HackitTech

HACKING SOCIETY

BestEthicalHackingNotes

INTRODUCTION

HackitTech

Module 1

I want to thank you and congratulate you for downloading the Notes, "HackingSociety:Bewheretheworldisgoing."

WhatisHacking

• Hackingreferstoexploitingsystemvulnerabilitiesandcompromisingsecurity controlstogainunauthorizedaccesstothe system.

Eg:-Stealing,disclosureofSensitiveinformation

WhyHackHappens?

• ATTACKS=MOTIVE(GOAL)+METHOD+VULNERABILITY

• MOTIVE: - Information theft, manipulating data, Financial loss,Revenge,Ransom,DamagingReputation.

EthicalHacking

• Ethical Hacking involves the use of hacking tools, tricks, andtechniquestoidentifyvulnerabilitysoastoensuresystemsecurity.

• Ethical Hackers performs security assessment of their organizationwiththepermissionofconcerned authorities

In simple - Ethical hacking involves an authorized attempt to gainunauthorizedaccesstoacomputersystem,application,ordata. Carrying out an ethical hack involves duplicating strategies andactionsofmaliciousattackers....Alsoknownas"whitehats,"ethicalha

ckersaresecurityexpertsthatperformtheseassessments

Why?

* Topreventhackersfromgainingaccess
* Touncovervulnerabilities
* Tostrengthentheorganization
* Tosafeguard thedata
* ToavoidsecurityBreaches
* Toenhancesecurityawareness

TypeofHackers

Blackhat

Black hats are hackers who use their knowledge and skills todiscover and exploit security vulnerabilities for financialgain or malicious reasons. Their activities can cause majordamage to their targets and their systems. Black hats areusually involved with criminal activities such as stealingpersonal and financial information or shutting downwebsitesandnetworks.

Whitehat

White hats are ethical hackers who use their knowledge andskills to improve security of a system by discoveringvulnerabilities before black hats do. They pretty much usethe same methods and tools black hats do, but unlike blackhats, white hats have a permission of the system owner to usethosemethods.

Greyhat

Grey hats are hackers who are not as bad as black hats, butalso not as ethical as white hats. They might help black hatsin their endeavors, but they also might help in discoveringvulnerabilitiesorcheckingthelimitationsofasystem.

Suicidehackers

Suicide hackers are ready and willing to perform an attackfora"cause",eveniftheygetcaughtandprosecuted.

Scriptkiddies

Script kiddies are hackers who are new to hacking and don'thave much knowledge or skills to perform hacks. Instead,they use tools and scripts developed by more experiencedhackers.

Cyberterrorists

Cyber terrorists are hackers who are influenced by certainreligious or political beliefs. They work to cause fear anddisruptionofsystemsandnetworks.

Statesponsoredhackers

Statesponsoredhackersarerecruitedbygovernmentstogainaccessto secretinformationofothergovernments.

Hacktivists

Hacktivistsbreakintogovernmentorcorporatesystemsoutofprotest. They use their skills to promote a political or socialagenda. Targets are usually government agencies or bigcorporations.

Terminologies

Adware – Adware is software designed to force pre-chosenadstodisplay onyoursystem.

Attack – An attack is an action that is done on a system togetitsaccessand extractsensitivedata.

Back door – A back door, or trap door, is a hidden entry to acomputing device or software that bypasses security measures,suchasloginsandpasswordprotections.

Bot – A bot is a program that automates an action so that itcan be done repeatedly at a much higher rate for a moresustained period than a human operator could do it. Forexample, sending HTTP, FTP or Telnet at a higher rate orcallingscripttocreateobjectsata higher rate.

Botnet–A botnet,also knownaszombiearmy, isagroupofcomputerscontrolledwithouttheirowners'knowledge. Botnets are used to send spam or make denial of serviceattacks.

Brute force attack – A brute force attack is an automated andthe simplest kind of method to gain access to a system orwebsite. It tries different combination of usernames andpasswords,overandoveragain,untilit getsin.

BufferOverflow-BufferOverflowisaflawthatoccurswhenmore data is written to a block of memory, or buffer, thanthebufferisallocatedtohold.

