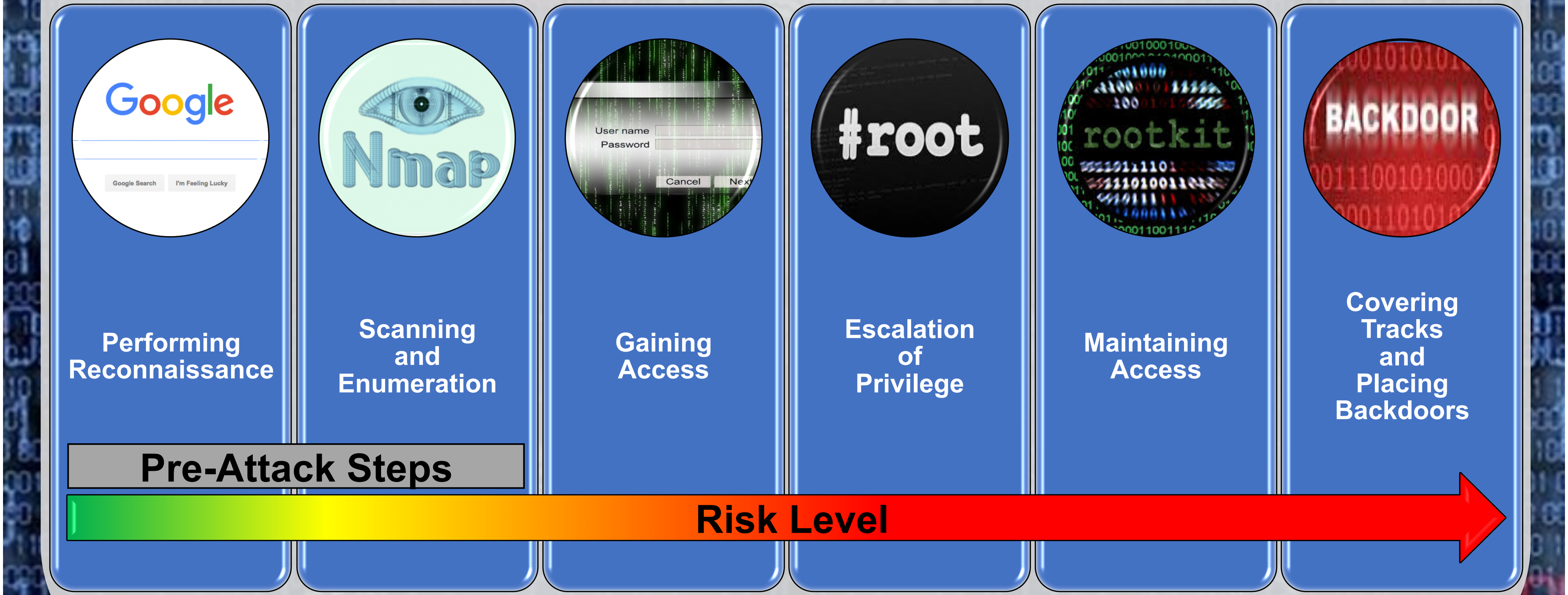
Covering Tracks and Installing Backdoors

(…Dig in deep)

