Sigurnost Active Directory-a

Šostarec, Magdalena

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Magdalena Šostarec

SIGURNOST ACTIVE DIRECTORY-A

ZAVRŠNI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Magdalena Šostarec

Matični broj: 35918/07–R

Studij: Primjena informacijske tehnologije u poslovanju

SIGURNOST ACTIVE DIRECTORY-A

ZAVRŠNI RAD

Mentor/Mentorica:

Ph.D. Igor Tomičić

Varaždin, lipanj 2024.

Magdalena Šostarec

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Tema ovog rada je sigurnost Active Directory-a, koji je Microsoftova usluga za upravljanje identitetima i pristupom. Upravo ova usluga je ključna komponenta u mnogim organizacijama, zbog toga što je upravo sigurnost AD-a od velike važnosti zbog osiguranja integriteta, resursa i povjerljivosti. Sam početak zaštite Active Directory-a je kontrola nad identitetima u pravilima pristupa. Kada se implementira politika snažnih zaporki, višerazinska autentikacija, praćenje logova i ograničavanje privilegija, već je velika razlika od nekorištenja ovih metoda kod sigurnosti. Neki od alata kao što su Microsoft Security Compliance Toolkit, SolarWinds Security Event Manager i ManageEngine ADAudit Plus pružaju timovima sredstva za sigurnosne događaje. Ti alati su napredna rješenja za detekciju nepravilnosti, praćenje ponašanja korisnika te brzoj reakciji na sigurnosne prijetnje. Uz to, kada se implementiraju redovita ažuriranja sustava, testiranje i analizu slabosti, ojačavaju integritet Active Directory-a.

Zaključak ovog završnog rada je da Activ Directory i sigurnost AD-a spaja ljudske, tehničke i proceduralne aspekte. Niti jedan od ova tri čimbenika se ne smije zanemariti i zapostaviti jer je jedanko važan kao i ostali i nužan je za očuvanje cjelokupne sigurnosti informacijskih sustava informacija i zaštitu od kibernetičkih prijetnji.

Sadržaj

1.UVOD

U današnjem životu i okruženju koje se sve više okreće digitalizaciji i informatici, sigurnost informacijskih sustava postaje sve važnija tema za organizacije u cijelom svijetu. Jedan od ključnih elemenata infrastrukture informacijske tehnologije je Active Directory (AD), koji nam predstavlja temelj za upravljanje korisnicima, računalima i resursima unutar pojedine organizacije. Sigurnost AD-a je ključ za održavanje integriteta, povjerljivosti i dostupnosti podataka.

Ovaj završni rad istražuje i sistematično prikazuje različite aspekte sigurnosti Active Directory-a, a kao cilj ima pružanja uvida sigurnosne prijetnje, prakse i tehnike zaštite, kao i planiranje zaštite i oporavka u slučaju napada.

Uvodna poglavlja će se fokusirati na razumijevanje samog koncepta Active Directory-a, ključne termine koji su vezani uz njegovu sigurnost te primjere napada koji ciljaju AD infrastrukturu. Nakon toga, istražit ćemo sigurnosne prakse koje organizacije mogu primijeniti kako bi zaštitile svoj Active Directory. Posebno ću se posvetiti tehničkim mjerama sigurnosti i konfiguraciji sigurnosnih postavki unutar AD-a, istražujući implementaciju zaštite od poznatih prijetnji te alate i tehnike za praćenje sigurnosti AD-a i reagiranje na sigurnosne incidente. U okviru ovog završnog rada je izvšeno korištenjem Nmap-a u PowerShellu na Windows Serveru 2008 R2 mrežno skeniranje ciljane IP adrese.

Nadalje, detaljno ćemo razraditi što je sve potrebno za sigurnost, a glavni naglasak ću staviti na važnost backupa i oporavka Active Directory-a u slučaju napada te zaključiti sa sažetkom ključnih termina.

Kroz ovaj rad, cilj je pružiti praktične smjernice i preporuke koje će organizacijama pomoći u jačanju sigurnosti Active Directory-a i očuvanju integriteta informacijskih sustava.

2. ACTIVE DIRECTORY I KLJUČNI POJMOVI VEZANI UZ SIGURNOST AD-a

Kako bismo razradili temu ovog završnog rada, za početak ćemo definirati temeljne pojmove i ključne koncepte vezane uz sigurnost Active Directoryja. U ovom poglavlju obradit ću terminologiju i pojmove bitne za razumijevanje ovog završnog rada. Active Directory je Microsoftova usluga za upravljanje identitetima i resursima unutar neke organizacije. Važne komponente Active Directoryja, kao što su grupe, korisnički računi, organizacijske jedinice i domene, kao osnovne komponente AD-a, dodatno ću razraditi u ovom poglavlju, ali i kroz cijeli rad.

Osim osnovnih definicija, potrebno je razraditi i pojmove usko vezane uz autorizaciju, autentikaciju i auditiranje, jer pomoću njih možemo u potpunosti razumjeti sigurnost AD-a. Prvi ključni pojam su grupe i uloge, koje moramo analizirati unutar AD-a kako bi upravljanje pravima pristupa bilo olakšano. Ovaj pojam detaljno razrađuje način na koji koristimo grupe za grupiranje korisnika sa sličnim dozvolama i kako bismo pojednostavili upravljanje, dodavanje uloga radi maksimalnog unapređenja procesa upravljanja.

Drugi ključni pojam koji je usko vezan uz grupe i uloge su pristupne kontrole. Na temelju grupa i uloga, prema pravilima za određivanje resursa unutar AD-a, dodjeljujemo prava pristupa korisnicima. Vrlo je važno poznavati ova pravila jer su ključna za osiguravanje da osobe koje su s namjerom dobile pravo pristupa važnim informacijama i sustavima, doista i dobiju ta prava, dok osobe koje ne spadaju u određene grupe ili imaju određene uloge za koje nije predviđen pregled i pristup kritičnim sustavima ili informacijama, taj pristup imaju ograničen

Treći ključni pojam su lozinke i politike lozinki. U ovoj komponenti istražujemo važnost korištenja snažnih i sigurnih lozinki. Potrebno je razumjeti važnost učestalosti mijenjanja lozinki, njihove složenosti i duljine. Važno je da prilikom izrade lozinke koristimo kombinaciju malih i velikih slova, brojki i znakova.

Active Directory je Microsoftova tehnologija koja služi za upravljanje identitetima i pristupom u mrežnom okruženju. Sigurnost Active Directoryja ima veliko značenje u

zaštiti resursa i podataka organizacije. Neki od ključnih aspekata sigurnosti u Active Directoryju su kontrola pristupa, autentikacija, auditiranje i praćenje, grupiranje i organizacija, rezervne kopije i oporavak, nadogradnje i zakrpe te sigurnosni protokoli.

Kontrola pristupa je važna kako bi se određenim i ovlaštenim korisnicima omogućio pristup određenim informacijama. Pomoću AD-a možemo definirati i upravljati pravima pristupa korisnicima i resursima. AD nam uz kontrolu pristupa pruža i različite načine autentikacije, uključujući lozinke, pametne kartice i dvofaktorsku autentikaciju. To nam pomaže da se samo legitimni korisnici mogu prijaviti. Auditiranje i praćenje pomažu u otkrivanju sumnjivih aktivnosti ili sigurnosnih incidenata. Važno je da se pravilna organizacija i grupacija korisnika formira radi olakšavanja pristupa i sigurnosnih pravila i politika. Kod rezervnih kopija i oporavka bitno je redovito ažuriranje i stvaranje najnovijih sigurnosnih kopija i nadogradnji radi održavanja sigurnosti i sprječavanja ranjivosti. Posljednji korak su sigurnosni protokoli, jer njihova implementacija pomaže u sprječavanju napada i zaštiti osjetljivih podataka. Izvrstan primjer za sigurnosni protokol je Kerberos. Sam Active Directory može biti vrlo snažan alat za zaštitu identiteta i pristupa unutar organizacije, ali je važno obratiti pozornost na pravilno upravljanje i primjenu sigurnosnih praksi, te na redovitu provjeru i ažuriranje sigurnosnih postavki kako bi se održao integritet i pouzdanost Active Directoryja.

Dodatni aspekti AD-a uključuju višestruku faktorsku autentikaciju (MFA). Aktivacija MFA za korisničke račune u Active Directoryju otežava pristup neovlaštenim osobama. MFA je ključ za jaču sigurnost jer predstavlja sigurnosni pristup koji traži od korisnika da pruži više od samo jednog načina identifikacije, kako bi identitet bio uspješno potvrđen. Ovaj pristup, koji je malo složeniji, pruža dodatnu sigurnost u odnosu na tradicionalne metode kao što su korisničko ime i lozinka. Postoji više vrsta višestruke faktorske autentikacije, a to su dvostruka faktorska autentikacija (2FA), trostruka faktorska autentikacija (3FA) i višestruka faktorska autentikacija u oblaku. 2FA je kada korisnik autentikaciju provodi na način da koristi dvije od tri kategorije (znate, jeste, imate). 3FA je nešto složenija jer uključuje autentikaciju korištenjem sve tri kategorije, dok autentikacija u oblaku uključuje korištenje MFA u kombinaciji s cloud-based identifikacijskim rješenjima kao što je Azure MFA.

Vezano uz to, bitno je spomenuti politike lozinki, jer postavljanjem strogih lozinki i redovitim mijenjanjem starih lozinki osigurava se integritet. Nadalje, kontrola i monitoring privilegiranih računa osigurava da se privilegiranim korisnicima prati i ograničava pristup kako bi se smanjila mogućnost zloupotrebe. Iduća tema koja je vezana uz prethodne je redovno obrazovanje korisnika kako bi se informirali o sigurnosnim praksama i opasnostima internetskog okruženja, te se na taj način smanjuje rizik od socijalnog inženjeringa i drugih napada. Sigurnosni informacijski događaji omogućuju brzo otkrivanje potencijalnih incidenata te pravovremenu reakciju na njih. Nakon toga, zadnji, ali nimalo manje važan korak je sigurnosno testiranje i revizija kako bi se identificirale ranjivosti i izazovi, te brzi način njihova rješavanja.

Sama sigurnost Active Directoryja zahtijeva stalnu pažnju i brigu kako bi se očuvala provjera korisnika i osigurao integritet podataka i resursa. Kombinacija tehničkih mjera i sigurnosnih politika ključna je za uspješno upravljanje sigurnošću Active Directoryja unutar organizacije.

