DESHIFRIMI I SULMEVE KIBERNETIKE

CLICKJACKING

Është një teknikë ku elementë keqdashës fshihen nën përmbajtje në dukje të padëmshme, duke i mashtruar përdoruesit të klikojnë dhe të kryejnë veprime të paqëllimta

BUFFER OVERFLOW

Shfrytëzimi i një dobësie programimi për të ngarkuar hapsirën e buffer-it të një programi dhe duke sjellë pasoja të paqëllimta si akses i paautorizuar.

BRUTE FORCE

Një metodë për të fituar akses të paautorizuar duke provuar sistematikisht të gjitha kombinimet e mundshme të fjalëkalimeve derisa të gjendet e sakta.

EAVESDROPPING (PËRGJIMI)

Duke përgjuar dhe monitoruar në mënyrë të paligjshme komunikimin privat, të bërë shpesh pa dijeninë ose pëlqimin e palëve të përfshira.

PASSWORD CRACKING(THYERJA E FJALËKALIMIT)

Procesi i përpjekjes për të deshifruar fjalëkalimet duke përdorur teknika të ndryshme, përfshirë sulmet e fjalorit, për të fituar akses të paautorizuar.

PHARMING

Ridrejtimi i trafikut të faqes në internet nga faqet legjitime në ato mashtruese me qëllim të mbledhjes së informacionit të ndjeshëm siç janë kredencialet e login.

MALVERTISING

Shpërndarja e malware përmes reklamave në internet, shpesh duke vendosur kodin keqdashës në reklama në dukje të padëmshme.

DNS SPOOFING

Sigurimi i përgjigjeve false të sistemit të emrave të domain -it (Domain Name System) për të ridrejtuar trafikun e ligjshëm në vendet me qëllim të keq.

WIRELESS SNIFFING

Përgjimi dhe ekzaminimi i trafikut të rrjetit për të kapur informacione të ndjeshme të transmetuara në rrjet.

DNS TUNNELLING

Mbështetja e trafikut jo-DNS brenda paketave DNS për të anashkaluar kontrollet e sigurisë dhe për të ekzaminuar të dhënat.

SMISHING

Një formë e sulmit të phishing të kryer përmes shërbimit të mesazheve të shkurtra (SMS) ose platforma të tjera të mesazheve

VISHING

Sulmet e phishing të kryera duke përdorur komunikimin me zë, zakonisht thirrjet telefonike.

SUPPLY CHAIN ATTACK

Kompromentimi i një objektivi duke infiltruar zinxhirin e tij të furnizimit(supply chain), duke infektuar produkte ose software gjatë prodhimit ose shpërndarjes.

DNS HIJACKING

Ridrejtimi i kërkesave(queries) të DNS në serverë me qëllim të keq, duke sjellë përgjimin e të dhënave të mundshme ose manipulime.

SULME TË BAZUARA NË USB

Shfrytëzimi i dobësive përmes pajisjeve USB ku shpesh përfshihet edhe përdorimi i pajisjeve USB të infektuara.

WATERING HOLE

Një strategji sulmi ku sulmuesit synojnë faqet e internetit të frekuentuara nga një grup specifik i individëve, duke shfrytëzuar besimin që lidhet me ato faqe.

SESSION HIJACKING

Marrja e paautorizuar e seancës aktive të një përdoruesi, duke lejuar sulmuesin të fitojë kontrollin dhe të hyjë në informacione të ndjeshme

CLICK FRAUD (KLIKIMI I PALIGJSHSHËM)

Klikimi i paligjshëm në reklamat në internet për të gjeneruar të ardhura ose për të shteruar buxhetin e një reklamuesi.

SQL INJECTION

Sulmuesi injekton kodin me qëllim të keq SQL duke shfrytëzuar dobësitë në një bazë të dhënash dhe duke fituar potencialisht qasje të paautorizuar ose të dhëna manipuluese.

MAN-IN-THE-MIDDLE (MITM)

Palët e treta të paautorizuara përgjojnë dhe ndryshojnë komunikimin midis dy palëve, duke çuar në manipulim të mundshëm të të dhënave ose përgjim.

MOHIMI I SHËRBIMIT (DOS)

Mbingarkon një sistem ose rrjet me kërkesa të tepërta, duke e bërë atë të paarritshëm për përdoruesit e ligjshëm.

SHFRYTËZIMI I VOICE ASSISTANT

Manipulimi i pajisjeve të aktivizuara me zë për të kryer veprime të paqëllimta ose për të nxjerrë informacione të ndjeshme .

