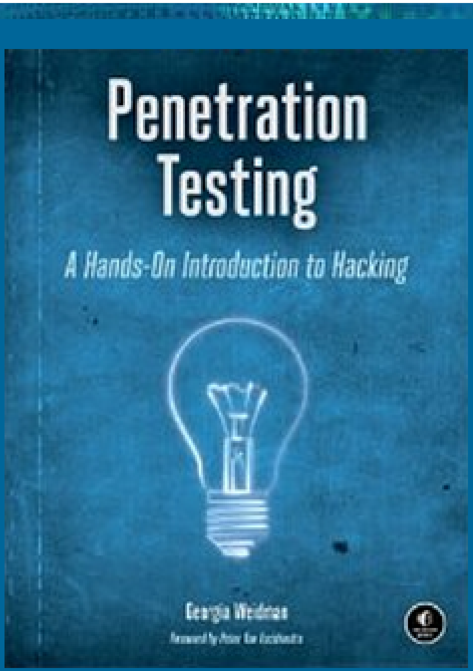


Required book ($25 - $33)

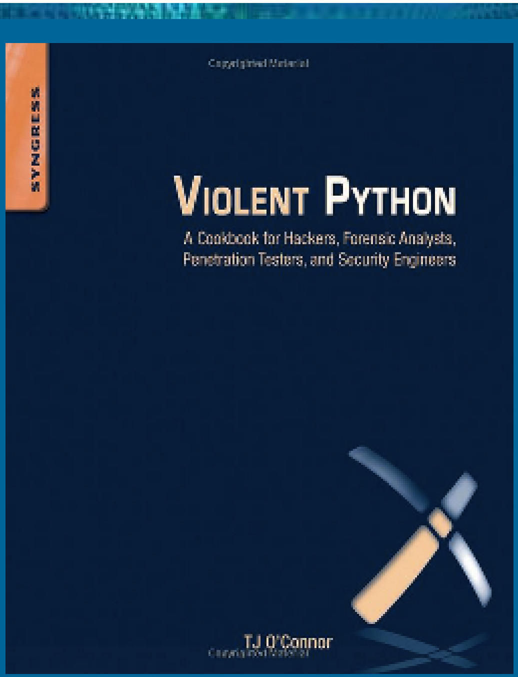
CNIT 124
Advanced Ethical Hacking

Fall 2017 Sam Bowne

Scores

Open Lab Hours for Sci 214

Schedule · Lecture Notes · Projects · Links · Home Page



Optional book ($35)

`CRN 77818 Thu 6:10-9:00 MUB 388`

Catalog Description

Advanced techniques of defeating computer security, and countermeasures to protect Windows and Unix/Linux systems. Hands-on labs include Google hacking, automated footprinting, sophisticated ping and port scans, privilege escalation, attacks against telephone and Voice over Internet Protocol (VoIP) systems, routers, firewalls, wireless devices, Web servers, and Denial of Service attacks.

Prerequisites: CNIT 123.

Upon successful completion of this course, the student will be able to:

A. **Use Google and automated footprinting tools to locate vulnerable Web servers, passwords, open VNC servers, database passwords, and Nessus reports**

B. **Perform sophisticated ping and port scans with several tools, and protect servers from the scans**

C. **Enumerate resources on systems using banner-grabbing and specific attacks against common Windows and Unix/Linux services including FTP, Telnet, HTTP, DNS, and many others, and protect those services**

D. **Use authenticated and unauthenticated attacks to compromise Windows and Unix/Linux systems and install backdoors and remote-control agents on them, and protect the systems from such attacks**

E. **Enter networks through analog phone systems, defeating many authentication techniques, and defend networks from such attacks**

F. **Penetrate PBX, voicemail, Virtual Private Network (VPN), and Voice over Internet Protocol (VoIP) systems, and defend them**

G. **Perform new wireless attacks, including denial-of-service and cracking networks using Wi-Fi Protected Access (WPA) and WPA-2**

H. **Identify firewalls and scan through them**

I. **Perform classical and modern Denial of Service (DoS) attacks, and defend networks from them**

J. **Locate Web server vulnerabilities, exploit them, and cure them**

K. **Describe many ways Internet users are attacked through their browsers and other Internet clients, and the protective measures that can help them**

Student Learning Outcomes (measured to guide course improvements)