Kao što je prethodno navedeno, Active Directory je centralizirana usluga za upravljanje identitetima. AD organizacijama omogućuje pohranu, pristup i upravljanje resursima u mreži organizacije. AD je temeljna komponenta Microsoftovih operativnih sustava i igra ključnu ulogu u organizaciji korisničkih računa, resursa, pristupne kontrole i grupa. Organizacijske jedinice unutar AD-a su kontejneri koji organizaciji omogućuju da mrežu strukturira logički prema poslovnim jedinicama. Upravo te jedinice olakšavaju upravljanje korisnicima, računalima i grupama u skladu s hijerarhijom firme. Bitna komponenta je i Domain Controller (DC) koji je server unutar mreže s replikama podataka iz Active Directoryja, a odgovoran je za autentikaciju korisnika, autorizaciju pristupa resursima i održavanje podataka unutar domene. Još jedan protokol koji služi za upravljanje informacijama koje su pohranjene u direktoriju je Lightweight Directory Access Protocol, koji služi kao standardni protokol za komunikaciju direktorija i klijenta. Group Policy Objects predstavljaju skup postavki koje primjenjujemo na računala i njihove korisnike unutar domene. Te postavke kontroliraju sigurnosne politike, postavke sustava i druge oblike konfiguracije kojom se održava konzistentnost i sigurnost unutar pojedine organizacije. Još jedan sustav koji služi za autentikaciju je Kerberos koji omogućuje da se identitet korisnika i

računala sigurno provjeri unutar mreže. Kerberos je često korišten i spominjan pojam u Active Directoryju za osiguravanje sigurnih procesa autentikacije. Također, bitno je spomenuti i Trust Relationship, koji predstavlja povjerenje između domena u AD-u. Trust Relationship omogućuje korisnicima iz jedne domene pristup resursima koji se nalaze u drugoj domeni. Vezani pojam uz Trust Relationship je i Forest. Forest označava skup svih domena u Active Directoryju koje dijele strukturu sheme, i omogućuje organizaciji upravljanje s više domena unutar jednog zadanog okvira. Važan pojam za spomenuti su i Flexible Single Master Operations roles, koji predstavljaju pet različitih operacija za upravljanje promjenama u AD-u. Ove uloge uključuju ulogu Operations Mastera koji upravlja određenim aspektima unutar foresta i domene. Vezane uz Operations Mastera su i Security Groups koje predstavljaju skupine unutar Active Directoryja koje se koriste za upravljanje pristupom resursima. Potrebno je dodijeliti korisnike u skupine kako bi administratori mogli kontrolirati tko ima pristup nekim mapama, datotekama, dokumentima ili drugim resursima.

Zaključak ovog poglavlja je da svi navedeni pojmovi, usko povezani s Active Directoryjem, čine osnovu za upravljanje identitetima i resursima unutar organizacije. Razumijevanje svih ovih pojmova ključno je za uspješno implementiranje i održavanje Active Directory okoline, čime se osiguravaju stabilnost, dosljednost i sigurnost informacijskog sustava.

3. NAPADI, IZAZOVI I PREVENCIJA NAPADA NA ACTIVE DIRECTORY

Active Directory predstavlja ključnu komponentu informacijskih sustava u modernim organizacijama. Kako je AD u današnje doba centralizirana usluga za upravljanje identitetima, logično je da je vrlo česta meta različitih napada i napadača koji žele iskoristiti ulogu s visokom važnošću u svakoj organizaciji. Iako AD predstavlja hijerarhijski sustav za centralizirano upravljanje ulogama, grupama, korisničkim računima i pristupnim pravima unutar organizacije, složenom strukturom čini srž IT infrastrukture, a samim tim je i vrlo privlačno za napadače koji žele pristupiti upravo tim informacijama. Metode napada na Active Directory su različite. Neke od metoda su napadi na autentikaciju kada napadači pokušavaju putem neovlaštenih pristupa krađe identiteta korisnika provaliti u sustav. Druga metoda napada na AD je napad na autorizaciju. Glavni cilj ovog napada je dobivanje neovlaštenog pristupa resursima unutar Active Directory često iskorištavanjem ranjivih postavki. Treća metoda je zloupotreba privilegiranih računa. Napadači ciljaju privilegirane račune, kao što su administratorski i slični računi, kako bi dobili kontrolu nad sigurnošću Active Directorya. Iduća metoda napada je napad na sigurnosne ranjivosti koji uključuje iskorištavanje ranjivosti u softveru ili u konfiguraciji Active Directorya. Zadnja metoda napada je društveni inženjering i phishing, gdje napadači koriste manipulaciju i obmanjivanje korisnika kako bi dobili informacije koje su potrebne za napad.

Ključni napadi na Active Directory su Pass-the-Hash Attack, gdje napadači preuzimaju lozinke u obliku heševa iz memorije i koriste ih za neovlašteni pristup resursima. Idući ključni napad je Kerberos Ticket Attacks, napad na Kerberos autentikaciju, koja uključuje napade na propuste u Kerberos ulaznicama. Idući ključni napadi su Golden Ticket i Silver Ticket, gdje se stvaranjem lažnih Kerberos ulaznica omogućava napadačima proizvoljan pristup AD resursima. Idući ključni napad na AD je BloodHound napad, gdje se analizira i kartira AD okolina kako bi se otkrile ranjivosti i putovi za eskalaciju privilegija. Zadnji ključni napadi su DcShadow napadi, koji omogućavaju napadačima manipuliranje i kopiranje podataka u AD okruženju. Još neki od napada su Brute Force napadi, kojima korisnik pokušava otkriti korisničku lozinku pomoću sustavnog isprobavanja različitih kombinacija lozinke. Ovo

je najjednostavniji napad i većinom je to početna faza napada na Active Directory. Zlonamjerne grupne politike (GPO) i skriptiranje su idući napadi koji mogu iskoristiti AD GPO-e i skripte za distribuciju malicioznog sadržaja po cijeloj mreži. Zadnja vrsta napada je Token Impersonation, koji označava napad kada napadač stvori kopiju sigurnosnog tokena drugog korisnika kako bi stekao neovlašteni pristup resursima.
Svi ti napadi se mogu uz nekoliko preventivnih koraka minimizirati. Prvo je jaka autentikacija, gdje se koristi višefaktorska autentikacija koja otežava brute force napade, nakon toga je bitno i praćenje prometa. Redovitom analizom i praćenjem prometa u mreži se može brzo prepoznati napadi i sumnjiva aktivnost. Još jedan korak u prevenciji napada na Active Directory je pravilna konfiguracija privilegija, gdje je ideja da se korisniku ograniči privilegija na najmanju mjeru koja je potrebna za obavljanje određenog posla kako bi se smanjio obujam napada. Još jedan vrlo koristan korak je redovita obuka osoblja, jer upravo edukacija zaposlenika o potencijalnim prijetnjama ili prepoznavanje phishing napada i kako pravilno postupati s osjetljivim informacijama. Također, najvažnija prevencija napada, uz prethodno nabrojene, je korištenje naprednih sigurnosnih metoda. Potrebno je implementirati napredna sigurnosna rješenja, IPS/IDS sustava, firewalla, antivirusne programe i sustave za upravljanje incidentima kako bi se mreža dodatno osigurala. Nastavno na korištenje naprednih sigurnosnih rješenja je i redovito ažuriranje sustava, kako bi se održavanje svih softvera i sustava održalo standard i ispravile se ranjivosti koje su u međuvremenu postale poznate. Vrlo bitno je napomenuti da postoji konstantna potreba za testiranjem sigurnosti i pronalaženjem slabosti postojećih sigurnosnih sustava i mjera. Samo uz konstantno testiranje mogu se preciznije odrediti potrebe za poboljšanjem i reagiranjem na incidente.

Izazovi koji se pojavljuju u otkrivanju napada na Active Directory su unutarnje prijetnje, nevidljivost i privremeni napadi. Kod unutarnjih prijetnji se smatra da zaposlenici koji imaju unutarnji pristup mogu predstavljati veliki izazov, jer kod njih postoji veći potencijal za nanošenje štete Active Directory infrastrukturi. Nadalje, nevidljivost je još jedan izazov koji se pojavljuje, jer su napadi često jako teško uočljivi i vrlo suptilni. Najčešće se napadi primijete i otkriju tek dok uzrokuju značajne štete. Kako bi napadači što duže izbjegli otkrivanje napada, koriste tehnike koje su vrlo napredne i povećavaju složenost procesa identifikacije i sprječavanja. Još neki od izazova su naprednost prijetnji, jer u suvremenom dobu prijetnje i napadi postaju

sve kreativniji, sofisticiraniji i teži za uočiti. Još jedan od izazova uz nedovoljnu edukaciju korisnika mogu biti i mobilnost radne snage, s obzirom na remote pristup i korištenje mobilnih uređaja kod zaposlenika. Također, izazov je i raznolikost platformi. Kada se uzme u obzir integracija različitih platformi, kao što su Linux, MacOS i Windows, zahtijeva velike napore u osiguravanju jednake razine na svim nabrojanim sustavima.

Active Directory svakodnevno evoluira kako bi se prilagodio modernom poslovanju. Samim tim rastom se svakodnevno povećava potreba za testiranjem sustava i njegove sigurnosti. Ključno je prilagoditi strategiju kako bi odgovor na prijetnje i napade bio pravovremen i odgovarajući. Ono što je budućnost za sigurnost Active Directorya je umjetna inteligencija, jer upravo AI nam može pomoći u detekciji prijetnji i pokretanju automatskog odgovora, tj. reakciju na novu vrstu napada. Idući korak u budućnosti sigurnosti AD-a je Zero Trust arhitektura koja se bazira na ideji da niti jedan uređaj ili identitet unutar mreže po defaultu nije pouzdan i samim tim potiče na dodatne razine verifikacije. Posljednje su Blockchain i biometrija jer integracijom ova dva pojma se može dodatno ojačati autentikacija korisnika.

Zaključak ovog poglavlja je da je upravo Active Directory temelj sigurnosti modernog poslovanja. Samim time što svakodnevno neprestano se događaju promjene i novi izazovi sigurnosti informacijskog sustava, potrebno je blagovremeno reagirati i konstantno biti u korak sa promjenama koje se događaju, a utječu na ranjivost AD-a. Ključno je da se sigurnosne strategije prilagode kako bi se suvremene prijetnje minimizirale ili barem pravovremeno otkrile, te kako bi se očuvala sigurnost podataka.

Ono što je bitno u Active Directory-u je da za suvremene prijetnje imamo suvremene odgovore u slučaju ispada i incidenata, a sve to se može postići višefaktorskim autentikacijama, Zero Trust pristupom i korištenjem umjetne inteligencije kao pomoći u otkrivanju napada. Kako bi se očuvala sigurnost Active Directory-a, treba korisnike educirati, te pratiti najnovije trendove u kibernetskoj sigurnosti i tehnologiji.

1.1. Primjeri napada u Active Directory infrastrukturu

Kako bi bila jasnija štetna posljedica napada i sam cilj određenog napada, u nastavku ćemo proći kroz neke osnovne napade i njihove ciljeve. Najčešći napad je pokušaj kombinacija lozinki i korisničkih imena, Brute Force, zatim Pass-the-Ticket, Token Impersonation i slični napad.

1.1.1. Brute force

Brute Force napadi na autentikaciju su kada napadač koristi automatizirani alat koji kontinuirano isprobava različite kombinacije korisničkih imena i lozinki sve dok ne pronađe ispravnu kombinaciju. Brute Force predstavlja jedan od najučestalijih i samim time najjednostavnijih oblika napada na sustav. Ovaj oblik napada je posebno važan u kontekstu Active Directory infrastrukture jer korisnički računi i pripadajuće lozinke predstavljaju ključni element u sigurnosti. Brute Force ima 4 faze: faza 1 - identifikacija cilja, faza 2 – pronalaženje korisničkih imena, faza 3 – Brute Force napad i faza 4 – otkrivanje ispravnih autentikacijskih podataka. U prvoj fazi napadač mora identificirati ciljani resurs ili sustav unutar Active Directory infrastrukture gdje želi dobiti pristup. U fazi 2 napadač koristi različite tehnike kako bi došao do korisničkih imena unutar domene. Napadači koriste različite tehnike za skeniranje mreže ili socijalni inženjering. U fazi 3 napadači koriste automatizirane alate koji sustavno isprobavaju kombinacije lozinki za svako korisničko ime koje su pridobili u drugoj fazi. U posljednjoj fazi gdje se otkrivaju ispravni autentikacijski podaci, napadač dobiva pristup ciljanom računu i resursima unutar Active Directory-a.