Clone phishing – Clone phishing is the modification of anexisting, legitimate email with a false link to trick therecipientintoprovidingpersonalinformation.

Cracker – A cracker is one who modifies the software toaccessthefeatureswhichareconsideredundesirablebythepers on cracking the software, especially copy protectionfeatures.

Denial of service attack (DoS) – A denial of service (DoS)attack is a malicious attempt to make a server or a networkresource unavailable to users, usually by temporarilyinterrupting or suspending the services of a host connected totheInternet.

DDoS- Distributeddenialofserviceattack.

Exploit Kit – An exploit kit is software system designed torunonwebservers,withthepurposeofidentifyingsoftwarevulnerabilities in client machines communicating with itand exploiting discovered vulnerabilities to upload andexecute maliciouscodeontheclient.

Exploit- Exploitisapieceofsoftware,achunkofdata,orasequence of commands that takes advantage of a bug orvulnerability to compromise the security of a computer ornetworksystem.

Firewall – A firewall is a filter designed to keep unwantedintruders outside a computer system or network whileallowing safe communication between systems and users ontheinsideofthefirewall.

Keystroke logging – Keystroke logging is the process of trackingthe keys which are pressed on a computer (and whichtouchscreen points are used). It is simply the map of acomputer/human interface. It is used by gray and black hathackers to record login IDs and passwords. Keyloggers areusually secreted onto a device using a Trojan delivered by aphishingemail.

Logic bomb – A virus secreted into a system that triggers amaliciousaction whencertainconditions aremet.Themostcommon versionisthetimebomb.

Malware – Malware is an umbrella term used to refer to avariety of forms of hostile or intrusive software, includingcomputer viruses, worms, Trojan horses, ransomware,spyware,adware,scareware,andothermaliciouspr ograms.

Master Program – A master program is the program a blackhat hacker uses to remotely transmit commands to infectedzombie drones, normally to carry out Denial of Serviceattacksorspamattacks.

Phishing – Phishing is an e-mail fraud method in whichthe perpetrator sends out legitimate-looking emails, in anattempt to gather personal and financial information fromrecipients.

Phreaker – Phreakers are considered the original computerhackers and they are those who break into the telephonenetwork illegally, typically to make free longdistance phonecallsorto tapphonelines.

Rootkit – Rootkit is a stealthy type of software, typicallymalicious, designed to hide the existence of certain processesor programs from normal methods of detection and enablecontinuedprivilegedaccess toacomputer.

Shrink Wrap code – A Shrink Wrap code attack is an act ofexploitingholesinunpatchedorpoorlyconfiguredsoftware.

Social engineering – Social engineering implies deceivingsomeone with the purpose of acquiring sensitive andpersonalinformation,likecreditcarddetailsorusernamesand passwords.

Spam – A Spam is simply an unsolicited email, also knownas junk email, sent to a large number of recipients withouttheirconsent.

Spoofing – Spoofing is a technique used to gainunauthorized access to computers, whereby the intrudersends messages to a computer with an IP address indicatingthatthemessageiscomingfromatrustedhost.

Spyware – Spyware is software that aims to gatherinformation about a person or organization without theirknowledgeandthatmaysendsuchinformationtoanother

entitywithouttheconsumer'sconsent,orthatassertscontroloverac omputerwithouttheconsumer'sknowledge.

SQL Injection – SQL injection is an SQL code injectiontechnique, used to attack data-driven applications, inwhich malicious SQL statements are inserted into an entryfield for execution (e.g. to dump the database contents to theattacker).

Threat – A threat is a possible danger that can exploit anexisting bug or vulnerability to compromise the security of acomputeror networksystem.

Trojan – A Trojan, or Trojan Horse, is a malicious programdisguised to look like a valid program, making it difficult todistinguish from programs that are supposed to be theredesigned with an intention to destroy files, alterinformation,steal passwordsorotherinformation.

Virus – A virus is a malicious program or a piece of codewhich is capable of copying itself and typically has adetrimental effect, such as corrupting the system ordestroyingdata.