Enumerate resources on systems using banner-grabbing and specific attacks against common Windows and Unix/Linux services including FTP, Telnet, HTTP, DNS, and many others, and protect those services
Perform classical and modem Denial of Service (DoS) attacks, and defend networks from them
Locate Web server vulnerabilities, exploit them, and cure them

Textbook

Penetration Testing: A Hands-On Introduction to Hacking **by Georgia Weidman -- ISBN-10: 1593275641, No Starch Press; 1 edition (June 8, 2014)**
Buy from Amazon

Quizzes

The quizzes are multiple-choice, online, and open-book. However, you may not ask other people to help you during the quizzes. You will need to study the textbook chapter before the lecture covering it, and take the quiz before that class. Each quiz is available for one week, up 30 minutes before class. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts. If you take the quiz twice, the higher score counts.

To take quizzes, first claim your RAM ID and then log in to Canvas here:

https://ccsf.instructure.com

Live Streaming

Live stream at: ccsf.edu/webcasts

Classes will also be recorded and published on YouTube for later viewing.

Live Streaming for Kahoots

During the Kahoots, I'll also stream the class via Zoom.

Join from PC, Mac, Linux, iOS or Android: https://zoom.us/j/4108472927
Meeting ID: 410-847-2927

Schedule (may be revised)

Date	Quiz	Topic
Thu 8-24		Demo: Projects 1, 1x, 2, 2x, 3, and 8x

```
GNU nano 2.7.4                    File: grab.py

import socket
s = socket.socket()

s.connect(("attackdirect.samsclass.info", 22))
print s.recv(1024)
s.close()

                 [ Color syntax highlighting disabled ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Linter
```

Thu 8-31	**Ch 2: Using Kali Linux**

CNIT 124 - Advanced Ethical Hacking, Au...
Watch later
Share
CNIT 124 - Advanced Ethical Hacking
Instructor - Sam Bowne
Distance Learning Classroom
eatv

Thu 9-7	**Ch 3: Programming**

Fri 9-8	*Last Day to Add Classes*	
Thu 9-14		**Ch 4: Using the Metasploit Framework**

Thu 9-21	Quizzes Ch 2 & 5 due* Proj 1-3 due	Ch 5: Information Gathering

Thu 9-28	Quizzes Ch 3 & 6 due* Proj 4 & 5 due	Ch 6: Finding Vulnerabilities

Thu 10-5	Quizzes Ch 4 & 7 due* Proj 7 due	Ch 7: Capturing Traffic

CNIT 124 - Advanced Ethical Hacking, Oc...
Watch later
Share
CNIT 124 - Advanced Ethical Hacking
Instructor - Sam Bowne
Distance Learning Classroom
eatv

Thu 10-12	**Quiz Ch 8 due*** **Proj 8 due**	**Ch 8: Exploitation**

eatv
CNIT 124 - Advanced Ethical Hacking, Oc...
Watch later
Share
acer
CITY COLLEGE OF SAN FRANCISCO
CNIT 124 - Advanced Ethical Hacking
October 12, 2017
Distance Learning Classroom
eatv