Posljedice Brute Force napada su kompromitiranje korisničkih računa, povećan je rizik od unutarnjih prijetnji i gubitak povjerenja korisnika. Kada se dogodi uspješan Brute Force napad, omogućuje napadaču pristup korisničkim računima, što se klasificira kao neovlašten pristup osjetljivim ili povjerljivim informacijama. Druga posljedica, kao povećani rizik od unutarnjih prijetnji, događa se dok napadač stekne kontrolu nad privilegiranim korisničkim računima; tada se povećava rizik od neovlaštenih promjena u konfiguraciji Active Directory-a ili se može dogoditi distribucija zlonamjernih skripti. Zadnja, ali jednako važna, posljedica napada je gubitak povjerenja korisnika, jer ti napadi često rezultiraju zaključavanjem korisničkog računa zbog velikog broja pokušaja prijave. Nakon što korisnik ostane "zaključanog" računa, dolazi do frustracije, preispitivanja povjerenja, te čak i do potpunog gubitka povjerenja u sustav.

Brute Force napadi se mogu spriječiti na različite načine, a neki od najpoznatijih su već prethodno spomenuti, kao što su višefaktorska autentikacija (MFA), blokiranje IP adresa, jačanje lozinki i praćenje logova s uzbunjivanjem. Kod višefaktorske autentikacije dodan je dopunski sloj autentikacije koji znatno otežava Brute Force napad jer pored korisničkog imena i lozinke postoje i drugi autentikacijski faktori. Automatskim blokiranjem IP adresa koje izvode velik broj pokušaja autentikacije se može otežati ili čak i onemogućiti napad. Jačanje lozinki je osnovna razina prevencije koju bi svaki korisnik trebao imati na umu pri kreiranju lozinke. Jake i zahtjevne lozinke mogu značajno smanjiti uspjeh napada.

Dakle, kako bi se minimizirala uspješnost Brute Force napada, potrebno je stvoriti snažnu obranu protiv kibernetskih prijetnji. Prevencija tih napada zahtijeva kombinaciju edukacije korisnika, tehnoloških rješenja i politike sigurnosti.

1.1.2. Pass-the-Ticket napad

Ovaj napad predstavlja sofisticiranu prijetnju sigurnosnih sustava u kontekstu Active Directory infrastrukture. Ovaj napad konkretno cilja na Kerberos autentikaciju, jer se zloupotrebljuju Kerberos tiketi kako bi se omogućio neovlašten pristup resursima. Pass-the-Ticket napad funkcionira na način da se koristi Kerberos, koji je sustav za

autentikaciju koji koristi tajne ključeve za provjeru identiteta korisnika i servera. Zatim, u trenutku kada se Kerberos tiket šalje između korisničkog računala i domain controllera, napadač pokušava presresti tiket prilikom autentikacije. Kada se to presretanje tiketa uspješno dogodi, napadač ga može zloupotrijebiti na brojne načine, a najčešći način upotrebe je stvaranje "Golden Ticketa" ili lažnih tiketa. Lažni tiket se može stvoriti sa podacima o tajnom ključu iz tiketa kojega je presreo. Golden ticket je tiket koji omogućava dugotrajne privilegije. Iduća faza je da napadač dobiva neovlašten pristup resursima Active Directory infrastrukture, a taj pristup uključuje korisničke račune koji imaju velike privilegije. Posljedice napada su povećani rizik od neotkrivenih napada, kompromitiranje privilegiranih računa i narušavanje integriteta podataka. Pass-the-Ticket napadi su često neotkriveni zbog korištenja lažnih tiketa, a njih je teško detektirati konvencionalnim sigurnosnim alatima. Ako napadač uspije stvoriti lažni tiket sa privilegijama administratorskog računa, napadač može preuzeti potpunu kontrolu. Nakon što se to dogodi, napadač može uređivati, mijenjati, brisati i kopirati povjerljive podatke u Active Directory-u, što dovodi do ozbiljnog narušavanja integriteta podataka i organizacije. Prevencija takvih napada može se odviti na 4 načina, implementacijom višefaktorske autentikacije (MFA), pravilnim konfiguriranjem Kerberosa, praćenjem i analiziranjem logova, te redovitim ažuriranjem i zakrpama. Kod implementacije višefaktorske autentikacije dodaje se dodatan sloj autentikacije, čime se otežava uspjeh PtT napada jer napadači moraju presresti i zloupotrijebiti više faktora. Kod pravilne konfiguracije Kerberosa, uključujući pravilno postavljanje tajnih ključeva i revizije postavki, što može otežati napad. Praćenje i analiza logova autentikacije dovodi do detekcije neobičnih aktivnosti kada se stvaraju lažni tiketi. Redovitim ažuriranjem i promjenama na sustavima smanjuje se rizik od iskorištavanja starih i poznatih ranjivosti koje PtT napadači mogu koristiti. Zaključak je da PtT napadi predstavljaju veliku prijetnju sigurnosti Active Directory infrastrukture. Prevencija zahtijeva kombinaciju tehnoloških rješenja, praćenja aktivnosti i konfiguracijskih pravila kako bi se otkrili potencijalni napadi.

3.2.3. Token Impersonation

Dubliranje identiteta u sustavima sa tokenima predstavlja sofisticiranu tehniku kibernetskog napada koja je fokusirana na zloupotrebu tokena s neovlaštenim pristupom sustavima. Ova vrsta napada se vrlo često koristi u okruženjima koje imaju višestruke korisničke privilegije, kao što su sustavi koji koriste Windows Security Tokens. Token Impersonation funkcionira na način da sustavi koji koriste autentikaciju kao što su Windows Security Tokens generiraju sigurnosne tokene. Nakon uspješne autentikacije, korisniku se dodjeljuje sigurnosni token s kojim potvrđujemo njegov identitet i omogućuje pristup određenim resursima. Nakon toga, napadači pokušavaju presresti ili duplicirati sigurnosni token kako bi postali vlasnici identiteta drugog korisnika s više privilegija. Kada napadač nakon toga uspješno zloupotrijebi token, može djelovati u sustavu s ovlastima identiteta korisnika čiji je token duplicirao. Primjer napada je manipulacija Kerberos tiketima, ugrožavanje sesija ili Pass-the-Token.

4. SIGURNOSNE PRAKSE I POLITIČKE SMJERNICE

Kao što je ranije spomenuto, Active Directory je temeljni sustav pomoću kojeg upravljamo identitetima u pojedinoj organizaciji s ciljem očuvanja sigurnosti. Kada se implementiraju adekvatne sigurnosne prakse i uskladi s aktualnim i bitnim političkim smjernicama, tada AD igra ključnu ulogu u očuvanju integriteta i sprječavanju prijetnji. Kada implementiramo odgovarajuće sigurnosne prakse u Active Directory-u uz pomoć pravnih odredbi, tj. Zakona u državi u kojoj se organizacija nalazi, osigurava se pravna zaštita podataka i informacijske sigurnosti. U Republici Hrvatskoj postoji Zakon o sigurnosti mreža i informacijskih sustava, Zakon o zaštiti osobnih podataka i drugi relevantni zakoni koji su usko vezani uz temu sigurnosti.

Pravilna konfiguracija višestrukih faktora autentikacije (MFA) je ključna sigurnosna praksa gdje implementacija značajno povećava razinu sigurnosti autentikacije u Active Directory-u, jer MFA traži od korisnika dodatne informacije i korake u zaštiti osim korisničkog imena i lozinke. Druga dobra praksa je upravljanje pravima pristupa jer ograničavanje pristupa pojedinim resursima osigurava da se izbjegne pristup informacijama, datotekama i poslovnim pravima koji nisu predviđeni za određenog korisnika. Treća dobra praksa je prakticiranje praćenja logova jer praćenjem logova možemo brže identificirati sumnjive aktivnosti. U ovoj sigurnosnoj praksi potrebna je prilagodba politika praćenja logova prema zakonima koji definiraju vremenski rok čuvanja, obvezu čuvanja i analize podataka o sigurnosnim incidentima. Četvrta dobra praksa je redovito ažuriranje koje pomaže u smanjenju ranjivosti. Redovitim ažuriranjem ne dajemo napadačima dovoljno vremena da istraže ranjivosti trenutnog sustava, već ih stalno otežavamo. Zakon koji uređuje ovu praksu propisuje obvezu primjene zakrpi kako bi se očuvala sigurnost informacijskih sustava. Peta dobra praksa je edukacija korisnika kojom smanjujemo mogućnost ljudske pogreške i rizika socijalnog inženjeringa. Prema zakonima o sigurnosti informacijskih sustava i obuci zaposlenika, treba zaposlenike na odgovarajući način educirati o sigurnosti. Šesta dobra praksa je implementacija sigurnih postupaka za upravljanje korisničkim identitetima unutar organizacije. S obzirom na brojne zakone koji reguliraju prava pojedinca na zaštitu identiteta i privatnost, treba uključiti mjere zaštite identiteta. Sedma dobra praksa, koja je posebno zanimljiva, je korištenje kriptografije kako bi se zaštitila komunikacija između drugih sustava i Active Directory-a. Zakoni i političke

smjernice koje reguliraju ovu praksu su zakoni o sigurnosti elektroničkih komunikacija i šifriranja poruka

Dakle, ovo poglavlje bi mogla zaključiti tvrdnjom kako sigurnost informacijskog sustava, koja je i pravno uređena zakonima, ima vrlo važna uloga u očuvanju integriteta organizacije. Zaštita podataka i informacijske sigurnosti uz pravnu usklađenost koji uz tehnološka rješenja, edukaciju korisnika i pridržavanjem pravnih smjernica je ključ stvaranje usklađenog i sigurnog Active Directory okruženja.

5. TEHNIČKE MJERE SIGURNOSTI I KONFIGURACIJA SIGURNOSNE POSTAVKE U ACTIVE DIRECTORY-U

Kao što je već prethodno bilo spomenuto, Active Directory u mnogim organizacijama zahtijeva implementaciju nekih tehničkih mjera sigurnosti kako bi osigurali zaštitu osjetljivih podataka, korisničkog identiteta i resursa. U tekstu dalje ćemo proći opsežan niz tehničkih mjera sigurnosti u sklopu Active Directory-a, ali ipak uzimajući u obzir održavanje integriteta, dostupnosti i povjerljivosti podataka.

