* Introduction
* How Protected Do You Feel?
* Overview of the CEH Certifica…
* What Certification Brings You
* Should I Watch This Series
* What’s Expected of You
* Review the CCA
* Overview How to Build a Lab t…
  + Don’t try on production network
  + Host Machine
    - Hyper-V
    - VMware
    - VirtualBox
  + Windows 8.1 Enterprise/server 2012R2
  + 16GB RAM
  + 50GB hard drive
  + 1 NIC(network interface card)
  + Virtual Machines
    - Windows 8.1 box
    - Windows 7
    - Window servers 2008/2012
    - Linux(BackTrack/Kali)
  + Configure your virtual environment
    - Private LAN
  + Download
    - Install from DVD/ISOs/thumbdrive
* The Host Machine
  + Go to TechNet evaluation center website
  + Login
  + Click on ‘Evaulate now’
  + Download the windows server 2012 R2
  + Download windows 8.1 enterprise
  + Download windows server 2008 R2
  + Download windows 7 SP1 with IE9
  + Download kali
* Installing The Host Machine
  + install windows server 2012 R2 with GUI
    - do custom install
* Installing Hyper-V on Your Host
  + add role or feature
  + choose role based installation
  + click Hyper-V
  + add features
* Configure Hyper-V Networks
  + select a private virtual switch
* Using VMWare
  + VMWorkstation 14 Pro
  + change network adapter to custom network
* Summary
* Introduction
* Virtual Machine: Server 2012R2
  + install OS with ISO
  + select the GUI
  + do custom install
  + turn on DEP in performance tab
  + do role based installation
    - Web server(IIS)
    - BITS
    - BitLocker Network
    - BanchCache
    - Client for NFS
    - Data Center Bridging
    - Direct Play
    - Enhanced Storage
    - Failover Clustering
    - Group Policy Management
    - Ink and Handwriting Services
    - Internet Printing Client
  + Add roles and features
    - Install SNMP Service
    - Set up community rights as READ ONLY
    - Accept SNMP packets from any host
* Virtual Machine: Server 2008R2
  + Do full installation
  + Turn on internet explorer enhanced security configuration
* Summary
* Introduction
* Virtual Machine: Windows 8.1
* Virtual Machine: Windows 7
  + Delete program ‘Virtual PC Integration Component’
* Virtual Machine: Kali
  + install generation 1
* Virtual Machine: Housekeeping
* Summary
* Information Security Overview
* Hacking vs Ethical Hacking
  + hacking
    - tacking an object and make them do something they weren’t design to do
* Fundamentals of Information …
  + authenticity
    - user is who they are
  + Integrity
    - where data is stored is valid
  + Availability
    - user cant get to their data
    - DOS is design to refuse availability
  + Confidentiality
    - customer data confidentiality
  + Non repudiation
    - no modifying data without accountability
* Speak like a Hacker
  + Exploit
    - way of curcumvaitng security
  + Hack Value
    - value hacker associated with a system
    - which system is more advantageous to get into
  + Vulnerability
    - weakness in design or implementation of the system
  + Target of Evaluation
    - system the hacker has identified that requires a security evaluation
  + Zero-day Attack
    - attack an hacker can issue against a target where there has been no patch or fix
  + Daisy-chaining
    - compromise a system and use the system to attack other system
    - hiding your attack
* The Technology triangle
  + Usability
    - Gui
  + Security
    - Restrictions
  + Functionality
    - Features
* Summary
* Overview of Threats and Attac.
* Threats: Hosts
  + Foot printing thread
    - Every computer/system responds a specific way
  + Physical Security
  + Passwords
    - Length is better than special characters
  + Malware
  + Denial of Service
  + Unauthorized Access
  + Privilege Escalation
  + Back Doors
* Threats: Natural & Physical
  + Earthquakes
  + Hurricanes
  + Floods
  + Natural Disasters
  + Theft
  + Impact
  + Power
  + End of Life
    - Decommission
* Threats: Applications
  + Configuration
  + Buffer Overflow
  + Lazy Coding
  + Data/Input Validation
* Threats: Human
  + Malicious Employees
  + Lack of Training
  + Social Networking
  + Hackers
* Threats: Networks
  + Sniffing/Eavesdropping
  + ARP Poisoning
    - Address resolution protocol(ARP)
    - ARP in charge or resolving IP address to MAC address
  + DoS
  + Spoofing
    - Send data across network that make it seems like it came from another computer
* Threats: Where Do They Come..
  + External
* Attack Vectors
  + VM & Cloud environments
  + Unpatched OS/software
  + Social networking
  + Internal users
  + Hackivism - hacking for a cause
  + Malware
  + Botnets
  + Security staffing
  + Lack of security policies
  + Compliance with regulations/laws
  + Complexity of network infrastructure
  + Mobile devices
  + Ransomware
  + Advanced Persistent Threats
  + Phishing
  + Web Applications
  + IoT(internet of things)
* IPv6 Issues
  + Auto configuration
  + Incompatibility of logging systems
  + Default activation
  + Shortcuts
  + Bigger headers
  + 4to6 translation
  + Multiple IP’s per device
  + Network discovery
* Summary of Threats and Attac…
* Overview of Hacking Concepts
* Hacking Defined
  + Exploiting a systems vulnerabilities and security controls to gain access to system resources and features outside the creator’s original purpose
* History of Hacking: In the Begi..
* History of Hacking: Currently
* Ethical Hacking Defined
  + involves the use of hacking methods and tools to discover weaknesses for system security
  + skills an ethical hacker have
    - expert with programs and networks
    - proficient with vulnerability research
    - mastery with diverse hacking techniques
    - follow a strict code of conduct
* What Skills Should an Ethical…
  + Explicit Permissions in Writing
  + Use the Same Tactics & Strategies
  + No means NO!