SULMI DNSSEC

Synon vulnerabilitetet në shtesat e sigurisë së Domain Name System për të kompromentuar integritetin e informacionit

IOT (INTERNET OF THINGS)

Shfrytëzimi i vulnerabiliteteve në pajisjet e lidhura në internet për të fituar akses ose kontroll të paautorizuar.

CYPTOJACKING

Përdorimi i paligjshëm i kompjuterit të dikujt tjetër për të minuar kriptomonedha pa dijeninë ose pëlqimin e tyre.

KEYSTROKE INJECTION

Injektimi i tasteve keqdashës në një kompjuter për të ekzekutuar komanda ose veprime të paautorizuara.

TROJAN HORSE

Një software keqdashës i maskuar si i ligjshëm, për të mashtruar përdoruesit që ta instalojnë atë duke kompromentuar sistemet e tyre.

MALWARE

Software keqdashës i krijuar për të dëmtuar ose shfrytëzuar sistemet kompjuterike, duke përfshirë viruset, trojanët dhe worms.

CROSS-SITE SCRIPTING (XSS)

Injekton skripte keqdashëse në faqet në internet të vizituara nga përdoruesit e tjerë, duke kompromentuar sigurinë e tyre ose duke vjedhur informacionin.

FILE INCLUSION EXPLOITS

Shfrytëzimi i vulnerabiliteteve për të përfshirë skedarë në një server, duke lejuar akses të paautorizuar ose ekzekutimin e kodit arbitrar.

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Mbingarkon një rrjet ose shërbim duke koordinuar një numër të madh të sistemeve për ta përmbytur atë me trafik.

ADVANCED PERSISTENT THREAT (KËRCËNIM I PËRPARUAR I VAZHDUESHËM)

Sulme të sofistikuara dhe të zgjatura kibernetike të kryera nga kundërshtarë të financuar mirë dhe të organizuar.

PHISHING

Përpjekje mashtruese për të marrë informacione të ndjeshme duke u paraqitur si një entitet i besueshëm.

SESSION REPLAY

Kapja dhe riprodhimi i të dhënave të seancës së përdoruesit(user session). Zbulimi i informacionit të ndjeshëm të futur gjatë seancave në internet.

REVERSE ENGINEERING (INXHINIERIA E KUNDËRT)

Analizimi dhe dekonstruktimi i software-it ose hardware-it për të kuptuar modelin e tij, të bërë shpesh për hulumtime të sigurisë ose shfrytëzim.

SOCIAL ENGINEERING (INXHINIERIA SOCIALE)

Manipulimi i individëve në shpërndarjen e informacionit konfidencial ose kryerjen e veprimeve që mund të kompromentojnë sigurinë

FILELESS MALWARE

Software keqdashës që funksionon në memorje, duke lënë pak ose aspak gjurmë në disk dhe duke e bërë zbulimin e tij sfidues.

INSIDER DATA THEFT (VJEDHJA E TË DHËNAVE TË BRENDSHME)

Akses i paautorizuar dhe vjedhja e informacionit të ndjeshëm nga individë brenda një organizate.

RANSOMWARE

Kripton skedarët e një përdoruesi dhe kërkon pagesa për lëshimin e tyre

LOGIC BOMB

Kodi që mbetet joaktiv derisa të shkaktohet nga kushte specifike, duke çuar në veprime keqdashëse.

SULME TË BAZUARA NË AI

Shfrytëzimi i vulnerabiliteteve në sistemet e inteligjencës artificiale, përfshirë modelet e machine learning.

SULMET SIDE CHANNEL

Nxjerrja e informacionit të ndjeshëm nga një sistem duke analizuar efektet anësore të paqëllimta, të tilla si konsumi i energjisë ose rrezatimi elektromagnetik.

PASSWORD SPRAYING

Përpjekja për të zbuluar disa fjalëkalimeve të zakonshme në shumë llogari për të shmangur zbulimin dhe për të fituar akses të paautorizuar.

KEY LOGGING

Regjistrimi dhe kapja e tasteve të bëra nga përdoruesit, zakonisht për të marrë informacione të ndjeshme si fjalëkalimet ose numrat e kartave të kreditit

SHFRYTËZIMI I VULNERABILITETIT ZERO DAY

Shfrytëzimi i dobësive në software ose sisteme që janë të panjohura për shitësin e software-it, duke u dhënë sulmuesve një avantazh derisa të zhvillohet një rregullim.