Prva mjera sigurnosti, koja nam je već poznata od ranije, višefaktorska autentikacija ili MFA nam osigurava dodatan sloj sigurnosti kod autentikacije, jer zahtijeva više od jednog koraka pri autentikaciji korisnika. Prednosti MFA su što je povećana otpornost na napade kojima je cilj krađa korisničkih podataka jer otežava pristup čak i u slučaju ako napadač uspije prikupiti lozinke korisnika. Druga mjera sigurnosti je stroga kontrola pristupa jer se koristi inače princip najmanjih privilegija za kontrolu pristupa resursima. Prednost druge mjere je što je rizik od pristupa neovlaštenim informacijama minimiziran. Treća mjera je enkripcija podataka, koja služi za zaštitu podataka tijekom prijenosa i mirovanja, a podrazumijeva i podatke i informacije koje su pohranjene u nekom obliku, kao što su na disku. Prednost ove mjere sigurnosti je jer se smanjuje rizik neovlaštenog pristupa osjetljivim podacima. Tijekom prijenosa podataka je povjerljivost informacija održana, a samim time se i osjetljive informacije štite od neovlaštenog korištenja i pristupa. Četvrta tehnička mjera je praćenje i logiranje, koje postavlja sustav za logiranje i praćenje aktivnosti koje se događaju unutar Active Directory-a. Prednost je što se logiranjem i praćenjem omogućava brza detekcija aktivnosti ili čak neovlaštenog pristupa. Samim logiranjem i praćenjem se prikupljaju podaci za analizu sigurnosnih incidenata i izvješća. Peta mjera sigurnosti je periodičko ažuriranje sustava i aplikacija kako bi se izbjeglo prepoznavanje i iskorištavanje ranjivosti. Prednosti ove mjere su što se smanjuje rizik iskorištavanja propusta koji su poznati napadačima, a samim tim i poboljšava otpornost na napade. Šesta mjera tehničke sigurnosti je kreiranje sigurnosnih kopija (backup) koja osigurava da se uz pomoć redovitog izrađivanja sigurnosnih kopija podataka, omogući brži oporavak od gubitka podataka i sprječavanje trajnog gubitka važnih

informacija. Još jedna od mjera tehničke sigurnosti je sigurnosna politika lozinki kojom se traži da lozinke budu kompleksnije, redovito se mijenjaju i zabranjuje se korištenje istih lozinki na različitim mjestima. Ova mjera napadačima otežava pogađanje lozinki, a samim tim i povećava razinu sigurnosti autentikacije. Posljednja mjera tehničke sigurnosti su sigurni kanali komunikacije i virtualne privatne mreže (VPN) koji služe kao zaštita od neovlaštene manipulacije kanalima u prijenosu i od neovlaštenog prisluškivanja. Ovom mjerom se osjetljive informacije štite od napada na mrežni promet.

Koraci za zaštitu identiteta i resursa su vrlo slični kao i tehničke mjere sigurnosti, a odnose se na Višefaktorsku autentikaciju (MFA), upravljanje pravima pristupa, enkripciju podataka, praćenje i logiranje, periodičko logiranje sustava, sigurnosnu politiku lozinki i sigurnosne kopije, tj. backup i na kraju implementacija sigurnih kanala za komunikaciju.

Konfiguracija sigurnosnih postavki u Active Directory-u teži ka pažljivom pristupu i sustavnim implementacijama kako bi visoka razina sigurnosti postojala u organizaciji u kojoj se implementira zaštita i visoka razina sigurnosti. Konstantnim obrazovanjem timova smanjuje se mogućnost ljudskog faktora, tj. pogrešaka. Ukoliko su timovi stalno obrazovani i educirani, bit će stalno svjesni prijetnji koje vladaju i kako izbjeći pogreške koje bi kompromitirale sigurnost sustava neke organizacije.

5.1. Implementacija zaštite od poznatih prijetnji

Kada govorimo o implementaciji zaštite od prijetnji koje su već prethodno poznate u Active Directory-u, govorimo o pristupu koji treba kombinirati organizacijske, edukativne i tehničke mjere. Neki od ključnih koraka za zaštitu od poznatih prijetnji su ažuriranje sustava i aplikacija, antivirusna i antimalware rješenja, firewall i kontrola mrežnog prometa, web filteri, sistemi praćenja logova i detekcija prijetnji, edukacija i obuka korisnika, korisničke politike i sigurnosne smjernice, te redovite revizije sigurnosnih postavki.

Prilikom ažuriranja operativnog sustava, servisnih paketa i aplikacija kod operativnog sustava, pomaže se u elimininiranju napada sa sigurnosnim propustima. Što se implementacije tiče, automatsko ažuriranje treba biti na svim sustavima kako bi se izbjegla mogućnost ljudske pogreške i nepravovremenog ažuriranja. Dostupnost novog ažuriranja treba biti redovito provjeravana, a samim tim treba primjeniti sigurnosne zakrpe. Za antivirusna i antimalware rješenja preporuča se korištenje programa koji su pouzdani u rješavanju, otkrivanju i neutralizaciji programa sa zlom namjerom. Redovito treba instalirati i ažurirati antivirusne programe, te podesiti redovito skeniranje datoteka i sustava. Kod korištenja Firewalla i kontrole mrežnog prometa je zanimljivo da upravo pomoću ova dva pojma pomažemo u sprječavanju neovlaštenog pristupa i širenja prijetnji putem mreža. Firewall treba konfigurirati na način da se blokira sav promet koji je nepotreban, a sustav treba postaviti tako da se prati i analizira mrežni promet. Korištenjem web filtera omogućava se blokiranje pristupa stranicama i preuzimanje datoteka koje su maliciozne, a kako bi se to spriječilo, u početku odmah treba blokirati pristup već od prije poznatim malicioznim stranicama. Također, treba omogućiti filtriranje i skeniranje web sadržaja. Vezano za to je praćenje logova i detekcija prijetnji što uvelike pomaže u detekciji i reakciji na aktivnosti koje bude sumnju. Kao prvi korak, sustav za praćenje logova treba konfigurirati na način da sav fokus bude usmjeren na aktivnost koja bude ukazivala na poznate prijetnje. Zatim se treba implementirati sustav koji će detektirati prijetnju koja koristi analizu ponašanja, heuristiku i potpise. Zatim, ono o čemu neprestano govorimo, edukacija i obuka korisnika jer upravo nam to pomaže u smanjenju ljudske pogreške i da se izbjegnu poznate prijetnje kao što je phishing. Redovito treba organizirati obuke o sigurnosti i stimulirati napad kako bi napravili procjenu znanja

korisnika. Još jedan korak su korisničke politike i sigurnosne smjernice koje pomažu u definiranju standarda i praksi za koje se smatra da su najbolje. Treba razviti dokumentirane smjernice gdje će korisnik u svakom trenutku moći provjeriti korake koje treba preduzeti, a lozinke treba redovito ažurirati i mijenjati kako bi održali sigurnost i prava pristupa. Kao zadnji korak je bitno napomenuti da treba raditi redovite revizije sigurnosnih postavki kako bi se periodički evaluirala razina sigurnosnih postavki, kako bi se uvjerili da je i dalje učinkovito. Treba planirati revizije unaprijed, a također treba ažurno pratiti preporuke za sigurnost.

Dakle, zaključak je da je potrebno napraviti visokoučinkovitu implementaciju zaštite od poznatih prijetnji u AD-u, a to obuhvaća vještine i aspekte na kojima se mora svakodnevno raditi i unaprijeđivati kako bi pratili otkrivanja slabosti implementiranog sustava.

6. ALATI I TEHNIKE ZA PRAĆENJE SIGURNOSTI ACTIVE DIRECTORY

Kao što je već prethodno više puta spomenuto, sigurnost Active Directorya ima veliku važnost u informatičkom sustavu mnogih firmi i organizacija. Kako bi se održala zadovoljavajuća razina sigurnosti i njeno neprestano održavanje, važno je koristiti alate i tehnike koji nam pomažu u praćenju sigurnosti, te analiziranju same potrebe za praćenjem, a naposljetku identificiranje potencijalnih prijetnji ili slabosti sustava. Definicija Active Directory-a, laički i najjednostavnije rečeno, predstavlja centraliziranu bazu podataka u kojoj se nalaze brojne i razne informacije o svim sudionicima u razmjeni podataka, a to su korisnici, zaporka, identifikacijski podaci, računala, resursi, povjerljive informacije i drugi entiteti u mreži. Kada uzmemo u obzir sve nabrojene sudionike u razmjeni podataka i same podatke, s jednostavnošću se da zaključiti da ugrožavanjem Active Directory-a za organizaciju može značiti ozbiljan gubitak podataka s vrlo ozbiljnim posljedicama. Samu prijetnju za sigurnost AD-a mogu predstavljati čak i zaposlenici organizacije, koji ljudskim pogreškama ili nedovoljnim informiranjem mogu ugroziti i "otvoriti put" napadačima. Upravo zbog tih razloga nam praćenje daje mogućnost analize, pregleda i identifikacije slabosti. Nakon identifikacije slabosti ili nepravilnosti, možemo osigurati brzu reakciju na otklanjanje potencijalnih nepravilnosti i slabosti. Samom konstantnom analizom i praćenjem neprestano se može održati otkrivanje i otklanjanje nepravilnosti i pomoći u održavanju standarda.

Alati za praćenje sigurnosti AD-a se mogu podijeliti u automatizirane tehnike, logičko i fizičko praćenje. Automatizirane tehnike koriste automatizirane alate koji osiguravaju konstantno praćenje i samim tim osiguravaju brzu reakciju na moguće incidente. Kod logičkog nadzora se mogu izvršavati audit logovi i SIEM. Audit logovi predstavljaju evidentiranje aktivnosti i događanja koja se izvršavaju na mreži, u sustavu ili aplikaciji. Audit logovi su vrlo korisna tehnika kojom se može identificirati nepravilnosti i održati sigurnosni standardi, a audit logovi nam daju uvid u sve bitne aktivnosti vezane uz korisnike, grupe, resurse, druge objekte i slično. U audit logovima se bilježe aktivnosti kao što su prijava korisnika, promjene unutar grupa kao što su dodavanje ili brisanje članova, promjena prava pristupa određenim

informacijama i odjave korisnika. Bitno je pratiti tko, što, kako i u koje vrijeme se služi resursima Active Directorya. Praćenjem ovih vrsta aktivnosti se mogu identificirati nepravilnosti i sumnjive aktivnosti kao što su pokušaj promjene ili dodjeljivanje prava za određenu grupu korisnika, neuspjeli pokušaj prijava, neuspjeli pokušaj pristupa informacijama i slično. Mnoge organizacije imaju određene regulative, politike i sigurnosne standarde, a pomoću audit logova prati se jesu li te regulative pridržavane jer je to ključno za održavanje sigurnosnih standarda. Pomoću audit logova se mogu kreirati brojni izvještaji kojima se mogu osigurati povećanje performansi sustava, otkrivanje trendova i identifikacija problema. Također treba imati na umu da se i sami audit logovi trebaju pravilno zaštiti kako bi se onemogućilo brisanje logova ili manipulacija zabilježenim podacima.