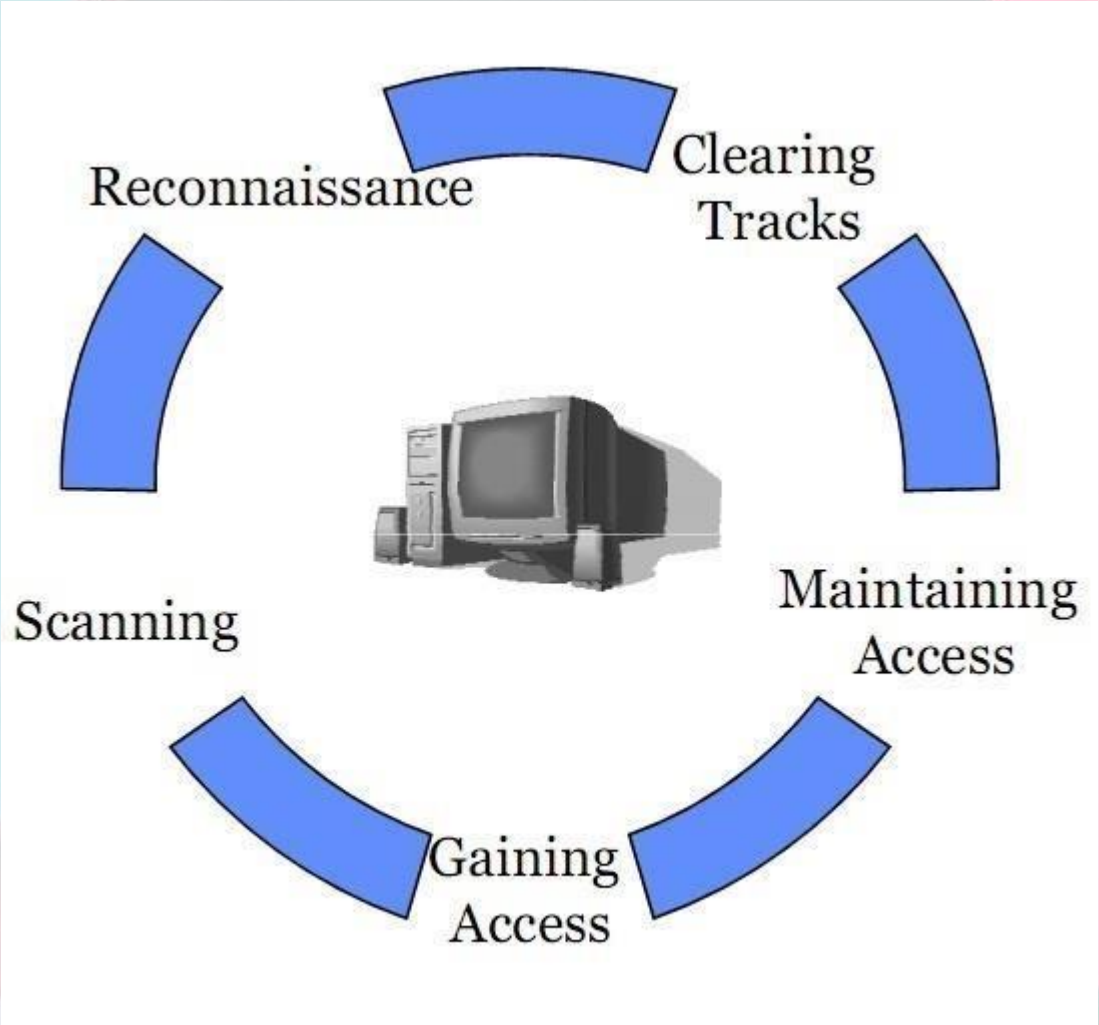
Vulnerability – A vulnerability is a weakness which allowsa hacker to compromise the security of a computer ornetworksystem.

Worms – A worm is a self-replicating virus that does notalterfilesbutresidesinactivememoryandduplicatesitself.

Cross-site Scripting – Cross-site scripting (XSS) is a type ofcomputer security vulnerability typically found in webapplications. XSS enables attackers to inject client-side scriptintowebpagesviewedbyotherusers.