http://www.JasonDion.com

Attacker’s Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

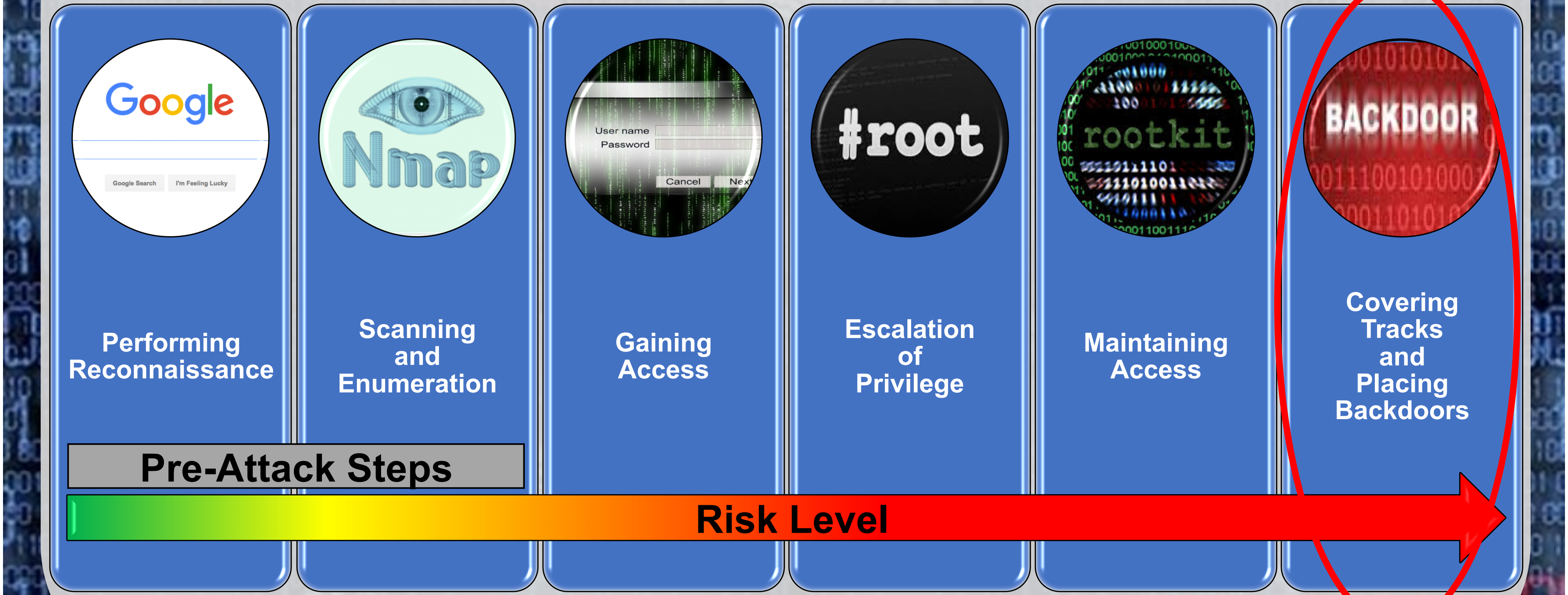
Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Attacker’s Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Covering Tracks and Installing Backdoors

- Erase the Evidence
- Modify the Evidence
- Disable Logging
- Clear Log Files
- Hiding files and folders
- Installing rootkits/backdoors
- Setup call backs for designated times

Erase the Evidence

- Temporary files
- Log files
- Previous stage malware (if used)

Modify the Evidence

- Change the contents of log files
- Timestomp access times
- Change the user identity

Timestomp

- touch (Linux, Unix, OSX)
  - Updates time to the current time
- ctime (Linux, Unix, OSX)
  - Change the time to a given date/time
- Meterpreter has built-in tool

Disable Logging

- Auditpol is command-line tool from NT Resource Kit

Clear Log Files

- Winzapper, Evidence Eliminator, and Elsave

- Erases the log file, covers your tracks but the administrators will know someone was there…

Hiding Files and Folders

- Linux, Unix, OSX
  - Hidden files start with .
- Windows
  - Alternate Data Streams
- Use hidden attribute
- Put files in low traffic areas
- Hide in slack space

