Network Pentesting

Vivek Ramachandran

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

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

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

Pentesting Windows Endpoints: Tampering the PAC

Proxy Auto Config or PAC

- Used for assigning proxies based on policies
- Very common in Enterprises
- File is written in Javascript and runs within a sandbox

Writing a PAC File

- dnsDomainIs
- shExpMatch
- isInNet
- myIpAddress
- dnsResolve
- isPlainHostName
- localHostOrDomainIs
- isResolvable
- dnsDomainLevels
- weekdayRange
- dateRange
- timeRange
- alert

http://findproxyforurl.com/pac-functions/

Metasploit Post Module

```
msf post(ie_proxypac) > show options

Module options (post/windows/manage/ie_proxypac):

   Name           Current Setting                  Required  Description
   ----           ---------------                  --------  -----------
   AUTO_DETECT    false                            yes       Automatically detect settings.
   DISABLE_PROXY  false                            yes       Disable the proxy server.
   LOCAL_PAC                                       no        Local PAC file.
   REMOTE_PAC     http://192.168.1.10/pac/proxy.pac  no        Remote PAC file. (Ex: http://192.168.1.20/proxy.pac)
   SESSION        1                                yes       The session to run this module on.

msf post(ie_proxypac) >
```

Security Concerns

- Single file controls where the browser goes to fetch URLs
- Can be:
  - Local (overwritten in post exploitation phase)
  - Remote (breaking into server or MITM over network)
- Very popular among malware authors
  - https://www.securelist.com/en/analysis/204792308/PAC_the_Problem_Auto_Config

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

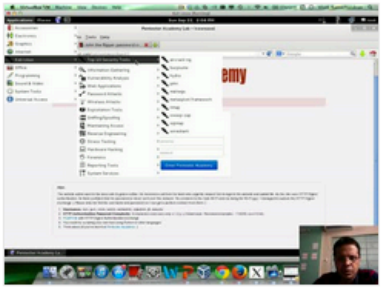
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

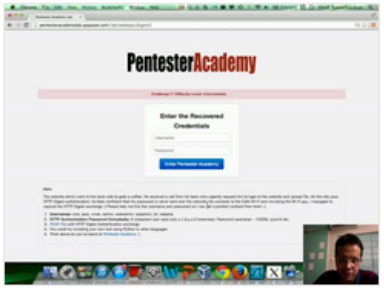
Start Learning Today!

Latest Videos

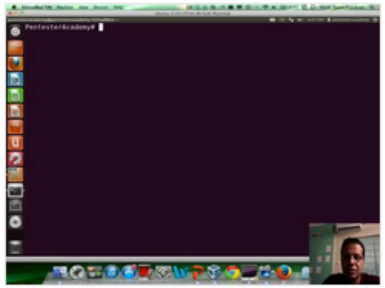
New content added weekly!



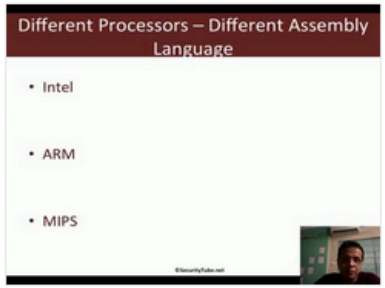
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux