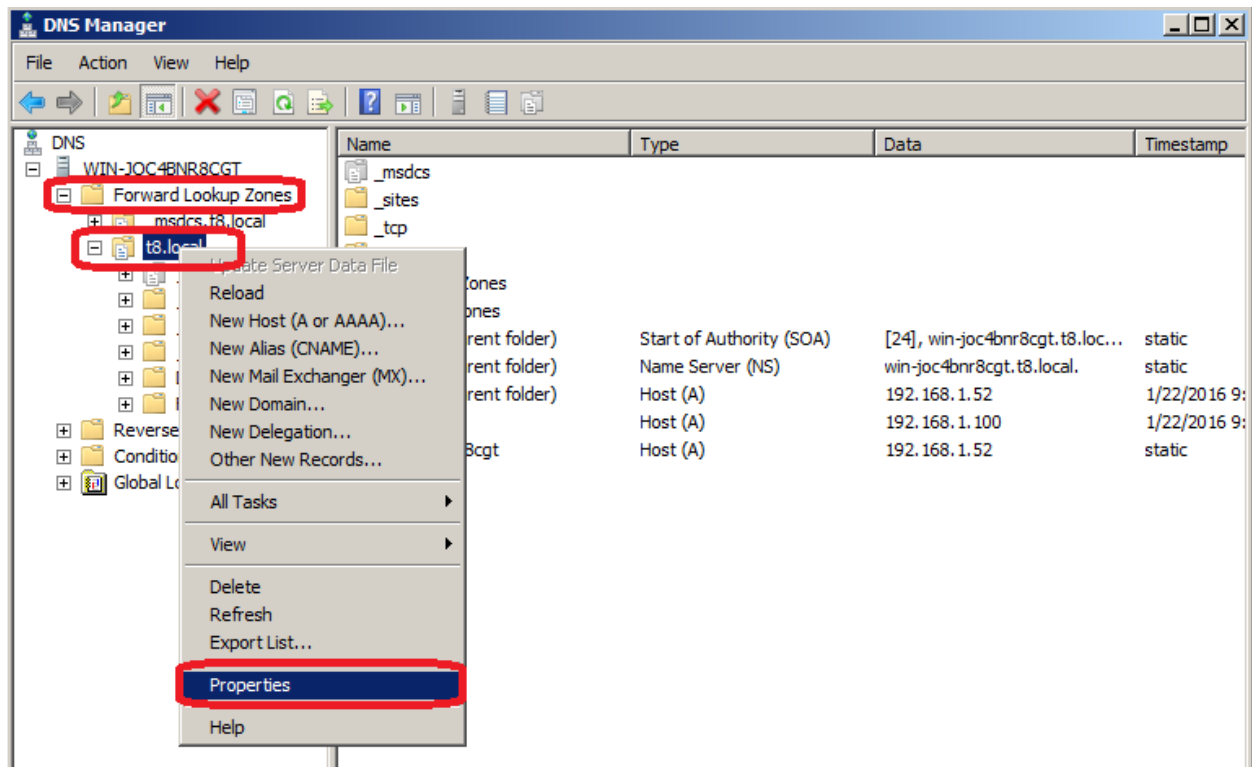
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>_
```

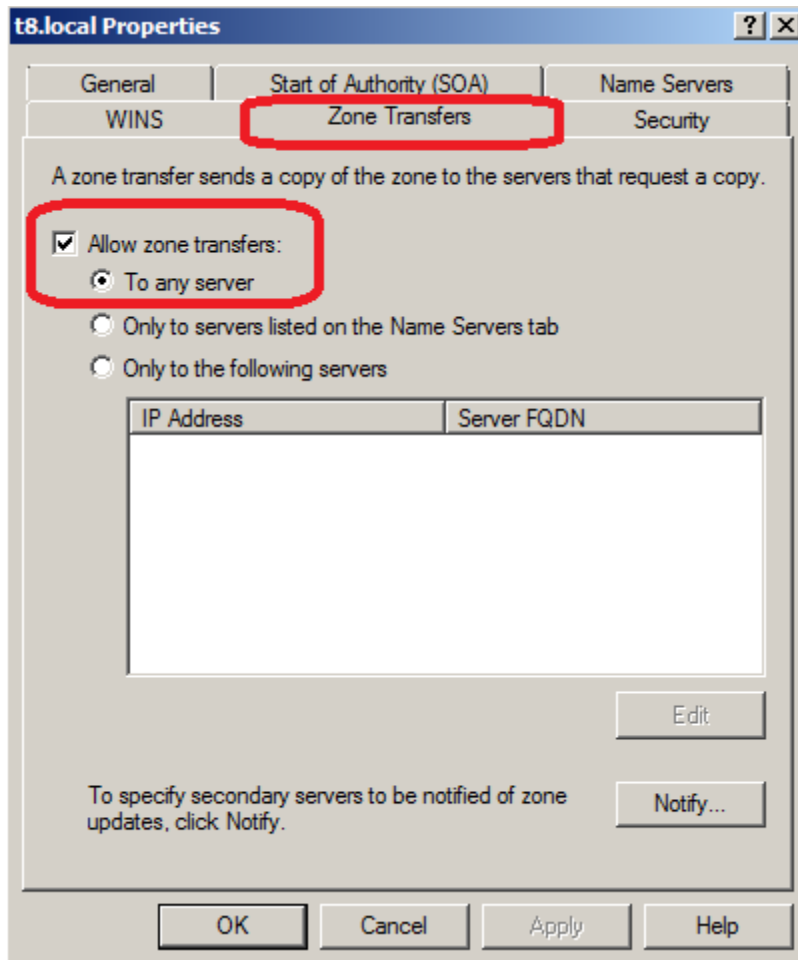
یکی دیگر از متدهای Enumeration استفاده از DNS Zone Transfer Enumeration می باشد
اگر DNS Zone Transfer بر روی سرور های ویندوزی فعال باشد شما می توانید با استفاده از ابزار
Nslookup یک کپی از تمامی رکوردهای مربوط به آن zone را بر روی سیستم خود دانلود کنید.

روش کار به صورت زیر می باشد:

برای مشاهده تنظیمات مربوط به DNS Zone Transfer بر روی سرور به صورت زیر عمل کنید:







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

```
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
