**Sulmet dhe Kërcnimet**

**Sipërfaqja e sulmit** paraqet pika të ndryshme në sistem ku sulmuesi mund të futet në sistem dhe të marrë të dhëna.

**Shfrytëzimi** paraqet një mekanizën që përdoret për të nxitur një dobësi ose për të komprementuar një pasuri.

**Rreziku** paraqet ndjenien se një kërcënim mund të shfrytëzoj cenushmërinë e një aseti për të shkaktuar pasoja të pa dëshiruara.

**White Hat Hackers** : Hakera etik që përdorin njohurit e tyre për qëllime etike dhe ligjore si teste e pentrimit.

**Grey Hat Hackers** : Hakera që bëjn krime dhe veprime jo etike por jo për qëllim përfitimi ose dëmitimi.

**Black Hat Hackers** : Hakera që kryejn krime jo etike për qëllime të periftimeve personale ose dëmtimin e indivdëve ose organizatave.

Akterët e kërcimit është term që i referohet hakerve gri dhe të zi.

Akterët e kërcnimit mund ti ndajmë në : **Script-kiddies** – hakera pa përvojë që drejtojnë dhe përdorin mjete ekzistuese për të bër dëme, nuk kanë qëllime përfitimi. **Hakerët e bardh ose të zi** që sulmojnë sekretet qeveritare, rrëzojnë rrjete ose mbledhin informata intelegjente. **Kriminelët kibernetik** – Haker të zi që për qëllim kanë paran dhe fitojn miliarda nga konsumatorët dhe bizneset. **Hackaktivistët** – Hakerët gri që protestojnë kundër ideve politike dhe shoqërore.

**Detyrat e cyber security** : Vedisimi i individëve rreth sigurisë kibernetike, mbrojtia e asteve të përdoresve dhe konsumatorëve, rapotimi i sulmeve ndaj autoriteteve, njohuri rreth kërcnimeve në e-mail dhe internet, ruajtia e informatave nga vjedhia.

Në kohët e fundit është rritur përdorimi i mjeteve për të shfrytëzuar dobësit për qëllime hakimi.

Kategorit e sulmeve : **Përgjimi** – Kapin dhe ndëgjojnë treafikun në rrjet. **Modifikimi i të dhënave** – Bëjn ndryshme në të dhënat pa dijenin e marrësit ose dërguesit. **IP Spoofing** – Falsifikim i adresave dhe paraqitja valide e tyre. **Fjalkalimi i bazuar** – Përdorin qasjen në një llogari për të marrur informata për llogarit tjera. **Mohimi i shërbimit** – Parandalojnë ose ngadalsojnë përdorimin e një kompjuteri apo rrjeti. **Man-in-the-middle** – Sulmuesi vendoset në mes të burimi dhe destinacionit ku arrin të monitoroj, knotrolloj dhe ndrsyhoj komunikin mes tyre. **Compromised Key** – Fiton qasje në komunikim duke përdorus qels të fshetë.

**Malware** – Janë programe ose kode qëllim kqija të cilat janë të projektuar për të dëmtuar, vjedhur, prishur ose shkaktuar veprime të pa ligjshme në hose dhe rrjeta të dhënave.

**Viruset** – Janë lloj i malware që propagandohen duke u vendosur në programe legjitime, shpërndahen me usb, cd, email etj mund të rrin të qeta për një koh të caktuar dhe pastaj të fillojnë kryerjen e veprimeve të pa dëshiruar që mund ta dëmtojnë kompjuterin.

**Trojan Horses** – Janë malware të cilat paraqiten si legjitime, zakonisht qenden në lojat online fitojn qasje të privilegjuar dhe mund të shkaktojnë dëme të menjëhershme.

**Kalsifikimi i Trojan Horses** : **Trojan Horses për qasje të largët** – i mundësojn akterit të kërcnimit qasje të pa autorizuar nga largësia. **Trojan Horses për kalim të të dhënave** – i sigurojnë akterit të kërcnimit të dhëna konfidenciale si fjalkalime. **Trojan Horses shkatërrues** – Korruptojnë ose fshijnë skederët. **Trojan Horses proxy** – përdorin pasijet e viktimës për të kryer veprime dhe sulme të paligjshme. **Trojan Horses FTP** – përdoren për ti mundësuar transferimin e pa autorizuar të skederëve në paisje të pa autorizuara. **Trojan Horses caktivizues** - bën ndaljen e funksionimit të programeve antiviruse dhe firewall. **Trojan Horses DoS** – Ndalon ose ngadalson ndonjë aktivitet në rrjet.

**Worms** janë lloj i malware të cilat kur infektojnë një sistem vet ekzekutohen përhapen shpejtë prej sistemit në sistem, për dallim nga viruset nuk presin aktivizim e bëjn vet një gjë të tillë.