Zatim još jedan od alata vezanih uz logičko praćenje je SIEM ili Security Information and Event Management koji predstavlja složeni i kompleksan sustav kojim pratimo, analiziramo i reagiramo na sigurnosne događaje u stvarnom vremenu. SIEM sustav analizira podatke iz nekoliko različitih izvora kako bi se potencijalna prijetnja identificirala i kako bi odgovarajući timovi mogli poduzeti ključne korake u zaštiti integriteta podataka. Prikupljanje podataka iz nekoliko izvora uključuje prikupljanje logova operativnih sustava, mrežnih podataka, logova aplikacija, mrežnih uređaja i sigurnosnih sustava, a informacije iz ovih izvora se prikupljaju na jednom mjestu kako bi se dalje mogle izvršiti analize svih prikupljenih podataka. Analiza u stvarnom vremenu je jako važna jer iako je kasnije otkrivanje korisno, iznimno je važno da se u stvarnom vremenu otkrije prijetnja ili aktivnost kako bi odgovarajućim mehanizmima se obranilo od napada.

6.1. Detekcija i reagiranje na sigurnosne incidente

Kako živimo u digitalnom dobu, kada je uobičajeno i čak preporučljivo koristi i oslanjati se na informacijske mreže i sustave, te samim tim sigurnost postaje osnova takve vrste poslovanja. Sa sve većim razvojem tehnologije i konstantnim naporima da se korisnicima osigura kvalitetan i siguran sustav za poslovanje, pojava sigurnosnih prijetnji je postala skoro neizbježna pojava. Pošto je za detekciju sigurnosnih incidenata bitno da se reagira skoro u pravo vrijeme.

Detekcija sigurnosnih prijetnji podrazumijeva da se pomoću nekoliko koraka ili preporuka, ta detekcija može biti brža i ograničiti pristup. Kod analize ponašanja pratimo uobičajeno ponašanje korisnika i sustava i upravo to je velika pomoć za detekciju neobičnih aktivnosti. Korištenjem ovog pristupa u detektiranju prijetnji uvelike pomaže i smanjuje „lažne uzbune“ kod detekcije. Bitno je spomenuti i korelaciju podataka, s tim da moramo imati na umu da integracija informacija iz nekoliko područja, kao što su logovi, spajanje podataka iz mrežnih sustava, uređaja i aplikacija kako bi se moglo usporediti uobičajne podatke sa onima koji nisu. Također je bitno pratiti Threat Intelligence izvora koji organizacijama pomaže predvidjeti i zatim detektirati nove prijetnje. Sve informacije o napadima, potencijalnim rizicima i zlonamjernim IP adresama su korisne kako bi se minimizirala mogućnost za ponavljanja istog napada. Korištenje alata za detekciju i implementacija IDS-a (Intrusion Detectio System) i IPS-s (Intrusion Prevention System) te brojni antivirusni programi i drugi alati za detekciju i prepoznavanja različitih vrsti prijetnji. Ovi sofisticirani alati mogu raditi analizu prometa, identificirat neke potencijalno zlonamjerne aktivnosti i ukoliko se trigerira sumnja na nedozvoljene aktivnosti, mogu pokrenuti određene korake za zaštitu sustava. Samim tim detekcija tih nepravilnosti u mrežnom prometu mogu ukazati na pokušaje napada ili neautorizirani pristup. Kada se poveća razina prometa prema resursima ili broj upita koji se izvršavaju, za alate to može značiti prijetnja i pokrenuti proces zaštite.

Vrlo bitno je kakva je reakcija na sigurnosne prijetnje. Ono što je vrlo bitno je da treba biti jasno definiran plan u slučaju incidenta (IRP Incident Response Plan) koji točno definira korake koji se moraju poduzeti u slučaju nekog incidenta. Taj plan treba imati detaljan opis, korake za analizu, identifikaciju, suzbijanje i oporavak od incidenta. Vezano za plan u slučaju incidenta su važni i automatski odgovori koji u slučaju napada pruža brze reakcije na poznate prijetnje. Tako na primjer alat može u slučaju

velikog broja upit blokirati IP adresu sa koje upiti dolaze. Na taj način ograničava štetu ili poduzima drukčije korake koji pomažu u očuvanju sigurnosti sustava. Kod suradnje i komunikacije unutar odjela neke organizacije podrazumijeva da svi bitni sudionici budu obavješteni i svijesni incidenta, te da se prema tome poduzmu odgovarajući koraci i donesu odgovarajuće odluke. Forenzička analiza je idući korak koji se događa nakon incidenta, a pomaže nam u prepoznavanju uzroka, metode napada i do kojeg obujma štete je došlo. Ove informacije su vrlo korisne i kasnije služe za poboljšanje sigurnosti i sprječavanje incidenata koji se mogu ponoviti ili dogoditi koristeći prethodni napadi. Nakon svih ovih poduzetih koraka je također bitno i pratiti performanse sustava, te ih analizirati kakva poboljšanja bi bila odgovarajuća u budućnosti. Dakle, sama detekcija i reagiranje na sigurnosne prijetnje su ključni koraci u obrani organizacije od cyber prijetnje. Kombinacijom tehničkih alata, educiranog osoblja, suradnje i stope pripreme organizacija ima vrlo važnu ulogu u očuvanju organizacija u slučaju napada ili otkrivanja prijetnji.

7. PLANIRANJE ZA SIGURNOST

Živimo u suvremenom dobu gdje se svi životni čimbenici vežu uz tehnologiju i neprestano smo obasipani novim izmjenama, ažuriranjima i upgrade-ima. Svim tim napretkom su i organizacije krenule sa prihvaćanjem tog načina rada. S obzirom da su organizacije s tim načinom rada otvorile novi put napadačima kako bi mogli iskoristiti slabosti sustava. Upravo zbog tih razloga je bitno dobro isplanirati kako se zaštititi i ponašati u slučaju napada. Proces planiranja u slučaju napada se ne treba odnositi samo na tehničke aspekte, već na umu treba imati ljude, procese i tehnologiju. Samo kombinacijom svih čimbenika i dionika je moguće isplanirati potencijalno dobar plan u slučaju napada, ali i za očuvanje sigurnosti. Svaki od navedenih čimbenika ima vrlo važnu ulogu kako bi se održala stabilnost u digitalnom okruženju.

Dakle, kako bi započeli sa planiranjem, prvo je važno razumijeti okolinu i napraviti analizu rizika te riješiti pravna pitanja. Analiza rizika je prvi korak kod sigurnosti jer detaljni izvještaji mogu pomoći u identifikaciji prijetnji, ranjivosti sustava i procjeni koje točno utjecaje to može imati na poslovanje, te sa svim tim informacijama možemo prioritizirati koje akcije su najvažnije za poduzeti prve. Nakon toga je bitno da se uskladi sa zakonima, regulativama i standardima. Kako bi pravne regulative ogranizacije mogle pratiti izgradnju sigurnosnih politika, važno je njihovo proučavanje.

Nakon što smo razumjeli okolinu i riješili pravno pitanje, trebamo definirati sigurnosne politike i podići razinu edukacije zaposlenika. Kod sigurnosnih politika se očekuje jasno formuliranje za očekivanje ponašanje zaposlenika, te pruža smjernice za zaštitu resursa organizacije. Kod edukacije zaposlenika je bitno da svi budu upućeni o kibernetičkoj sigurnosti, phishing napadima i raznim sigurnosnim prijetnjama i kako ih izbjeći.

Kod tehničkih mjera važno je napomenuti praćenje i detekciju, te upravljanje pristupima i identitetom. Praćenje i detekcija se odvija pomoću alata koji nam pomažu u detekciji aktivnosti koje nisu uobičajne. SIEM sustavi, analiza logova i drugi alati su ključni za reakciju i detekciju prijetnji. Kod upravljanja identitetima i pristupom je bitno implementirati sustav koji kasnije pomaže u kontroli tko ima pristup čemu i kada i zašto se to bude ili već je promijenilo. Kod upravljanja identitetima i

pristupom ima nekoliko metoda koje mogu otežati napad, a jedna od njih je višerazinska autentikacija koja onemogućuje pristup napadaču korištenjem samo korisničkog imena i zaporke, već korisnik mora napraviti uz to dodatne korake kako bi se uspješno prijavio u sustav.

Ono što bi svaka organizacija trebala imati je plan za postupanje u slučaju incidenta, koji će opisivati sve korake koji se trebaju poduzeti ako se dogodi sigurnosni incident. Upravo nam planiranje unaprijed u takvim slučajevima pomaže da reakcija bude brza i koordinirana u trenucima kada je to potrebno, a ne da se trenutku kada se događa incident smišlja ili pokušava napraviti nešto što nije predviđeno u planu. Ovakve situacije se donekle mogu kontrolirati na način da se timovi educiraju i osposobe kako bi za vrijeme incidenata bili maksimalno smireni i znali kako postupiti. Samo vježbom i testiranjem se mogu identificirati slabosti, greške i nepreciznosti u planu. Kada konstantno plan testiramo i procjenjujemo njegovu efektivnost, dolazimo do zavidne razine spremnosti za incident. Uz temu testiranja nam je vezana iduća tema, a to je redovito ažuriranje sustava koji podrazumijeva održavanje i zakrpe. Svaki sustav ima sigurnosne rupe, a upravo one su cilj napadača. Ako mi te rupe redovito ažuriramo i održavamo, smanjujemo rizik da napadač iskoristi te rupe jer su upravo one „slaba točka“ ulaska u sustav. Uz ažuriranja i održavanja je vrlo bitno i pratiti nove tehnološke trendove. Praćenjem ovih trendova omogućuje da se na vrijeme implementira novo rješenje, kako bi se testiralo i kako bi se sigurnost još poboljšala. U današnje vrijeme kada je sve digitalizirano, upravo plan za sigurnost postaje temeljno za uspješno poslovanje jer organizacije kada pažnju usmjere na razumijevanje rizika, usklade i primjene pravilnike i zakone, educiraju svoje zaposlenike, donose tehničke mjere i slično, odaju dojam stabilnog i sigurnog digitalnog okruženja. Redovitim ažuriranjem planova i sustava, dinamična priroda sigurnosnog sustava se osigurava da napadačima skratimo vrijeme potrebno za pronalazak „slabe točke“ sustava kroz koji bi uspjeli izazvadi sigurnosnu prijetnju.