Default server:  192.168.1.52
Address:  192.168.1.52

> ls -d t8.local
[[192.168.1.52]]
t8.local.
cal. (24 900 600 86400 3600)
t8.local.
t8.local.
_tsdcs
_gc._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=326
8, win-joc4bnr8cgt.t8.local
_kerberos._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, po
rt=88, win-joc4bnr8cgt.t8.local
_ldap._tcp.Default-First-Site-Name._sites SRV    priority=0, weight=100, port=3
89, win-joc4bnr8cgt.t8.local
_gc._tcp
SRV    priority=0, weight=100, port=3268, win-jo
```

Module 05 System Hacking




System Hacking

Module 05

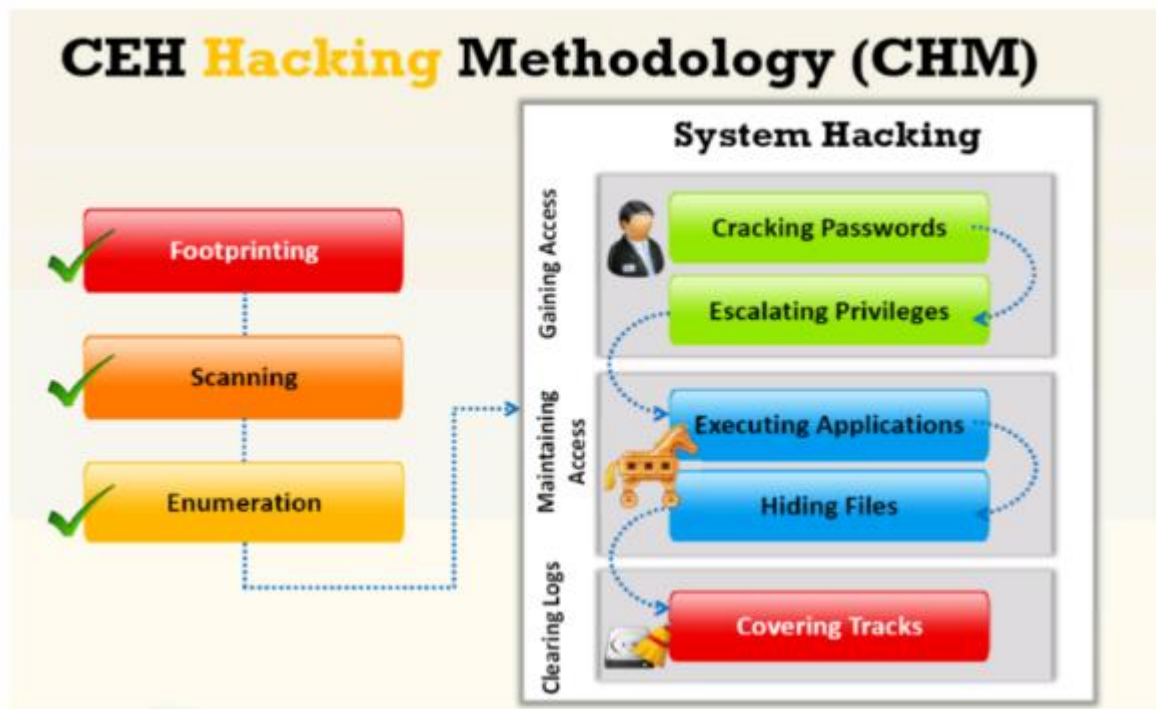