Zombie Drone – A Zombie Drone is defined as a hi-jackedcomputer that is being used anonymously as a soldier or'drone' for malicious activity, for example, distributingunwantedspame-mails.

PhasesofHacking



Reconnaissance:- This is the primary phase where theHackertriestocollectasmuchinformationaspossibleaboutthe target. It includes Identifying the Target, finding out thetarget'sIPAddress Range,Network,DNSrecords,etc.

Scanning:-It involves taking the information discoveredduring reconnaissance and using it to examine the network.Tools that a hacker may employ during the scanning phasecan include dialers, port scanners, network mappers,sweepers, and vulnerability scanners. Hackers are seekingany information that can help them perpetrate attack suchas computer names,IPaddresses,anduseraccounts.

Gaining Access:- After scanning, the hacker designs theblueprintofthenetworkof thetargetwiththehelpofdatacollected during Phase 1 and Phase 2. This is the phasewhere the real hacking takes place. Vulnerabilitiesdiscovered during the reconnaissance and scanning phaseare now exploited to gain access. The method of connectionthe hacker uses for an exploit can be a local area network(LAN, either wired or wireless), local access to a PC, theInternet, or offline. Examples include stack based bufferoverflows,denialofservice(DoS),andsessionhijacking. These topics will be discussed in later chapters. Gainingaccessisknowninthehackerworldasowningthe system.

Maintaining Access:- Once a hacker has gained access, theywant to keep that access for future exploitation and attacks.Sometimes, hackers harden the system from other hackers orsecurity personnel by securing their exclusive access withbackdoors, rootkits, and Trojans. Once the hacker owns thesystem, they can use it as a base to launch additionalattacks. In this case, the owned system is sometimes referredtoasazombiesystem.

Covering Tracks:- Once hackers have been able to gain andmaintain access, they cover their tracks to avoid detection bysecurity personnel, to continue to use the owned system, toremove evidence of hacking, or to avoid legal action. Hackerstry to remove all traces of the attack, such as log files orintrusion detection system (IDS) alarms. Examples ofactivities during this phase of the attack includesteganography, the use of tunneling protocols, and alteringlogfiles.

SecurityPolicies

AccessControlPolicy

Information is a valuable asset and access to it must be managed withcare to ensure that confidentiality, integrity and availability aremaintained.

The University of Sheffield provides access to information assets,accounts,systemsandresourcesbasedontheprincipleofleastprivilege(seeInformationSecurity Glossaryforexplanation).

This policy outlines the rules relating to authorising, monitoring andcontrollingaccesstoUniversityaccounts,informationandinformationsystems.

firewall policy defines how an organization's firewalls should handleinbound and outbound network traffic for specific IP addresses andaddress ranges, protocols, applications, and content types based on theorganization'sinformationsecurity policies

passwordpolicyisasetofrulesdesignedtoenhancecomputersecuritybyencouraging users to employ strong passwords and use themproperly. A password policy is often part of an organization's officialregulationsandmaybetaughtaspartofsecurityawarenesstraining..

email policy is to set proper expectations with your employees. Whataretherulesandguidelinesregardingemailandwhathappensifyouignore the rules? The email policy should be written and reviewedwiththe employeeatthe timeofemployment.

Information protection policy is a document which provides guidelinesto users on the processing, storage and transmission of sensitiveinformation. Main goal is to ensure information is appropriatelyprotectedfrommodificationordisclosure....Itshoulddefinesensitivitylevelsofinformation.

user account policy is a document which outlines the requirements forrequesting and maintaining an account on computer systems ornetworks, typically within an organization. It is very important forlargesiteswhereuserstypicallyhaveaccountsonmanysystems.

Physicalsecurity

Is the protection of personnel, hardware, software, networks and datafrom physical actions and events that could cause serious loss ordamagetoanenterprise,agencyorinstitution.Thisincludesprotectionfrom fire, flood, natural disasters, burglary, theft, vandalism andterrorism.