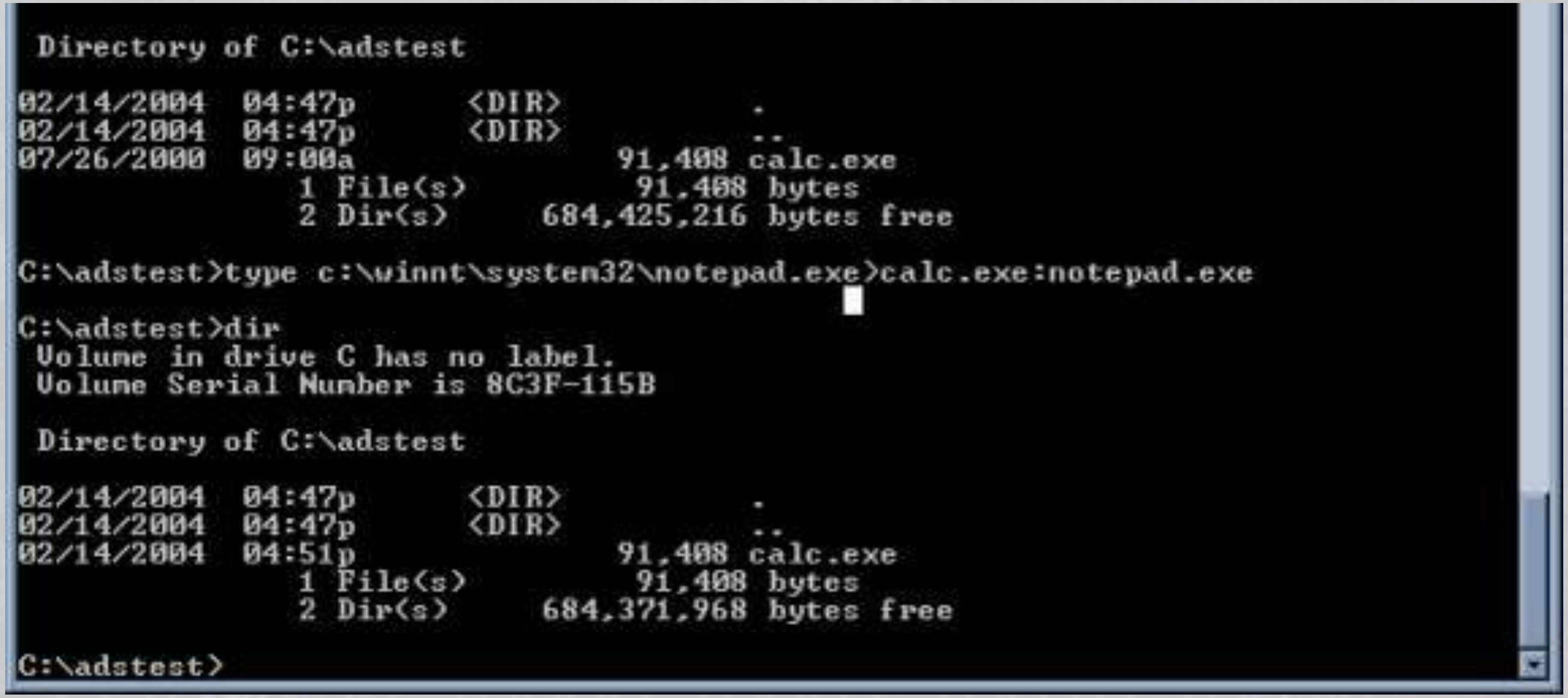
Alternate Data Streams

- ADS provides a method to hide malware on NTFS systems
  - Streams are almost completely hidden