Unmask the **Invisible Hacker.**

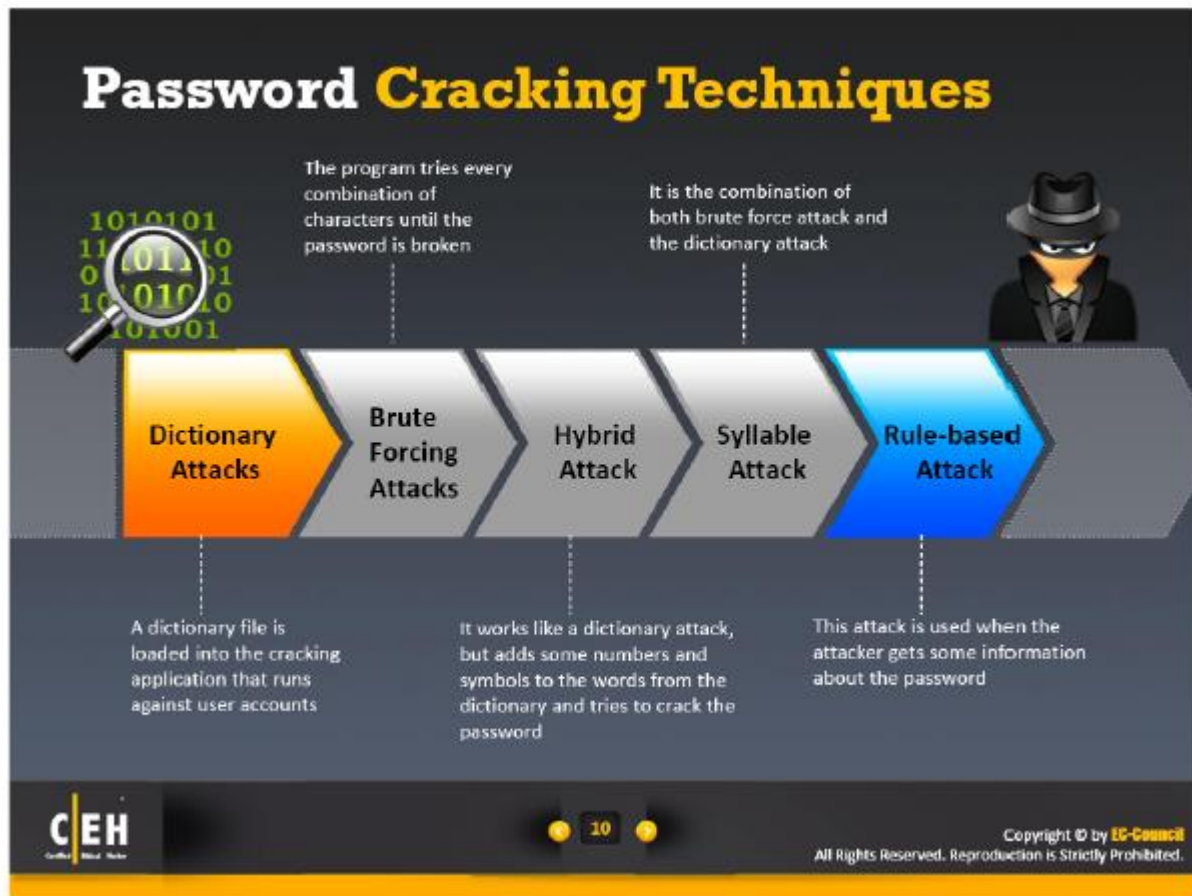


System Hacking: Goals

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

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

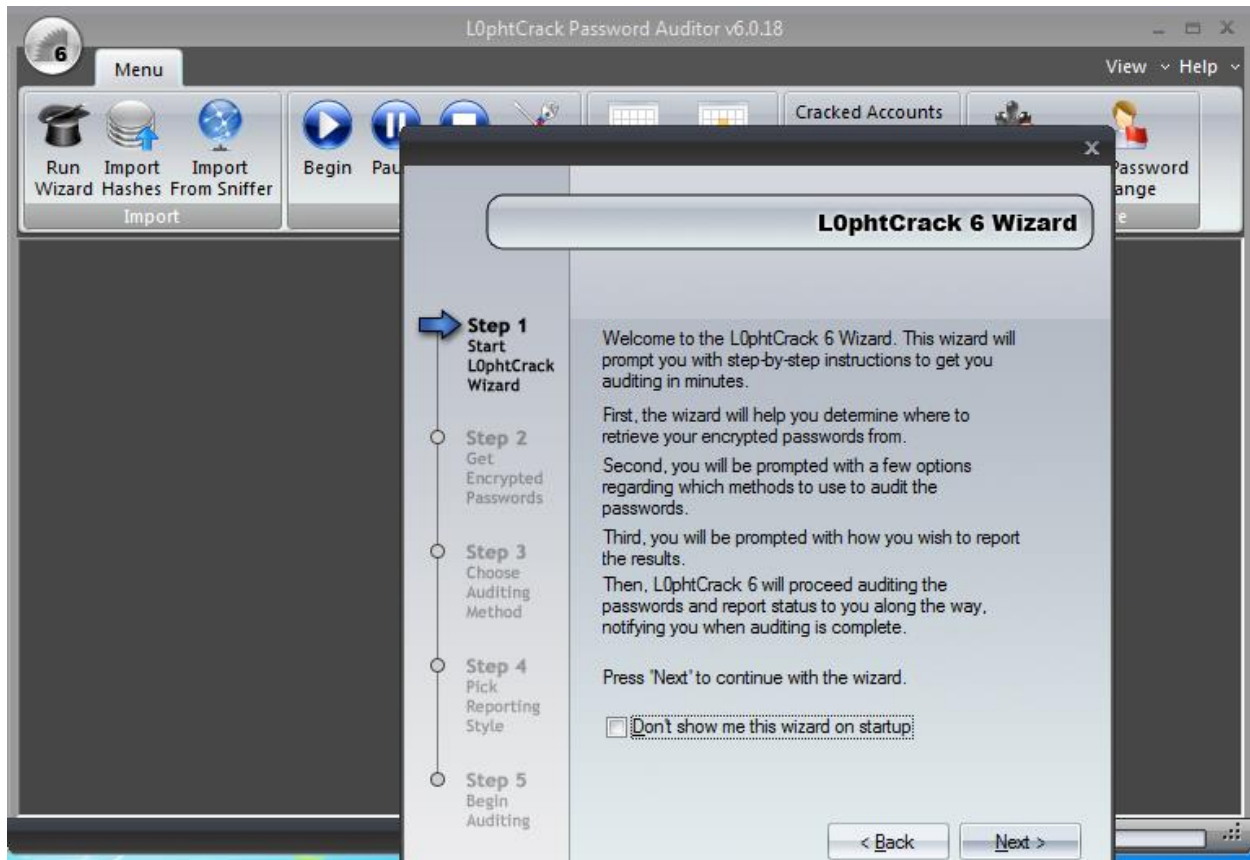




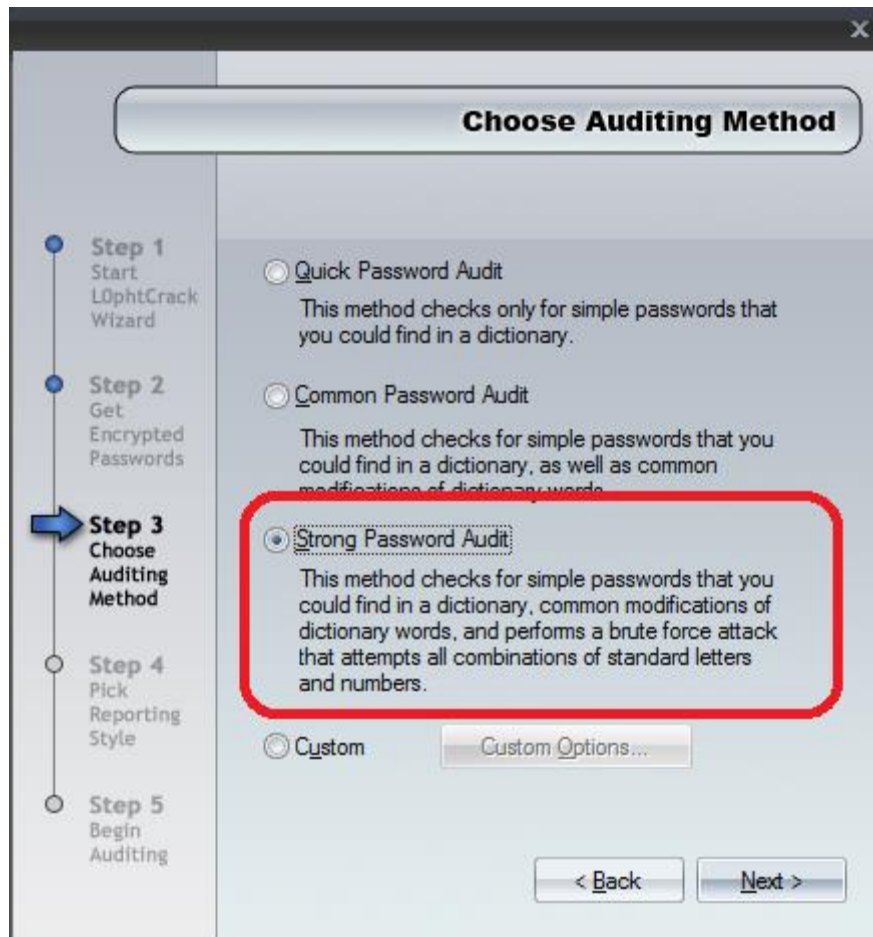
یکی از ابزارهایی که برای Crack Password استفاده می شود L0pht Crack می باشد که هم به صورت Local و هم به صورت Remote کار می کند با اجرای این برنامه بر روی یک سیستم می توانید کلیه پسوردهای یک سیستم را بدست آورید.

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

روش کار این ابزار به صورت زیر می باشد:







The screenshot shows a window titled "Pick Reporting Style" with a close button (X) in the top right corner. On the left side, there is a vertical progress bar with five steps: Step 1 (Start L0phtCrack Wizard), Step 2 (Get Encrypted Passwords), Step 3 (Choose Auditing Method), Step 4 (Pick Reporting Style), and Step 5 (Begin Auditing). Step 4 is currently selected, indicated by a blue arrow pointing to it. The main area of the window contains five checkboxes, all of which are checked. Each checkbox is followed by a label and a descriptive paragraph. At the bottom right, there are two buttons: "< Back" and "Next >".

Pick Reporting Style

- ☒ Display passwords when audited
Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.
- ☒ Display encrypted password hashes
Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.
- ☒ Display how long it took to audit each password
Checking this box will add a column to the output view that shows how long it took to audit each password.
- ☒ Display auditing method
Check this box to display the method used to find each password. This can be useful for identifying users who have particularly weak passwords.
- ☒ Make visible notification when auditing is done

< Back Next >