  + Report All of Your Results
* Type of Pen Tests
  + Black Box
    - knowing nothing about the system
  + Gray Box
    - knowing some info about the system(ip address, os, etc)
  + White Box
    - knowing everything about the system
* Why a Hacker Hacks
  + Hobby
  + Illegal Activities
  + Malicious Intent
  + Gain Knowledge
* Types of Hackers
  + Black Hats
    - individual that does attack on system they don’t have privilege
    - they are typically breaking the law
  + White Hats
    - good guys
    - have permission to hack system
  + Gray Hats
    - black hat hackers that have been reformed
    - may be black hat one moment then white the next
  + Suicide Hackers
    - hacker that don’t care if they get caught
    - don’t cover their tracks
    - only care about doing the attack
  + Script Kiddies
    - no skills, basic things
    - use tools that walk them through
  + Spy Hackers / Cyber Terrorists /state sponsored hackers
    - malicious
  + Hacktivism
    - drive: political, social, ideology, vandalism, protest, humiliate
    - Political Agenda: defacing or disabling websites
    - Targets: government agencies, multinational corps
* How Does Hacking Influence ...
  + 1 Trillion a dollars a year companies spend
  + customer private information
  + intellectual property
  + down time / slow site
  + loss of revenues
  + financial information
  + reputation
  + loss of business
* Summary of Hacking Concepts
* Overview Hacking Phases
  + the most secure system is the one that is never built
* The Phases
  + Reconnaissance
  + Scanning
  + Gaining access
  + Maintaining access
  + Clearing tracks
* Phase 1 Reconnaissance
  + Passive
    - No direct interaction with a target
  + Active
    - Direct interaction with the target
* Phase 2 Scanning
  + Gather info
    - ID systems
    - Vulnerabilities
  + Tools Used
    - Port scanners
    - Vulnerability scanners
* Phase 3 Gaining Access
  + Path
    - Network
    - OS
    - Application
* Phase 4 Maintain Access
  + PWNing the system
  + Use system as a launch pad
  + Inject backdoor/Trojans
    - Used to revisit
    - Used to sniff/monitor network
  + Use resources
  + Harden up
    - So that other attackers can’t use the same system
* Phase 5 Clearing Tracks
  + Destroy proof
    - Instead of deleting logs, delete your specific entries
  + Hide my stuff
    - Rootkit
    - Hide things in audio files, images etc
  + Cyber blind
* Summary of Hacking Phases
* Overview of Attack Types
  + Application attacks
  + Misconfiguration attacks
  + Shrink-wrap code attacks
  + O/S attacks
  + Entry points
* Application Attacks
  + Causes
    - Time
    - Features
    - QA
    - Add-on
  + Results
    - Buffer overflows
    - Cross-site scripting
    - Active content
    - DoS and SYN
    - SQL Injection
  + Other App Attacks
    - Session hijacking
    - Man in the Middle
    - Directory traversal
* Misconfiguration Attacks
  + Targets
    - Web servers
    - Application platforms
    - Frameworks
    - Databases
    - Hardware
* Shrink-wrap Code Attacks
  + Lazy developers take short cuts
    - Copy and paste code
  + Fine tune scripts they reuse
  + Built-in scripts
* O/S Attacks
  + gaining access via vulnerabilities
  + O/S vulnerabilities via defaults
  + O/S attacks via non-updated systems
* Entry Points for an Attack
  + Remote Network
  + Dial-up Network
  + Local Network
  + Stolen Equipment
  + Social Engineering
  + Physical Entry
* Summary of Attack Types
* Overview of Information Secur…
  + Necessity of Ethical Hacking
  + What skills you must have
  + Multi-layered defense
  + Incident management
  + Security policies
  + Vulnerability research
  + Data leakage
  + The role of AI(artificial intelligence)/ ML(machine learning)
  + Penetration testing(pen testing)
* Necessity of Ethical Hacking
  + Rapid Growth in Tech = Trouble
  + What ethical hackers do for companies
    - review systems and infrastructure
    - test current security
    - create solution
    - retest
  + You have to answer questions
    - what can be seen
    - what is being monitored
    - what can be done
    - is there adequate protection
    - are compliances met
* What Skills You Must Have
  + O/S knowledge
  + Security awareness
  + computer professional
  + network guru
  + management skills
  + patience
  + software knowledge
  + a lot of sherlock holmes
* Multi-layered Defense
  + Policies, processes and awareness
  + physical
  + perimeter
  + network
  + host
  + application
  + data
* Incident Management
  + identify issues
  + analyze
  + prioritize
  + resolve
  + why incident management
    - meet availability
    - reduces impact
    - better service quality
    - more efficient and productive
    - customer/user satisfaction
    - pro-active
* IM Process
  + prepare for event handling and reaction
  + detection & examination
  + sorting and ranking
  + notification
  + containment
  + forensic examination
  + purge and recovery
  + post incident actions
* Data Leakage
  + unauthorized access to data
  + major risks to your organization
  + insider and external threats
  + DLP(Data Loss Prevention)
    - looks at the data
    - looks at the rules
    - determines what can be done
  + Back ups
    - ID the data
    - select the technology
    - choosing RAID(Redundant Array of Independent Disks)
    - choose a method
      * hot: system is continually performing backup
      * cold: offline backup when system isn’t working
      * warm: system receives periodic updates
    - location
      * onsite
      * offsite
      * cloud
    - choose the type of backup
      * full: backup everything
      * incremental: all data since last backup
      * differential: backup changes since last full backup
  + don’t ever assume it works! Validate your process
* Artificial Intelligence and Mac…