- Create an ADS
  - type notepad.exe > calc.exe:notepad.exe

- Run the hidden file
  - start calc.exe:notepad.exe

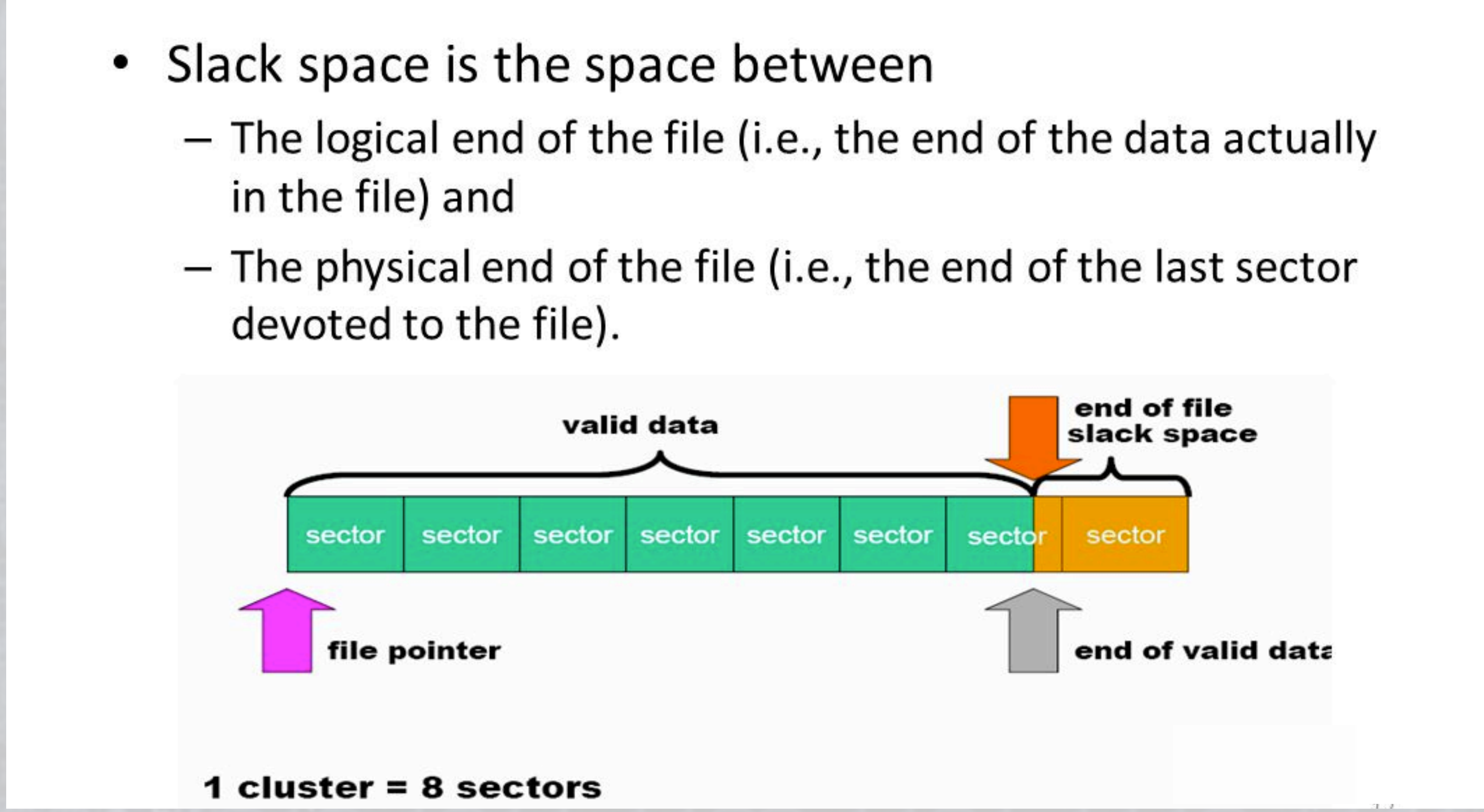
Alternate Data Streams



```
 Directory of C:\adstest

02/14/2004  04:47p      <DIR>          .
02/14/2004  04:47p      <DIR>          ..
07/26/2000  09:00a              91,408 calc.exe
               1 File(s)         91,408 bytes
               2 Dir(s)     684,425,216 bytes free

C:\adstest>type c:\winnt\system32\notepad.exe>calc.exe:notepad.exe

C:\adstest>dir
 Volume in drive C has no label.
 Volume Serial Number is 8C3F-115B

 Directory of C:\adstest

02/14/2004  04:47p      <DIR>          .
02/14/2004  04:47p      <DIR>          ..
02/14/2004  04:51p              91,408 calc.exe
               1 File(s)         91,408 bytes
               2 Dir(s)     684,371,968 bytes free

C:\adstest>
```

Hiding in the Slack Space

- Bmap is used on Linux to hide files in slack space



- Slack space is the space between
  - The logical end of the file (i.e., the end of the data actually in the file) and
  - The physical end of the file (i.e., the end of the last sector devoted to the file).