7.1. Backup i oporavak Active Directory-a u slučaju napada

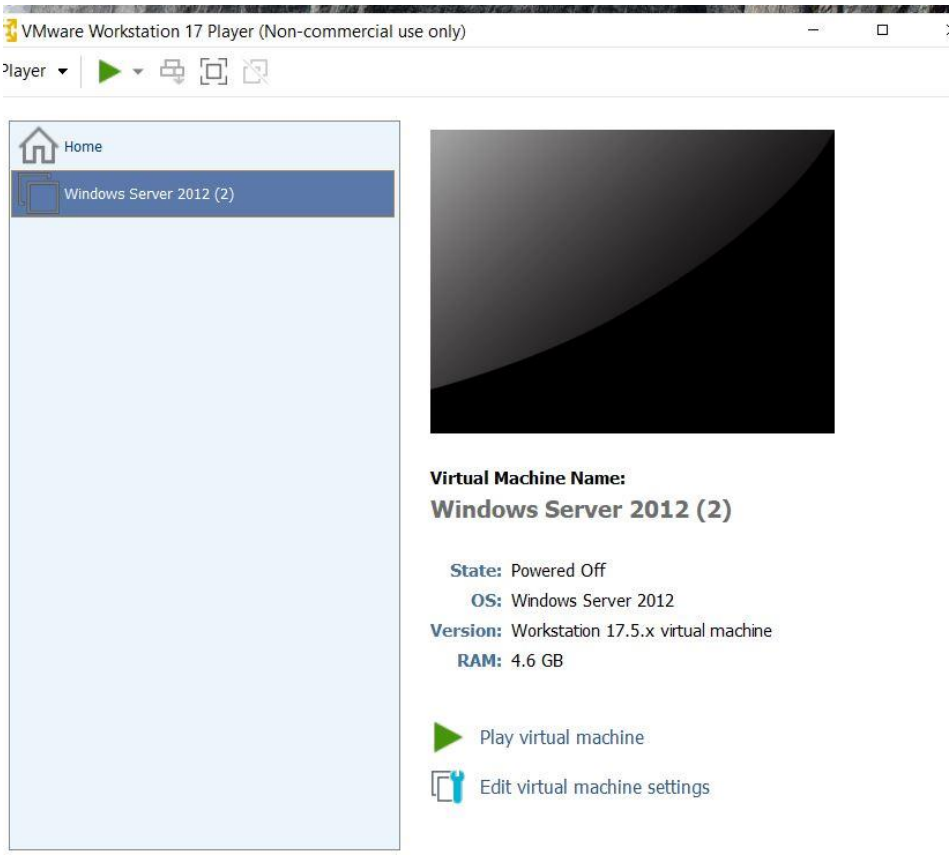
Backup i oporavak AD-a je od velike važnosti za osiguravanje nastavka poslovanja u slučaju napada, pogreške ili problema sa infrastrukturom. Kontinuitet poslovanja se mora osigurati na način da je organizacija nakon incidenta spremna za nastavak sa radom. Planovi oporavka često uključuju redovite backup procedure, nakon toga testiranje toga i definiranje koji koraci će se poduzeti u slučaju nužde. Backup se treba redovito planirati i periodički izvršavati kako bi se osiguralo i očuvalo trenutno stanje podataka. Veličina i kompleksnost organizacije igraju veliku ulogu u odluci u kojem vremenskom intervalu će se odrađivati backup, dnevno, tjedno ili prema vremenskim intervalima koji se dogovore. Nakon što se backup napravi, treba se redovito pregledavati kako bi se osigurala cjelovitost i ispravnost podataka, a u kontroliranim uvjetima je to ključno da se stekne potvrda da ukoliko dođe do incidenta i moraju se stvarno koristiti podaci sa backupa, da su ti podaci ispravni i cjeloviti. Također, backup podaci također trebaju biti zaštićeni od neovlaštenog pristupa. Kriptiranje backeupa i kontrolni pristup su ključni za očuvanje sigurnosti.

Oporavak Active Directory-a se odvija uz pomoću nekoliko koraka. Prvi korak je da se napravi ispravan oporavak iz backupa, jer je u slučaju napada ključno da neka organizacija svoje podatke može ispravno povratiti. Prvo treba definirati iz kojeg backeupa se podaci budu vraćali i koristili. Nakon ovog koraka treba uključiti ponovno postavljanje autentikacije i autorizacije za sve korisnike i račune ove organizacije. Ovaj korak je jako važan jer se pomoću tog koraka može zaštititi zloupotreba privilegija. Nakon oporavka iz backupa, autentikacije i autorizacije, dolazi na red postavljanja repliciranja, kako bi se ubrzao proces oporavka, a to omogućava bržu distribuciju ažuriranih podataka unutar mreže. Nakon svih ovih koraka treba napraviti temeljito praćenje i analizu incidenta. U ovom koraku je bitno da napravimo identifikaciju izvora napada, utvrdimo kako se incident dogodio i napravimo prilagodbu sigurnosnih postavki da se budući napad spriječi. Nakon toga treba planirati kontinuitet poslovanja, gdje se razmatraju dugoročne mjere sigurnosti koje će moći spriječiti ponovan napad ili slične incidente. Upravo to planiranje uključuje implementaciju dodatnih sigurnosnih mjera. Na kraju treba napraviti da svi ovi procesi idu automatski, jer to može znatno smanjiti vrijeme oporavka i rizik od ljudskih resursa.

8. TESTIRANJE AKTIVNIH SIGURNOSNIH MJERA NA WINDOWS SERVERU 2008 R2

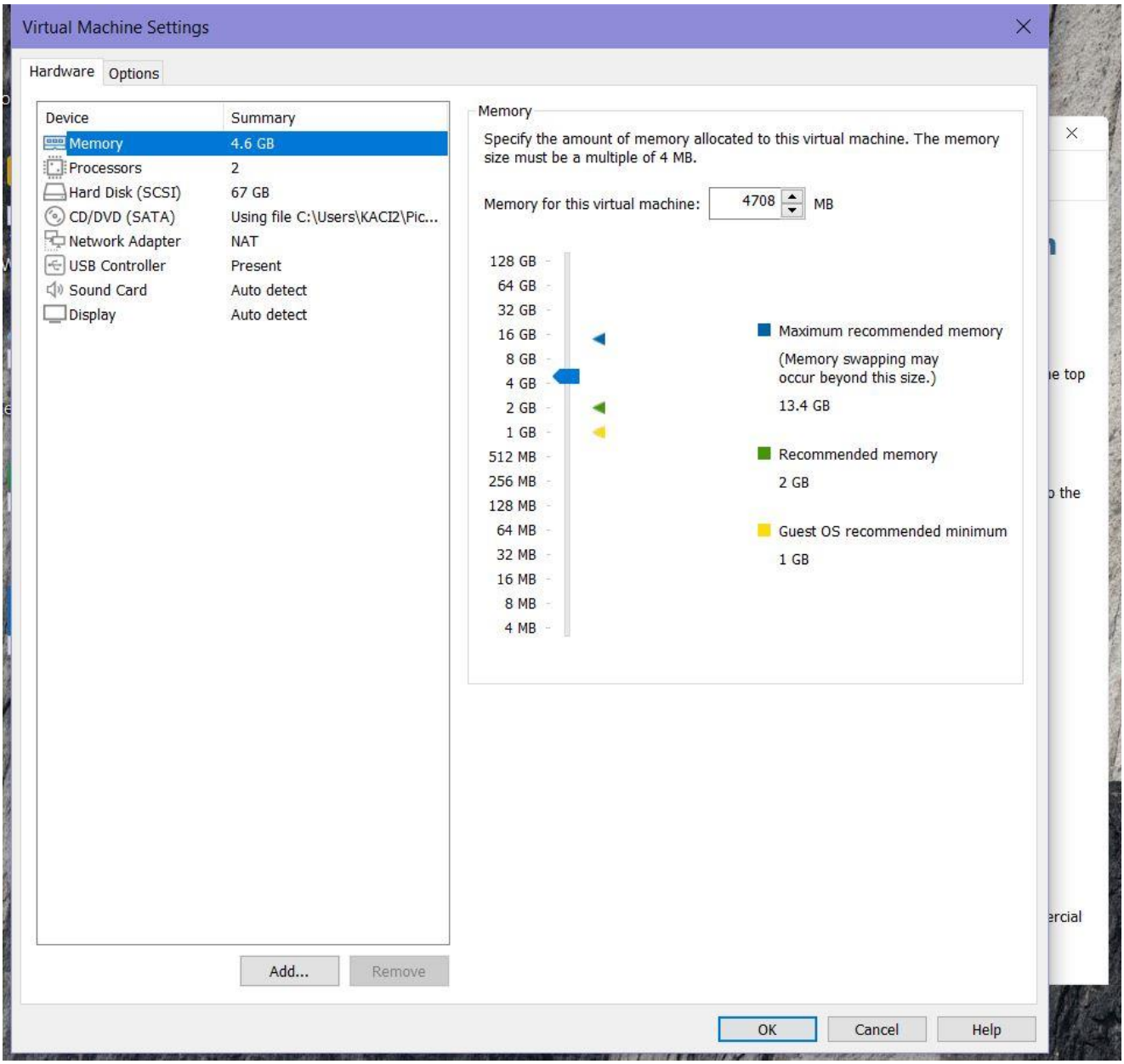
Nakon obrađenog teorijskog dijela ovog završnog rada, u praktičnom dijelu su objašnjene i istražene ranjivosti starijih verzija Windows Servera i Active Directorya, te demostrirano kako se općenito ranjivosti mogu iskoristiti i predstaviti kao neki savjeti i preporuke za zaštitu i unaprjeđenje sigurnosti Active Directory okruženja. Kao referentnu verziju sam odabrala Windows Server 2008 R2.

Prvi korak je bio instalacija Vmware Workstationa, koji je softver za virtualizaciju. Softver je preuzet sa službene stranice, a nakon instalacije sam slijedila upute za instalaciju. Također, sa Microsoft Evaluation Centra sam preuzela Windows Server 2008 R2 koji mi je bio potreban prilikom kreiranja virtualne mašine. Nakon instalacije sam kreirala novu virtualnu mašine koju sam nazvala „Windows Server 2008 R2“. Kako bi se kreirala nova virtualna mašina, potrebno je kliknuti na gumb „New“ i upisati ime mašine, zatim odabrati tip „Microsoft Windows“ i odgovarajuću verziju „Windows 2008 (64-bitni)“.



