Web Application Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: http://www.securitytube-training.com

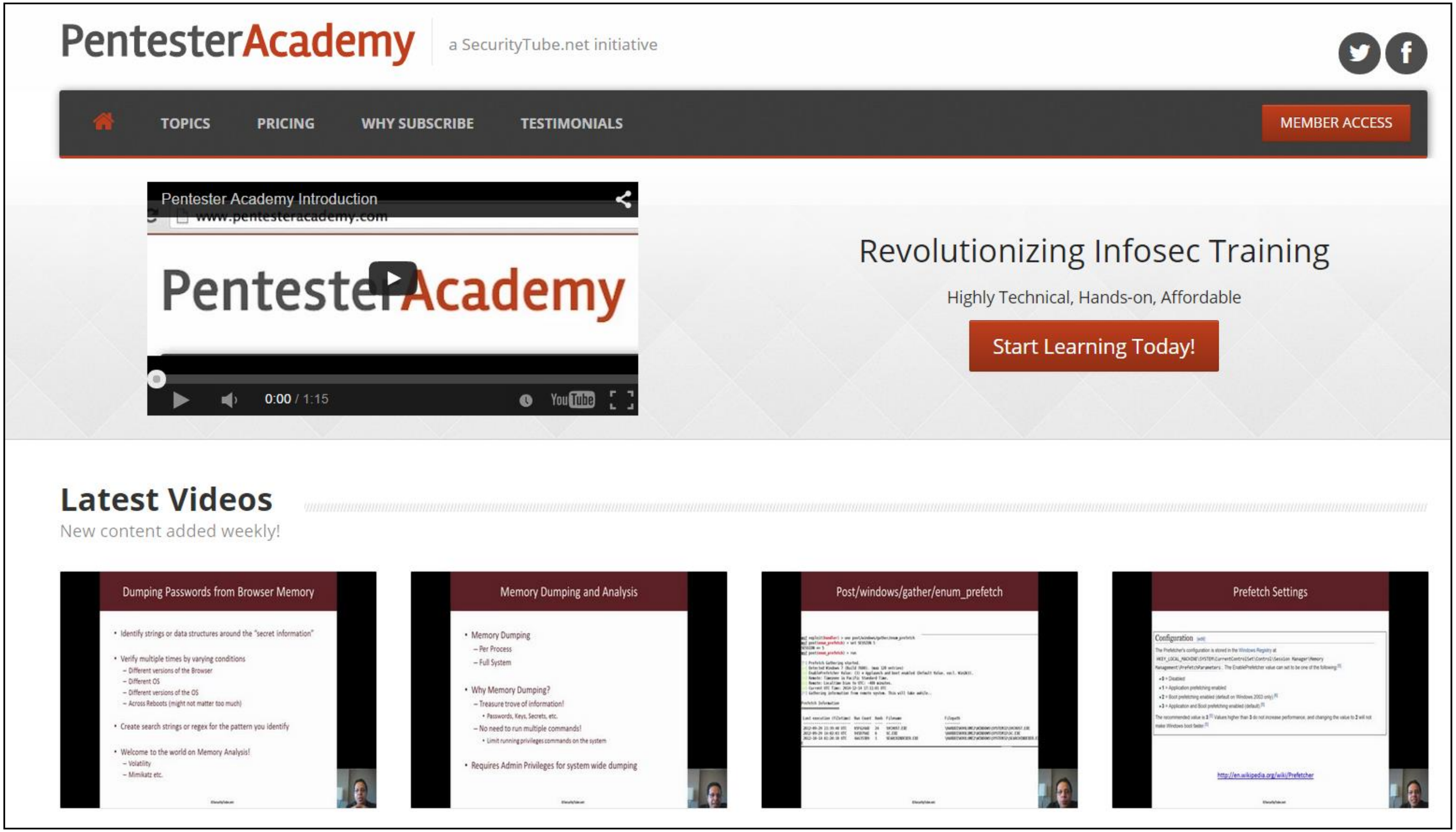
Pentester Academy: http://www.PentesterAcademy.com

Open Redirects: Beating Hashing

Hash Check

- Application creates hash of the URL
- Redirect URL contains both URL and Hash
- Hash is checked on the server side before redirecting

Pentester Academy



Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Latest Videos

New content added weekly!

Dumping Passwords from Browser Memory

- Identify strings or data structures around the "secret information"
- Verify multiple times by varying conditions
  - Different versions of the Browser
  - Different OS
  - Different versions of the OS
  - Across Reboots (might not matter too much)
- Create search strings or regex for the pattern you identify
- Welcome to the world on Memory Analysis!
  - Volatility
  - Mimikatz etc.

Memory Dumping and Analysis

- Memory Dumping
  - Per Process
  - Full System
- Why Memory Dumping?
  - Treasure trove of information!
    - Passwords, Keys, Secrets, etc.
  - No need to run multiple commands!
    - Limit running privileges commands on the system
- Requires Admin Privileges for system wide dumping

Post/windows/gather/enum_prefetch

```
msf exploit(handler) > use post/windows/gather/enum_prefetch
msf post(enum_prefetch) > set SESSION 1
SESSION => 1
msf post(enum_prefetch) > run

[*] Prefetch Gathering started.
[+] Detected Windows 7 (Build 7600). (max 128 entries)
[+] EnablePrefetcher Value: (3) = Applaunch and boot enabled (Default Value, excl. Win2k3).
[+] Remote: Timezone is Pacific Standard Time.
[+] Remote: Localtime bias to UTC: -480 minutes.
[+] Current UTC Time: [illegible]
[*] Gathering information from remote system. This will take awhile..

Prefetch Information
====================

Last execution (filetime)  Run Count  Hash  Filename           Filepath
-------------------------  ---------  ----  --------           --------
[illegible]                [illegible] 24   SVCHOST.EXE        [illegible]
[illegible]                [illegible] 6    SC.EXE             [illegible]
[illegible]                [illegible] 1    SEARCHINDEXER.EXE  [illegible]
```

Prefetch Settings

Configuration [edit]

The Prefetcher's configuration is stored in the Windows Registry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters. The EnablePrefetcher value can set to be one of the following:[1]

- 0 = Disabled
- 1 = Application prefetching enabled
- 2 = Boot prefetching enabled (default on Windows 2003 only)[8]
- 3 = Application and Boot prefetching enabled (default).[8]

The recommended value is 3.[1] Values higher than 3 do not increase performance, and changing the value to 2 will not make Windows boot faster.[1]

http://en.wikipedia.org/wiki/Prefetcher