Installing Rootkits and Backdoors

- Use rootkits (originally Linux only, now on Windows too)
    - FU
    - Vanquish
    - Hacker Defender
    - AFX
- Setup Backdoors

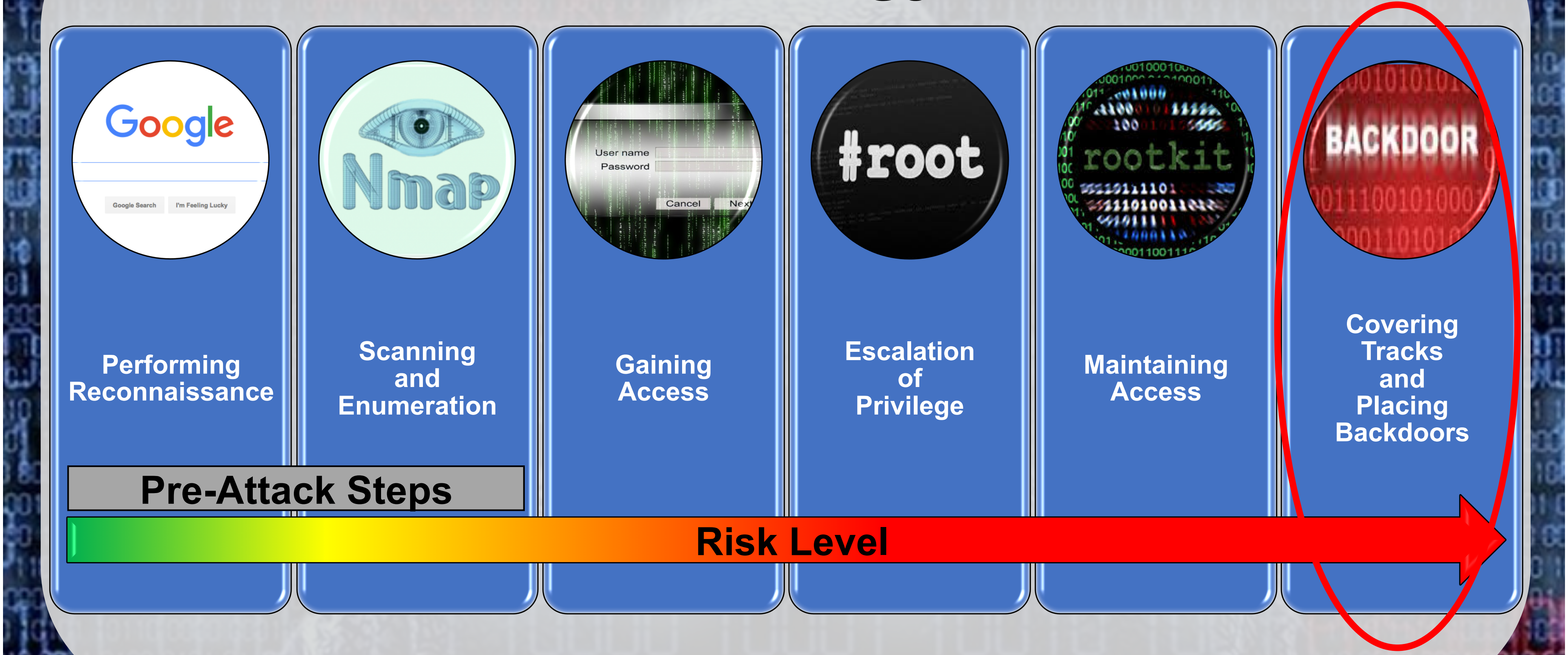
Setup Callbacks (Windows)

- sc
  - Manages services (start/stop)
- netsh
  - Use to modify Windows Firewall
- at
  - Schedule programs to run at certain times

Setup Callbacks (Linux, Unix, OSX)

- crontab
  - Setup tasks to run in the future
- at
  - Schedule programs to run at certain times

Attacker's Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Covering Tracks and Installing Backdoors

(…Dig in deep)

http://www.JasonDion.com