Thu 10-19	**Quiz Ch 9 due*** **Proj 6 & 9 due**	**Ch 9: Password Attacks**

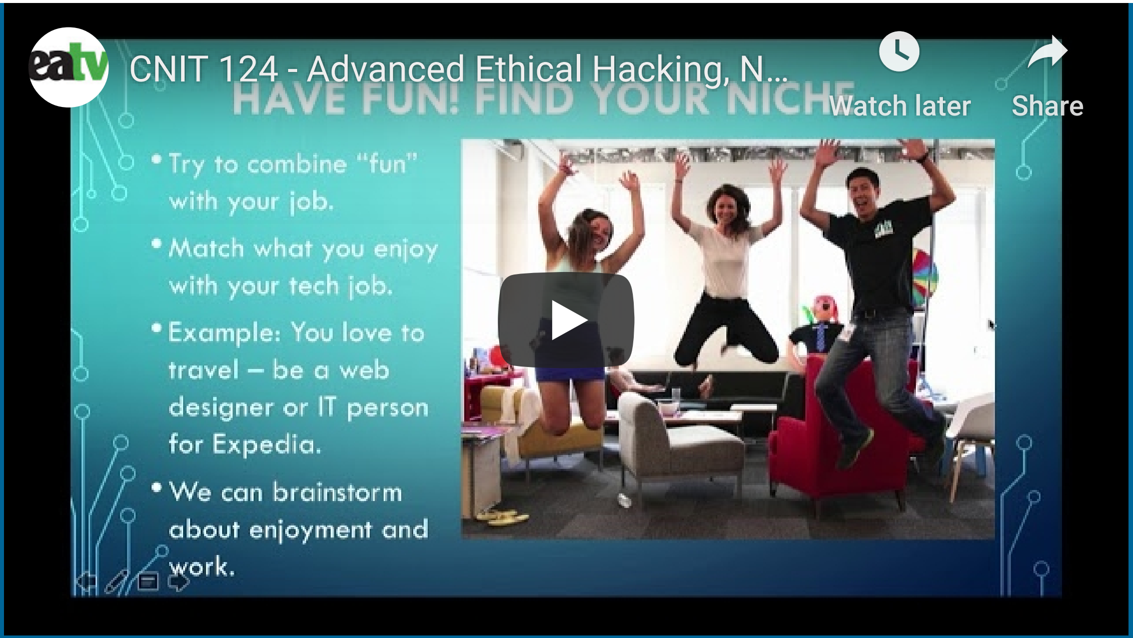
Thu 10-26	Quiz Ch 10-12 due* Proj 10 & 11 due	Ch 10: Client-Side Exploitation Ch 11: Social Engineering Ch 12: Bypassing Antivirus Applications

Thu 11-2	*Class Cancelled for the National CPTC in Rochester, NY*	
Thu 11-9	Quiz Ch 13 (Part 1) due* Proj 12 & 13 due	Ch 13: Post Exploitation (Part 1)

Thu 11-16	No Proj No Quiz due	Guest: Nate Lindstrom "Amazon AWS Technology Secrets"	

eatv
CNIT 124 - Advanced Ethical Hacking, N...
Watch later
Share
Bake your credential files into your AMI; keep them out of your code repo

Thu 11-23	*Holiday - No Class*	
Thu 11-30	**Quiz Ch 13 (Part 2) due*** **Proj 14 & 15 due**	**Job-Hunting and Resume Tips**



CNIT 124 - Advanced Ethical Hacking, N...