1. SecurityControls

Computersecurityisoftendividedintothreedistinctmastercategories,commonlyreferredtoas controls:

- Physical
- Technical
- Administrative

These three broad categories define the main objectives of propersecurity implementation. Within these controls are sub-categories thatfurtherdetailthecontrolsandhow toimplementthem.

2. PhysicalControls

Physical control is the implementation of security measures in adefined structure used to deter or prevent unauthorized access tosensitivematerial.Examplesofphysicalcontrolsare:

- Closed-circuitsurveillancecameras
- Motionorthermalalarmsystems
- Securityguards
- PictureIDs
- Lockedanddead-boltedsteeldoors

Biometrics(includesfingerprint,voice,face,iris,handwriting,andothera utomatedmethodsusedtorecognizeindividuals)

3. TechnicalControls

Technical controls use technology as a basis for controlling the accessand usage of sensitive data throughout a physical structure and over anetwork. Technical controls are far-reaching in scope and encompasssuchtechnologiesas:

- Encryption
- Smartcards
- Networkauthentication
- Accesscontrollists(ACLs)
- Fileintegrityauditingsoftware

4. AdministrativeControls

Administrativecontrolsdefinethehumanfactorsofsecurity.Itinvolvesall levels of personnel within an organization and determines whichusershaveaccesstowhatresourcesandinformationbysuchmeansas:

- Trainingandawareness
- Disasterpreparednessandrecoveryplans
- Personnelrecruitmentandseparationstrategies
- Personnelregistrationandaccounting

PenetrationTesting

• PenetrationTestingisamethodofevaluatingthesecurityofaninform ationsystemornetworkbysimulatinganattackto

• findvulnerability

• SecurityMeasures

• DocumentationandReportPreparation

Need?

1)Identification of

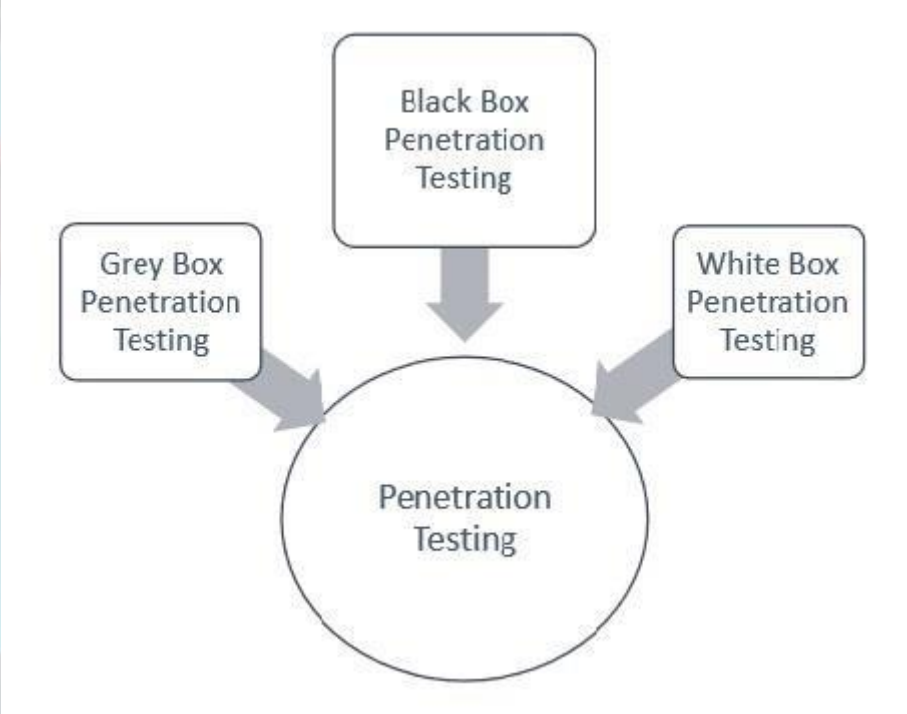
threats2)SecurityProtectionsandco

ntrols

3)AssessmentofOrganization'sSecurity

4)EvaluationofNetworkSecurity5)UpgradationofInfrastructure

TypesofPentesting:



BlackBoxPenetrationTesting

In black box penetration testing, tester has no idea about the systemsthat he is going to test. He is interested to gather information about thetarget network or system. For example, in this testing, a tester onlyknowswhatshouldbetheexpectedoutcomeandhedoesnotknowhowthe outcomesarrives. Hedoes not examine anyprogrammingcodes.

