PowerPreter:
Post Exploitation like a boss

Nikhil Mittal

Get-Host

- Hacker who goes by the handle SamratAshok
- Twitter - @nikhil_mitt
- Blog – http://labofapenetrationtester.blogspot.com
- Creator of Kautilya and Nishang
- Interested in Offensive Information Security, new attack vectors and methodologies to pwn systems.
- Freelance penetration tester ←***hint***
- Spoken at BlackHat, Troopers, PHDays and more

Get-Content

- Need for Post Exploitation
- PowerShell
- Why PowerShell?
- Introducing – Powerpreter
  - Architecture
  - Usage
  - Payloads
  - Capabilities
  - Deployment
- Limitations
- Conclusion

Need for Post Exploitation

- The most important part of a penetration test.
- Guy who will pay you $$$ do not understand technology (neither he wants to). A “shell” is not what he wants from you.
- IMHO, this differentiates a good pen tester and one-click-i-pwn-you-omg pen tester.
- Etc Etc

PowerShell

- A shell and scripting language present by default on new Windows machines.
- Designed to automate things and make life easier for system admins.
- Based on .Net framework and is tightly integrated with Windows.


BY DEFAULT ON WINDOWS?

Why PowerShell?

- Provides access to almost everything in a Windows platform which could be useful for an attacker.
- Easy to learn and really powerful.
- Trusted by the countermeasures and system administrators.
- Consider it bash of Windows.
- Less dependence on *msf* and *<insert_linux_scripting>-to-executable* libraries.

Powerpreter - Introduction

- A post exploitation tool written completely in powershell.
- To be a part of Nishang, powershell based post exploitation framework, written by the speaker.
- The name is similar to meterpreter. Powerpreter wants to be like meterpreter after growing up :)

Powerpreter - Architecture

- Powerpreter is a powershell module and/or script depending on the usage.
- Payloads and features in powerpreter are structured as functions. Separate function for each functionality.
- A bare bones powerpreter is also included which downloads the functionality as and when required.

Powerpreter – Usage

- Powerpreter is best used from a Powershell Remote Session.
- It could be imported as a module and the functionalities get loaded in the current session.
- It could also be used from meterpreter.

Powerpreter – Payloads

- Payloads depend on the privileges available.
- Many useful payloads.
- Better seen in the demo.

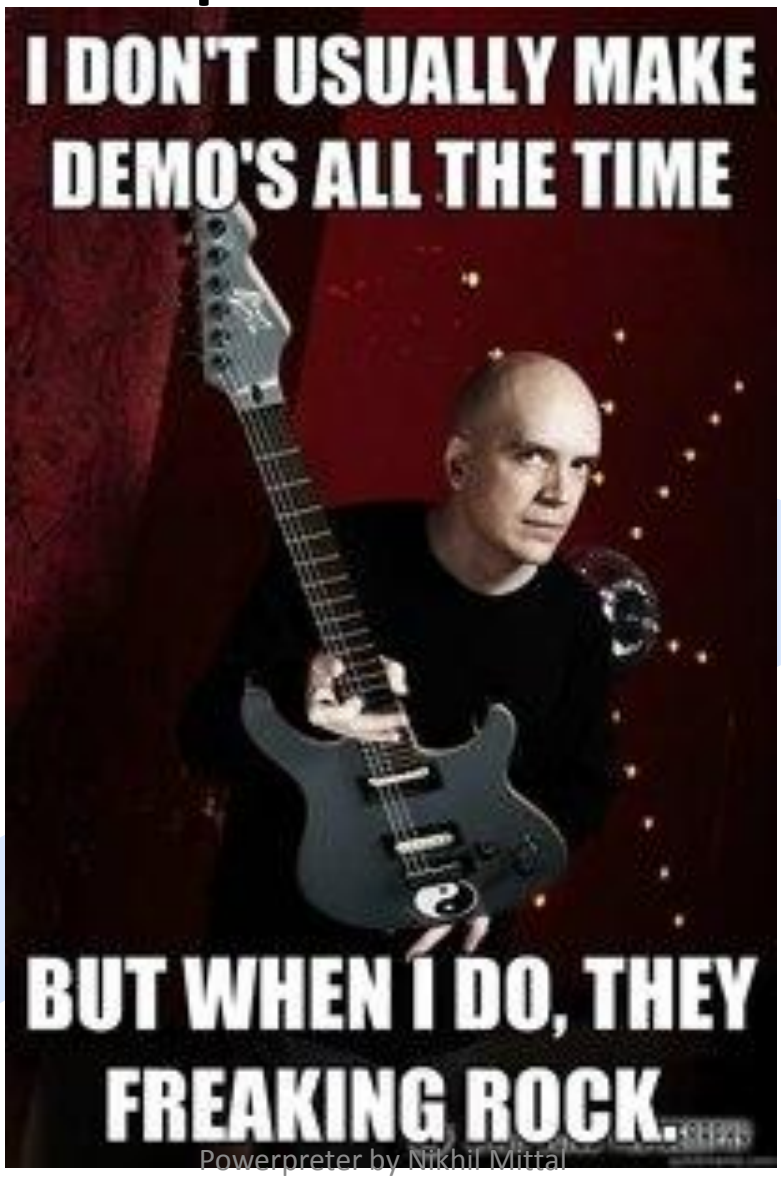
Powerpreter – Capabilities

- Persistence
- Pivoting
- Admin to SYSTEM
- Helper functionalities
- Tampering with logs
- Etc Etc

Powerpreter – Deployment

- From a powershell session
- Using meterpreter.
- Using psexec.
- Drive-by-download
- Human Interface Device (Bare bones preferred)

Powerpreter - DEMO



Limitations

- Yet to undergo community testing.
- Keylogger does not work from powershell remote session.
- Backdoors can be detected with careful traffic analysis.

Conclusion

- Powershell provides much control over a Windows system and Windows based network
- Powerpreter has been designed its power from above fact and provides (or at least attempts to) a useful set of features for penetration testers.

Thanks/Credit/Greetz

- Thanks to my friend Arthur Donkers for helping me to come to Defcon.
- Thanks/Credit/Greetz/Shoutz to powershell hackers (in no particular order)

  @obscuresec, @mattifestation, @Carlos_Perez, @Lee_Holmes, @ScriptingGuys, @BrucePayette, @adamdiscroll, @JosephBialek, @dave_rel1k and all bloggers and book writers.
- Go see another awesome powershell talk in Track- 2 tomorrow – “PowerPwning: Post-Exploiting By Overpowering PowerShell by Joe Bialek“

Thank You

- Questions?
- Insults?
- Feedback?
- Powerpreter would be available at http://code.google.com/p/nishang/
- Follow me @nikhil_mitt
- Latest slides for this preso could be found at:

  http://labofapenetrationtester.blogspot.in/p/blog-page.html