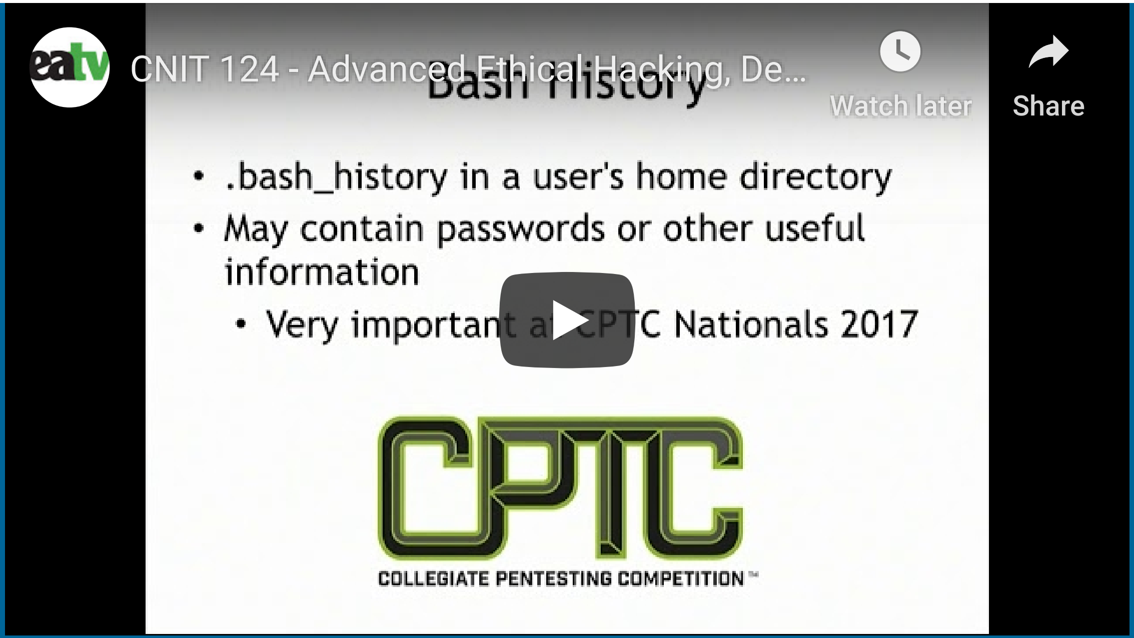
Watch later

Share

HAVE FUN! FIND YOUR NICHE

- Try to combine "fun" with your job.
- Match what you enjoy with your tech job.
- Example: You love to travel – be a web designer or IT person for Expedia.
- We can brainstorm about enjoyment and work.

Thu 12-7	No Quiz Proj 16 & 17 due	Ch 13: Post Exploitation (Part 2) & CCDC Training


CNIT 124 - Advanced Ethical Hacking, De...
Watch later
Share
CPTC
COLLEGIATE PENTESTING COMPETITION™

Bash History

- .bash_history in a user's home directory
- May contain passwords or other useful information
  - Very important at CPTC Nationals 2017

Thu 12-14	**No Quiz** **All extra credit projects due**	**Last Class: Open Lab in S214, no lecture**
Fri 12-15 - **Thu 12-21**	**Final Exam available online throughout the week.** **You can only take it once.**	

Lectures

[Policy](#) · [Schedule](#)

Ch 2: Using Kali Linux
Ch 3: Programming
Ch 4: Using the Metasploit Framework
Ch 5: Information Gathering · PDF · KEY
Ch 6: Finding Vulnerabilities and Exploiting Domains · PDF · KEY
Ch 7: Capturing Traffic · PDF · KEY
Ch 8: Exploitation · PDF · KEY
Ch 9: Password Attacks · PDF · KEY
Ch 10: Client-Side Exploitation
Ch 11: Social Engineering
Ch 12: Bypassing Antivirus Applications · PDF · KEY
Ch 13: Post Exploitation Part 1 · PDF · KEY

Ch 13: Post Exploitation Part 2 (pptx)

Projects

Download VMware Player
Download metasploitable **Size: 865,084,584**
SHA-256: 2ae8788e95273eee87bd379a250d86ec52f286fa7fe84773a3a8f6524085a1ff
Download Win2008-124 **Size: 2,180,234,212**
SHA-256: dc496623ef74fe1dac1dfb3053acea312350f02d83189bd15d2b48d6eb49be22
Download Kali Linux 32 bit VM PAE

Installing Python on Windows

Microsoft Evaluation Software

Proj 1: Basic Port Scanning with Python (15 pts.)
Proj 2: HTTP Requests with Python (15 pts.)
Proj 3: Setting Up VMs (15 pts.)
Proj 4: Metasploit v. Windows (15 pts.)

Proj 5: Enumerating Metasploitable (15 pts.)
Proj 6: Metasploit v. Linux (15 pts.)
Proj 7: Password Hashes with Python (15 pts.)
Proj 8: Nessus (15 pts.) (Updated 8-15-17)
Proj 9: Nmap Scripts, Metasploit Scanner Modules, and Nikto (15 pts.)

Do One Of These Two Projects

Proj 10: Hacking a PPTP VPN with Asleap (25 pts.) (rev. 10-19-17)

Proj 10a: Hacking a PPTP VPN with Asleap (25 pts.) (rev. 10-25-17 to use only 2 VMs)

Proj 11: Exploiting Win2008-124 and Metasploitable (20 pts.)
Proj 12: Exploiting PHP Vulnerabilities (15 pts.)
Proj 13: XOR Encryption in Python (10 pts.)
Proj 14: Attacking Internet Explorer and Migrating (10 pts.)
Proj 15: Stealing Passwords from RAM with Metasploit (10 pts.)
Proj 16: BeEF (10 pts.) (rev. 9-5-17)
Proj 17: Slowloris in Python (10 pts. + 10 pts. extra credit)