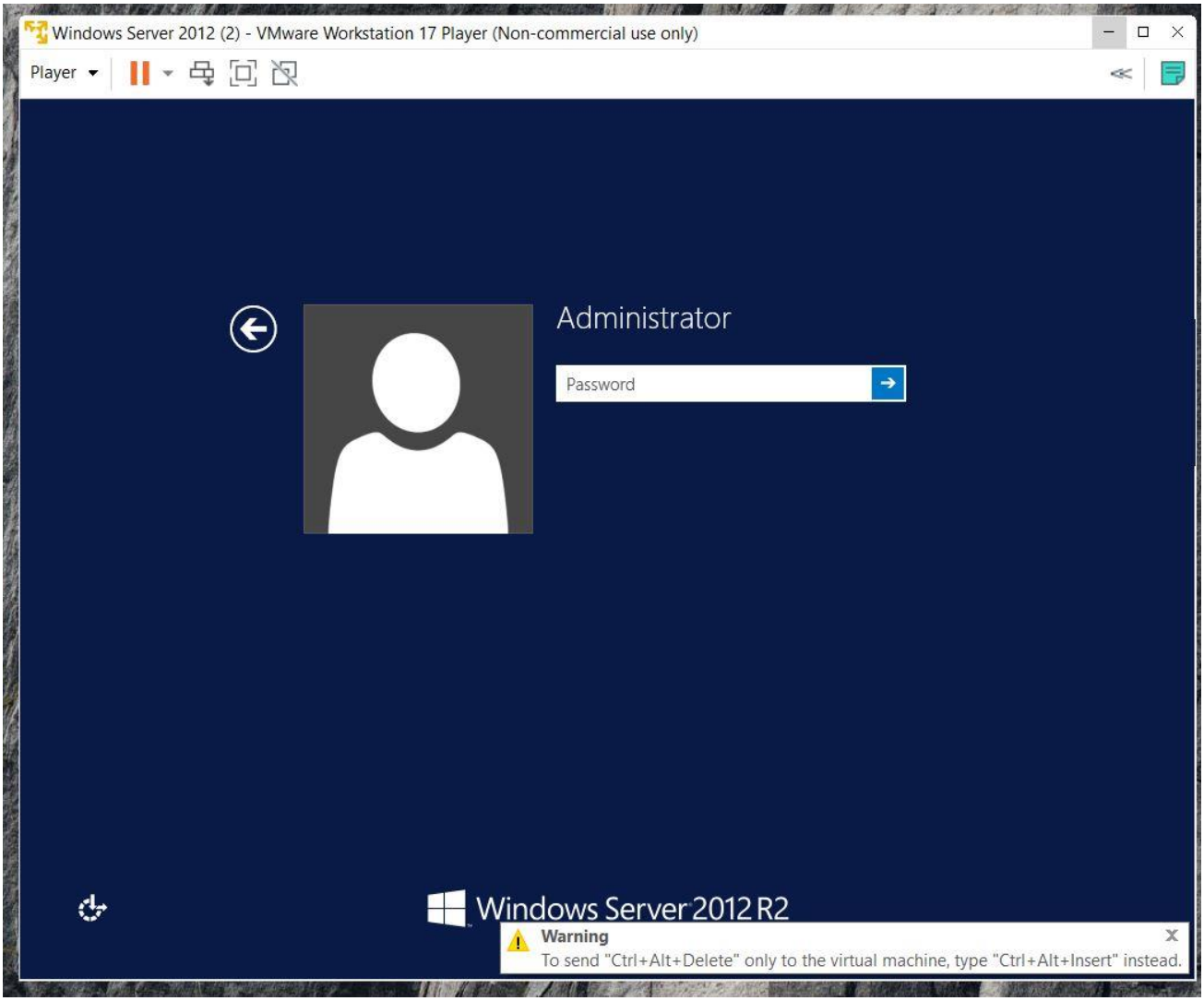
Slika 1Kreirana virtualna mašina

Nakon prelaska na idući korak moramo dodijeliti 2 GB RAM-a, što je neka i preporučena vrijednost, te kreirati novi virtualni disk sa 20 GB prostora. Na kraju je bilo potrebno dodati ISO datoteku koju smo preuzeli ranije, kao instalacijski medij i instalirati operativni sustav. Klikom na „Settings“ za ovu virtualnu mašinu, odlaskom na „Storage“ dodajemo ISO datoteku kao optički pogon.



Slika 2 Setup virtualne mašine

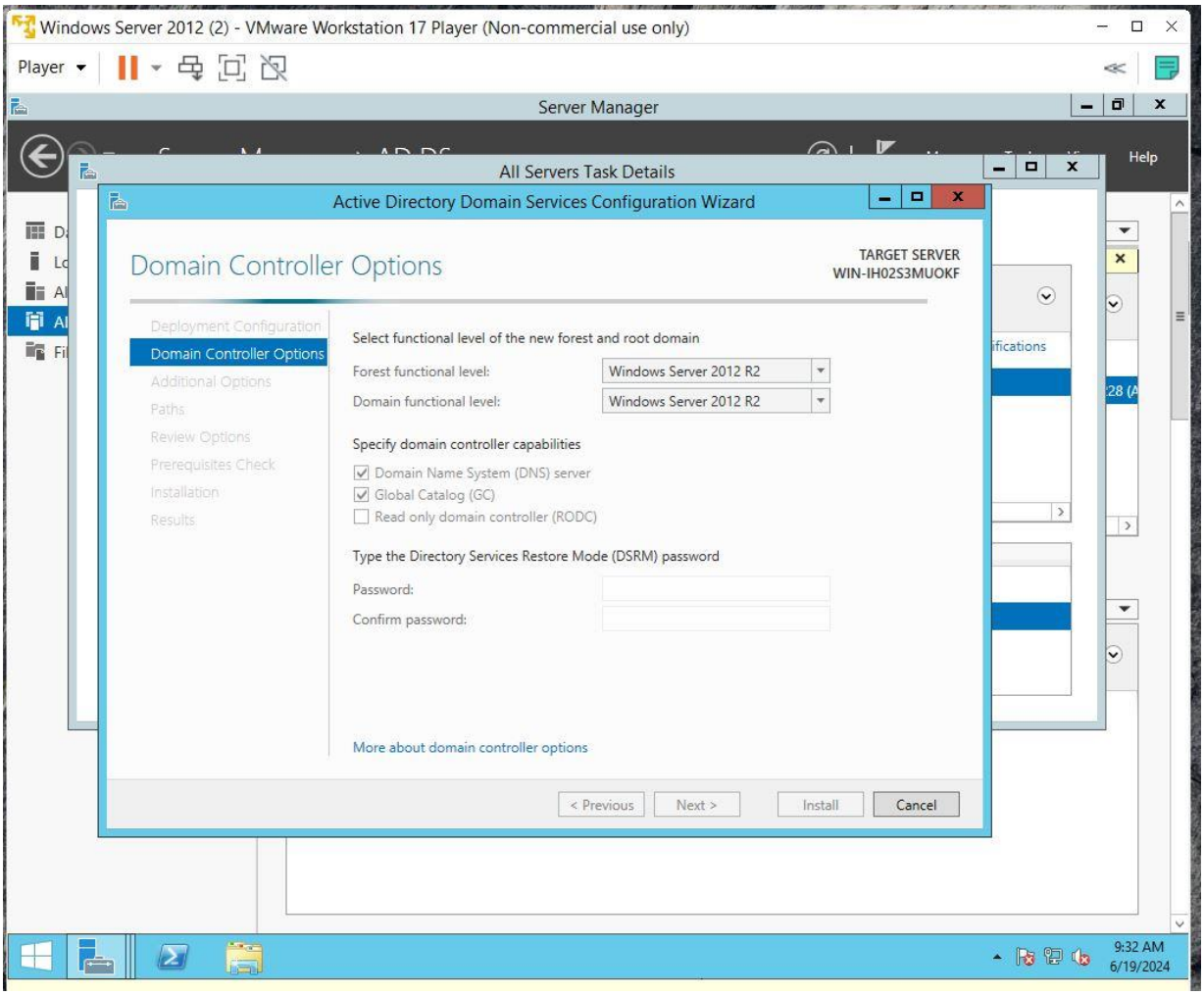
Nakon ovog koraka možemo početi sa pokretanjem virtualne mašine. Nakon pokretanja samo slijedimo upute za instalaciju Windows Servera 2008 R2, odabiremo „full instalation“ te postavimo administratorsku lozinku nakon instalacije.



Slika 3 Administratorski login nakon postavljanja lozinke

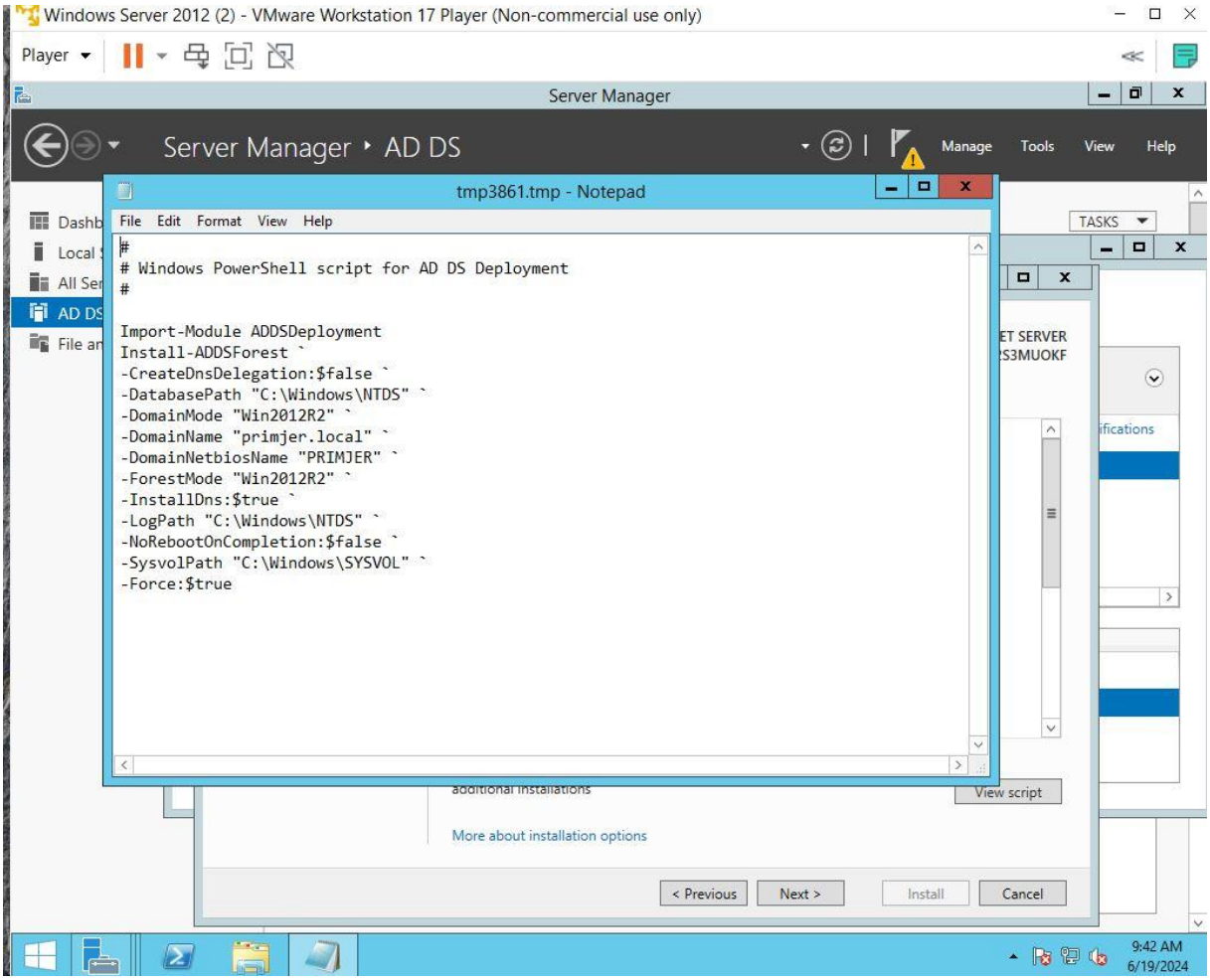
Nakon što nam je virtualna mašina spremna, instaliramo Active Directory Domain Services (AD DS). Nakon prijave prvo pokrećem Server Manager klikom na taskbar ili u izborniku. Nakon toga, u lijevom panelu imamo modul „Roles“, gdje klikom na „Add Roles“ na desnom panelu dodajemo uloge. Klikom na taj gumb, otvara se

wizard za dodavanje uloga, te samo kliknemo na gumb „Next“. Odabiremo „Active Directory Domain Services“ i samo klikom na gumb „Next“ dolazimo na kraju do gumba za instalaciju. Nakon šta ta instalacija završi, kliknemo na „Run the Active Directory Domain Services Installation Wizard (dcpromo.exe)“. Otvara nam se čarobnjak za kofiguraciju Active Directory-a, gdje samo klikom na gumb “Next“ prelazimo na iduće korake.