Sulmet e rrafshta pëbëhen nga tre komponent : **Aktivizimi i cenushmërisë** – Worm e instalon vetëm duke përdorur një mekanizëm të shërbimit si e-mail, trojan hourse etj. **Mekanizmi i propagandimit** – Worm fillon e përsërit veten dhe ndryshon objektivat. **Shitës me pages** – Worm mundëson qasje nga largë ose hap ndonjë back door ose krijon sulme DoS.

**Ransomware** janë malware të cilat mohojn qasjen në sisteme kompjuterike ose të dhëna një gjë të till e bëjn duke përdorur algoritmet për kriptim dhe për të rifituar qasjen kërkojnë para. Kto përhapen me email, ad-s dhe inxhinieri sociale.

Modern-malwares : Adware, Spyware, Scareware, Phishing, Rootkits.

Një kompjuter i infektuar me malware do ket kto karakteristika : Ndalje ekranit ose crash i sistemit, ikona të quditshme në desktop, shfrytëzim i madh i resurseve harduerike, ngadalsim i rrjetit, hapja e porteve TCP dhe UDP, ndalje e antiviruseve.

Sulmet ndahet në tri kategori kjo për të na mundësur ti trajtojm sulmet si lloje e jo si individuale : **Reconnaisancee, Acces, Denial of Services**.

**Sulmet e zbulimit(recon)** mledhin informata rreth sistemit dhe dobësive të tij, kto sulme i paraprijn sulmeve të hyrjes dhe DoS.

Sulmet e zbulimit fillojn duke marur informata nga ip aktive për portet dhe shërbimet në dispozicion, duke përdour ndonjë tool sic ështp nmap mund ti indetifikojnë portet e hapura.

Sulmet e qasjes i shfrytëzojn dobësit e porteve FTP ose HTTP për të vjedhur të dhëna, për të fituar qasje ose për të ndryshuar privilegjet e qasjes.

Llojet e sulmeve të qasjes : **Sulmet me fjalkalim** : Merren fjalkalimet e sistemeve kritike duke përdoru fjalorë, brtue force, inxhinieri sociale ose phishing. **Pass-the-hash** : Sulmuesi ka qasje në paisjen e vikitmës dhe me anë të ndonjë malware e mer hash passwordin me të cilin mund të qaset në serverat ose paisje tjera. **Shfrytëzimi i besushmërisë** : Përodren lidhjet e besuara për të fituar qajse në burimet e rrjetit. **Ridirective Port** : Përdor një sistem të kompromentuar për të zgjeruar sulmet në sistemet tjera. **Man-in-middle** : Sulmusi vendos veten midis dy njësive legjitime ku pastaj mund të përciell, lexoj ose ndryshoj të dhënat që kalojn në mes dy palëve. **IP, MAC, DHCP Spoofing** : Falsifikojnë adresat për tu dukur si paisje tjetër.

**Inxhinieria sociale** : Është qajse që sulmusit mundohen ti manipulojnë viktimat për të kryer ndonjë veprim ose shfaqur ndonjë të dhënë konfidenciale që do i mundësonte atyre qasje në rrjet.

**Llojet e inxhinieris sociale** : Phishing, Diqka-për-Diqka, Hacking Visualizion, Pretext, Bating, Spam.

**Phishing** është teknik e inxhinieris sociale që i kërcnon viktimat duke i dërguar e-mail që duken legjitime.

Llojet e Pshishing sulmeve : **Pshishing** : Synon një individ ose një biznes. **Wishing** : Synon objektiva të mëdha. **Phraming** : E infekton DNS. **Water hole** : Injekton malware në web. **Vishing** : Bëhet me anë të voice mail. **Smishing** : Me anë të sms.

Njerzit paraqesin lidhjen më të dobët të siguris kibernetike, për këtë organizatat duhet të mbajn trajnime me qëllim të ngritjes së vetëdijes për sigrurin kibernetike.

**Sulmet e mohimit të shërbimit** : Kto sulme për qëllim kanë mohin e shërbimeve ndaj përdoruesve, aplikacioneve ose paisjeve, një gjë të till e arrijnë duke e mbingarkuar trafikun me paketa keq të formatuara.

**DDOS** termet : **Zombie** : Hostet e kompromentuar të cilat shpërndaj malware të quajtura bot-s. **Bot-s** : Janë malware të dizajnuara për infektim të hostit dhe komunikim me sistemet tjera. **Botnet** : Janë grup i zombie që komandohen nga handler. **Handler** : Udhëheqës master-komadues i cili i kontrollon botnetet. **Botmaster** : Sulmuesi i cili i kontrollon handlers dhe botnetet.

**Sulmet e mbi popullimit** kanë për qëllim ti gjejnë mangësit në memorien e serverit dhe atë ta përdorin për të derguar vlera më të mëdha se që ka qen në pritje duke e bër serverin e pa operueshëm.

**Metodat e evazionit** përdoren për ta fshehur sulmin ose llojin e tij , kjo arrihet me anë të ecryption dhe tuneling.