Extra Credit Projects

Proj 1x: Port Scanning Challenges (15 pts. extra credit)
Proj 2x: HTTP Login Challenges (35 pts. extra credit)
Proj 3x: CodeCademy Python Lessons (45 pts.)
Proj 4x: Wechall.net (points vary)
Proj 5x: Simple Programming (15 pts. extra credit)
Proj 6x: CodeCademy Command Line Course (15 pts.)
Proj 7x: Password Hashing Challenges (40 pts. extra credit)
Proj 8x: ETERNALBLUE v. Windows (10 pts. extra credit)
Proj 9x: Exploiting Apache Struts with CVE-2017-5638 (15 pts. extra credit)
Proj 10x: Exploiting Apache Struts with CVE-2017-9805 (10 pts. extra credit)

Proj 13x: XOR Encryption Challenges (40 pts. extra credit)
Proj 14x: Pass The Hash (10 pts. extra credit)
Proj 15x: ETERNALROMANCE (15 pts. extra credit)

Exploiting Domains

Proj 11x: Making a Domain Controller (20 pts. extra credit)
Proj 12x: Member Server and Group Policy (20 pts. extra credit)
Proj 16x: ETERNALROMANCE v. 2012 Member Server (20 pts. extra credit)
Proj 17x: Pivoting and Exploiting a Domain Controller (20 pts. extra credit)

Proj 18x: Privilege Escalation in Metasploitable (15 pts. extra credit)
Proj 19x: Pen Test a Host (Up to 50 pts. extra credit)

Proj 20x: Independent Project (pts. vary) -- Do something cool and show it to the class!

Proj 21x: PicoCTF (Up to 40 pts.)

Links

CEH Certification Resources

CEH Tips
CEH: Certified Ethical Hacker - Taking the Exam
CEH: Practice Exams

CEH: TechExams -- Certified Ethical Hacker (CEH) exam
EC-Council - Certified Ethical Hacker (312-50) Practice Exam - This is the one I used

Links for Chapter Lectures

Ch 4a: Metasploit Module Search Page
Ch 4b: How to get started with writing an exploit for Metasploit
Ch 4c: Msfconsole one-liner example
Ch 4d: Scanner HTTP Auxiliary Modules - Metasploit Unleashed
Ch 4e: Metasploit: The New Metasploit Browser Autopwn:...
Ch 4f: Simple Take Over of Windows Server 2008 via ms09-050

Ch 5a: DNS Request Types
Ch 5b: 10 Linux DIG Command Examples for DNS Lookup
Ch 5c: Open Resolver Project
Ch 5d: Public DNS Server List
Ch 5e: DNS AXFR scan data
Ch 5f: DNS Hacking (Beginner to Advanced) - InfoSec Resources
Ch 5g Wildcard DNS record - Wikipedia
Ch 5h: Network tools for every sys admin
Ch 5i: The Strange History of Port 0

Ch 7a: HowToDecrypt802.11 - The Wireshark Wiki
Ch 7b: security - WEP/WPA/WPA2 and wifi sniffing - Server Fault
Ch 7c: Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)
Ch 7d: Details of Key Derivation for WPA

Ch 8a: An Improved Reflective DLL Injection Technique
Ch 8b: DLL injection - Wikipedia
Ch 8c: Windows DLL Injection Basics--Clear Explanation with Good Figures
Ch 8d: stephenfewer/ReflectiveDLLInjection -- Code from 2013
Ch 8e: Using Cadaver as a WebDAV Client
Ch 8f: WebDAV - Wikipedia
Ch 8g: helper: webdav xampp (= 1.7.3 default credentials
Ch 8h: How To Install and Secure phpMyAdmin on Ubuntu 14.04
Ch 8i: Docker Internals - Google Slides
Ch 8j: Docker: Understand the architecture

Ch 8k: Docker vs Virtualization

Ch 8l: UnionFS - Wikipedia

Ch 8m: Docker Hub

Ch 8o: Docker Container Breakout Proof-of-Concept Exploit | Docker Blog

Ch 8p: The Docker exploit and the security of containers | Xen Project Blog

Ch 8q: Docker breakout: brute-forcing a 32-bit number!