AdvantagesofBlackBoxPenetrationTestingItha

sthe followingadvantages –

- Testerneednotnecessarilybeanexpert,asitdoesnotdemand specificlanguageknowledge

- Testerverifiescontradictionsintheactualsystemandthespecifications
- Testisgenerallyconductedwiththeperspectiveofauser,notthedesigner

DisadvantagesofBlackBoxPenetrationTestingItsdis

advantages are –

- Particularly,thesekindsoftestcasesaredifficulttodesign.
- Possibly, itisnotworth,incasedesignerhasalreadyconductedatestcase.
- Itdoesnotconducteverything.

WhiteBoxPenetrationTesting

Thisisacomprehensivetesting,astesterhasbeenprovidedwithwhole range of information about the systems and/or network such asSchema,Sourcecode,OSdetails,IPaddress,etc.Itisnormallyconsideredasa simulationofanattackbyaninternalsource.Itisalsoknownasstructural,glas sbox,clearbox,andopenboxtesting.

Whiteboxpenetrationtestingexaminesthecodecoverageanddoesdataflowtes ting,pathtesting, looptesting, etc.

Advantages of White Box Penetration

TestingItcarriesthefollowingadvantages-

- Itensuresthatallindependentpathsofamodulehavebeen exercised.
- Itensuresthatalllogicaldecisionshavebeenverifiedalongwiththeirtr ue and falsevalue.
- Itdiscoversthetypographicalerrorsanddoessyntaxchecking.
- It finds the design errors that may have occurred because of thedifference between logical flow of the program and the actualexecution.

GreyBoxPenetrationTesting

In this type of testing, a tester usually provides partial or limitedinformation about the internal details of the program of a system. Itcan be considered as an attack by an external hacker who had gainedillegitimateaccesstoanorganization'snetworkinfrastructuredocum ents.

Advantages of Grey Box Penetration

TestingIthasthe followingadvantages-

- Asthetesterdoesnotrequiretheaccessofsourcecode,itisnon-intrusiveandunbiased
- As there is clear difference between a developer and a tester, sothereis least riskof personalconflict
- You don't need to provide the internal information about theprogram functionsand otheroperations

StandardsandCompliances

1) Payment Card Data Security Standard (PCI DSS)2) ISO/IEC27001:2013

3) Health Insurance Portability and AccountabilityAct(HIPPA)

4) SarbanesOxleyAct(SOX) – TopreventfraudulentFinancialActivities(shares)

5) The Digital Millennium Copyright Act(DMCA) – Copyrights

6) Federal Information Security Management Act(FISMA) – NaturalandManMadethreats

7) Governance,RiskManagementandCompliance(GRC)

8) General Data Protection Regulation (GDPR) – EU andTransferoutsideEUCyber Laws

- Section43-DamagetocomputerSystem
- Section65-TamperingofComputerSourceDocuments
- Section66-ComputerRelatedOffences
- SECTION66A-SendingoffensiveMessages

- SECTION66B– Smugglinggoods
- SECTION66C–Identitytheft
- SECTION66D–FalsePersonation(Telecallers)
- SECTION66E–ViolationofPrivacy
- SECTION66F–CyberTerrorismCyberLaws–Cont'd
- SECTION67–TransmittingObsceneMaterial
- SECTION71–Misrepresentation
- SECTION72–BreachingofConfidentialityandPrivacy
- SECTION73–PublishingElectronicSignatures

HelloEveryoneIhopeyoulikethecoursecontent… butthethingisifyouwanttodo something great you need to learn more and more everyday … This training is totally FREEof Cost the only thing I want from you guys is your time and efforts towards this training.Iwishyouthebestinyourfutureendeavors,HappyHacking

DofollowmeonInstagram-https://www.instagram.com/admirerr_20/