Ch 8r: Docker security

Ch 8s: Docker Addresses More Security Issues and Outlines "Pluggable" Approach

Ch 8t: Dump Windows password hashes efficiently

Ch 8u: Recovering Windows 7 Registry Hives/Files

Ch 8v: How To Install Bkhive on Kali 2

Ch 8w: Transferring files from Kali to Windows (post exploitation)

Ch 9a: Yahoo Mail eliminates passwords as part of a major redesign (Oct., 2015)

Ch 9b: Teen says he hacked CIA director\'s AOL account (Oct., 2015)

Ch 9c: Packetstorm Wordlists for password cracking

Ch 9d: Openwall wordlists collection for password recovery, password cracking, and password strength checking

Ch 9e: Why passwords have never been weakerand crackers have never been stronger (2012)

Ch 9f: "thereisnofatebutwhatÂwemake"Turbo-charged cracking comes to long passwords (2013)

Ch 9g: Cracking 16 Character Strong passwords in less than an hour (2013)

Ch 9h: How the Bible and YouTube are fueling the next frontier of password cracking (2013)

Ch 10a: Adobe Reader Metasploit Modules

Ch 10b: CCSF Application Form (pdf)

Ch 10b: CCSF Application (pdf, can be poisoned with Metasploit)

Ch 11a: Update Social Engineering Toolkit on Kali Linux - YouTube

Ch 12a: Notepad Plus Plus Download

Ch 12b: VirusTotal - Free Online Virus, Malware and URL Scanner

Ch 12c: How to Evade AV Detection with Veil-Evasion

Ch 13a: Post-Mortem of a Metasploit Framework Bug

Ch 13b: Post Exploitation Using NetNTLM Downgrade Attacks

Ch 13c: Mount shadow volumes on disk images - ForensicsWiki

Ch 13d Shell is coming ...: Metasploit: Getting outbound filtering rules by tracerouting

Ch 13e: 5 Step To Capture Windows User Login Using Metasploit Keylogger

Ch 13f: Windows Capture Winlogon Lockout Credential Keylogger | Rapid7

Ch 13g: Metasploit: Capturing Windows Logons with Smartlocker
Ch 13h: Windows 8.1 stops pass-the-hash attacks
Ch 13i: Pass-the-Hash is Dead: Long Live Pass-the-Hash
Ch 13j: Using claims-based access control for compliance and information governance (2011)
Ch 13k: Windows Internals - showing token structure
Ch 13l: Access token stealing
Ch 13m: Access Tokens (Windows)
Ch 13n: What's in a Token (Part 2): Impersonation - TechNet Blogs
Ch 13o: Fun with Incognito - Metasploit Unleashed
Ch 13s: PSExec Demystified
Ch 13t: 4 Ways to Capture NTLM Hashes in Network
Ch 13p: Excellent explanation of NTLMv2
Ch 13q: NTLMv2 cracking speed estimates
Ch 13r: Fast Introduction to SOCKS Proxy - EtherealMind
Ch 15a: HowToDecrypt802.11 - The Wireshark Wiki
Ch 15b: WPA 4-way handshake - Wireshark Q&A

Miscellaneous Links

Learn Python the Hard Way
Fuzzing for SQL injection with Burp Suite Intruder - USE FOR PROJECTS
Pythonista on the App Store on iTunes -- INTERESTING FOR PROJECTS
Pythonista: Using pipista to install modules
How to Build a DNS Packet Sniffer with Scapy and Python
Bypassing Antivirus with Shellter 4.0 on Kali Linux -- GOOD 124 PROJECT
Online JavaScript beautifier -- deobfuscates code! -- IMPORTANT FOR MALWARE ANALYSIS
Android Security: Adding Tampering Detection to Your App

Old Links

PwnWiki.io -- USEFUL RED TEAM TIPS
Hacking Secret Ciphers With Python (Free E-Book)
Introduction to Cryptography Video Lessons by Christof Paar - YouTube
Cryptography Textbook Slides
RSA is 100x slower than AES (figures 9-13)
How to Create a Bootable Ubuntu USB Drive, for Mac, in OS X

EDB (Evan's Debugger) Alternatives and Similar Software - AlternativeTo.net
How to install 32 bit software on a 64 bit Kali Linux system
How to Reverse Engineering with Radare2 -- INTERESTING FOR PROJECTS
OSCP study material : Georgia Weidman's book recommended
A book for those interested in PWK/OSCP -- Georgia Weidman's book recommended
Scapy Documents
Metasploitable 2 Exploitability Guide | Rapid7
Metasploitable 2 enumeration - Hacking Tutorials
Metasploitable 2 vulnerability assessment - Hacking Tutorials
Running Metasploitable2 on VirtualBox
The Kali Linux Certified Professional | Kali Linux
Monitor Apache Web Server Using Mod_status -- WORKS ON UBUNTU
Understanding Python's "with" statement
PSExec for Lateral Movement
Unable to Contact IP Driver, error code 5 Windows 2008 Server hosted on Vmware
How to Make a Domain User the Local Administrator for all PCs
Post-Exploitation in Windows: From Local Admin To Domain Admin (efficiently) | pentestmonkey
Pass-the-hash attacks: Tools and Mitigation (2010)
PSExec Pass the Hash - Metasploit Unleashed
How to download a file using windows command line
mouse pointer is offset up and to the left -- VMware Communities -- USEFUL TROUBLESHOOTING
The "SYSTEM" challenge -- Decoder's Blog
Attack Methods for Gaining Domain Admin Rights in Active Directory
Penetration Testing in Active Directory using Metasploit (Part 2)
Attack Simulation: from No Access to Domain Admin
Exploit MS17-010 vulnerability on Windows Server 2012/2016 using Metasploit and TheFatRat - YouTube
HOW TO EXPLOIT ETERNALROMANCE/SYNERGY TO GET A METERPRETER SESSION ON WINDOWS SERVER 2016
Eternalromance: Exploiting Windows Server 2003 - Hacking Tutorials
Network access: Named Pipes that can be accessed anonymously
A Red Teamer's guide to pivoting
Privilege Escalation - Metasploit Unleashed
VMware Fix: Windows cannot find the Microsoft Software License Terms
Meter your Ethernet connection in Windows 10
Metasploit: Module database cache not built yet, using slow search -- HANDY FIX
RDP hijackingâ€Šâ€"â€Šhow to hijack RDS and RemoteApp sessions transparently to move through an organisation
Pwning with Responder - USE IN PROJECT
Gladius: Automatic Responder Cracking

Seeing the unseen characters with cat!
How to see hidden characters..... | Unix
Metasploit privilege escalation with udev
virtual machine - Guest OS resolution (text too small) in vmware workstation 12 player
metasploit - How do you send a 64 bit meterpreter stager?
Locating Those Nasty Passwords in Group Policy Preferences Using PowerShell
Ubuntu Apache Default MaxKeepAliveRequests is 100
Enable SSH on Kali Linux Enable SSH on Kali Linux -- Doctor Chaos
The Easiest Metasploit Guide Youâ€™ll Ever Read -- MANY GOOD PROJECTS HERE
Transferring files from Kali to Windows (post exploitation)
Top Five Ways I Got Domain Admin on Your Internal Network before Lunch (2018 Edition)--GOOD FOR PROJECTS AND OSCP
My First Go with BloodHound
Windows Password Hashes: LM, NTLM, Net-NTLMv2, oh my!
RPC_ENUM - RID Cycling Attack - TrustedSec -- Recommended by @J0hnnyXm4s
CrackMapExec: post-exploitation for large Active Directory networks -- Recommended by @J0hnnyXm4s
InitString / evil-ssdp Spoof SSDP replies to phish for credentials and NetNTLM challenge/response
Seth: Perform a MitM attack and extract clear text credentials from RDP connections
Multiple Ways to Get root through Writable File
Setup of AD Penetration Lab
ifconfig - How can I display eth0's IP address at the login screen on Precise Server? - Ask Ubuntu
Privilege Escalation & Post-Exploitation Resources -- VERY USEFUL
Multiple Ways to Bypass UAC using Metasploit
Passing OSCP
OSCP Journey: Exam & Lab Prep Tips
ntroducing the Metasploit Vulnerable Service Emulator
Installing Python 3 on Mac OS X -- The Hitchhiker's Guide to Python
Pipenv & Virtual Environments -- The Hitchhiker's Guide to Python
SSH on Kali

New Unsorted Links

Ch 5j: Zone Transfer Test Online | HackerTarget.com
When target machine dont have "nc" installed ? Don't forget there is "Whois"
Malware writing - Python malware
The Journey to Try Harder: TJnull's Preparation Guide for PWK/OSCP
Modifying Empire to Evade Windows Defender :: Mike Gualtieri

Transferring files from Kali to Windows (post exploitation)--VERY USEFUL
Ricochet Security Assessment Public Report
public-pentesting-reports

Last Updated: 12-8-17 3 pm