Slika 4 AD Domain Services konfiguracija

Nakon toga odabiremo „Create a new domain in a new forest“ i unosimo ime domene „primjer.local“, odabiremo „Windows Server 2008 R2“ funkcionalni nivo za šumu i domenu. Ostavimo zadane postavke za DNS server, a nakon toga unosim lozinku za Directory Services Restore Mode (DSRM) i prelazim na idući korak gdje imam sažetak svih postavki, te klikom na gumb „Next“ započinjem sa instalacijom. Nakon završetka instalacije moram ponavno restartati server.



Slika 5 Detalji postavljanja AD DS-a

Nakon ove instalacije prelazim na kreiranje korisničkih računa i grupa. Prvo otvaram Active Directory Users and Computers (ADUC), te nakon restarta i prijave otvaram „Server Manager“ i klikam na „Active Directory Users and Computers“ pod stavkom „Roles“. Nakon toga kreiram organizacijsku jedinicu, gdje u istoj konzoli desnim klikom na domenu „primjer.local“ odabirem „New“ -> „Organisational Unit“, unosim ime OU-a „primjer.local“ i klik na „Ok“

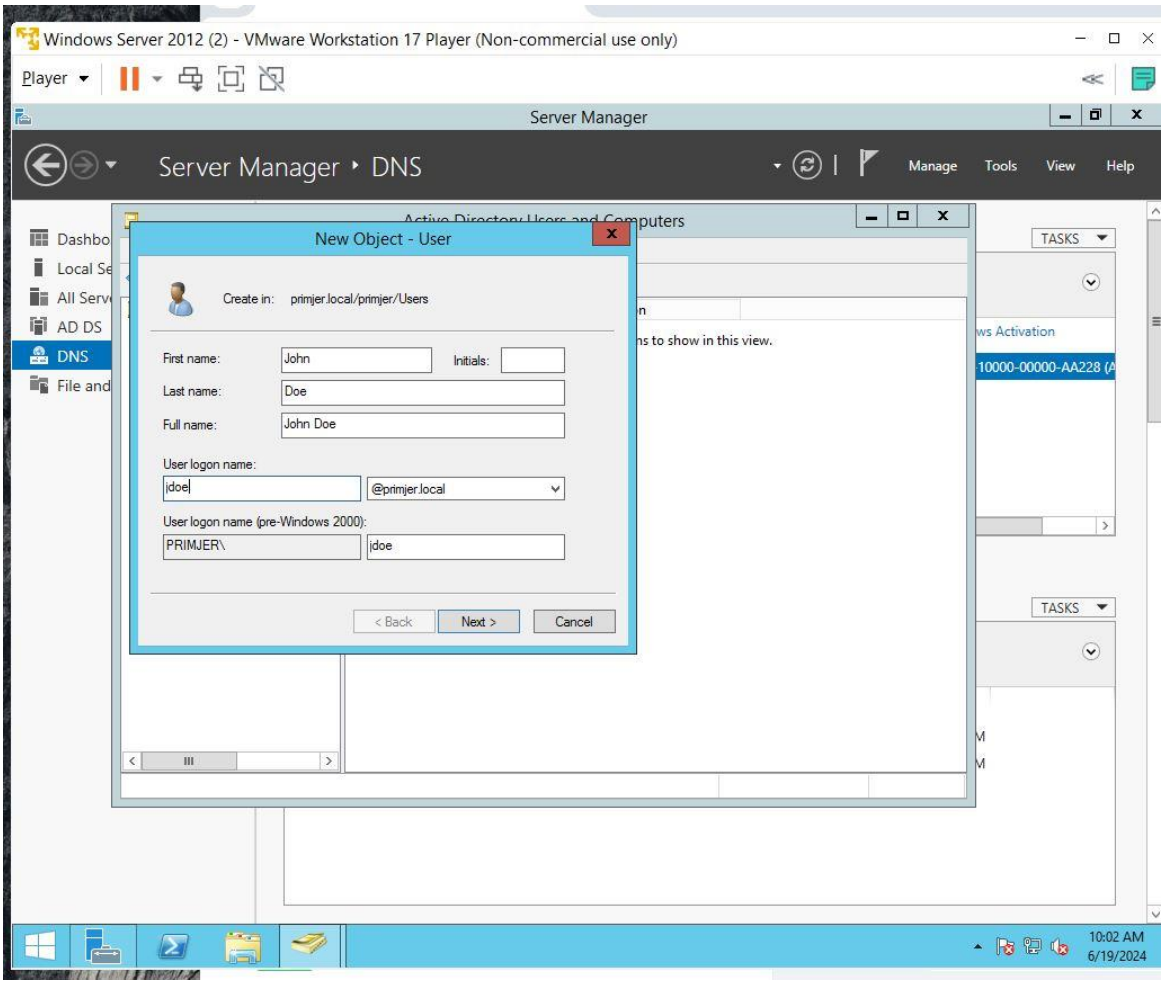
Nakon kreiranja organizacijskih jedinica (OU), na red dolazi kreiranje korisničkog računa. Desni klik na novokreiranu organizacijsku jedinicu „primjer“ i odabirem „New“ – „User“.

Tu unosim informacije za korisnički račun:

- First name: John
- Last name: Doe
- User logon name: jdoe

Kliknemo na gumb „Next“, unesemo lozinku za korisnika i potvrdimo je ponovnim unosom. Na ovom koraku možemo i postaviti odgovarajuće postavke za lozinku, te klikom na gumb „Finish“. Ako ima potrebe za kreiranjem dodatnih računa, ponavljanjem ovih koraka mogu se dodati još neki korisnici.

Nakon što smo kreirali korisnike, vrijeme je za kreiranje grupa. Klikom na novokreiranu organizacijsku jedinicu „Organization“ i klikom na „New“ -> „Group“ unosim ime grupe „Group“ i odabirem kao tip grupe „Security“.



Slika 6 Postavljanje usera

Kako bi se korisnici dodali u grupu, potrebno je desnim klikom na grupu odabrati „Properties“ i otići na karticu „Members“ pa nakon toga kliknuti na „Add“. Treba unjeti imena korisnika koje želimo dodati i kliknuti na „Ok“.

Nakon što smo instalirali i konfigurirali Active Directory, kreirali korisničke račune i grupe možemo započeti sa demonstracijom ranjivosti. Kako bi prvo napravili identifikaciju ranjivosti, istražila sam poznate ranjivosti Windows Servera 2008 R2 i Active Directorya. Neke od ključnih ranjivosti koji uključuju:

- SMBv1 ranjivost (EternalBlue) je protokol koji omogućava da se datoteke, pisači i drugi resursi na mreži dijele u sustavima Windows. Ranjivost poznata kao EternalBlue(MS17-010) omogućava da se kor izvršavana na udaljenom ranjivom sustavu. Eksploatacija je da se može iskoristiti ta ranjivost EternalBlue za preuzimanje kontrole nad sustavom bez da je iskazana ikakva potreba za autentifikacijom što omogućava da se instalira malware ili ukradu podaci ili izvrši neki proizvodljan kod. Kako bi se sustav zaštitio od ovih ranjivosti, potrebno je instalirati ažuriranje sistema jer je Microsoft redovto instalirao sigurnosne zakrpe kao odgovor na ranjivost MS17-010, a istovremeno se preporučuje onemogućavanje SMBv1 protokola na sustavima gdje nije neophodna kompatibilnost s mrežnim aplikacijama.

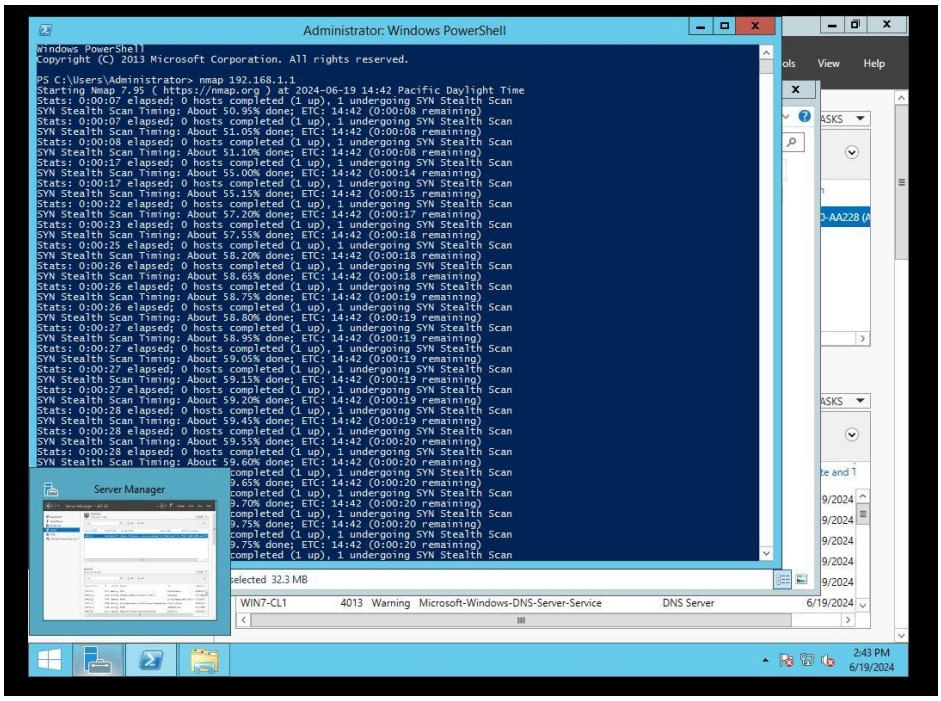
- Kerberos tiket ranjivosti je još jedan napad koji iskorištava slabo zaštićene Kerberos tikete za pristup mrežnim resursima. To je zapravo standardni mehanizam za autentifikaciju u sustavima Windows, a koristi tikete ta potvrdu identiteta korisnika. Upravo te ranjivosti u Kerberos porotokolo omogućuju napadaču da ukrade i ponovno iskoristi te tikete za neovlašteni pristup resursima unutar određene mreže. Napadač može izvršiti „Pass-the-Ticket“ napad ako je uspio ukrasti Kerberos tiket od pravog korisnika, što može omogućiti pristup resursima koje je korisnik autoriziran, ali samim tim i eskalaciju privilegija unutar mreže. Kao zaštita se preporučuje implementacija praksi kao što su korištenje usluga potvrde na bazi uloga i kratki intervali valjanosti Kerberos tiketa. Ažuriranjem najnovije verzije

Windows Servera koje uključuju poboljšanje sigurnosne mehanizme za autentifikaciju Kerberos.

- LDAP Injection ili Lightweight Directory Access Protocol je protokol koji je korišten za pretraživanje i upravljanje podacima u direktoriju kao što je Active Directoy. Ranjivosti u LDAP protokolu omogućuju napadaču da izvrši neovlaštene upite koji rezultiraju otkrivanjem osjetljivih podataka, kao što su pretraga lozinki ili promjena privilegija korisnika u Active Directory-u, te manipulacijom struktura direktorija. Kao zaštita može se upotrijebiti ograničavanjem privilegija korisnika i grupa unutar Active Directorya kako bi se smanjio utjecaj napada, a moguće je da i implementacijom mehanizma za filtriranje i sanitizaciju ulaznih podataka kako bi se spriječilo izvršavanje neovlaštenih LDAP upita.

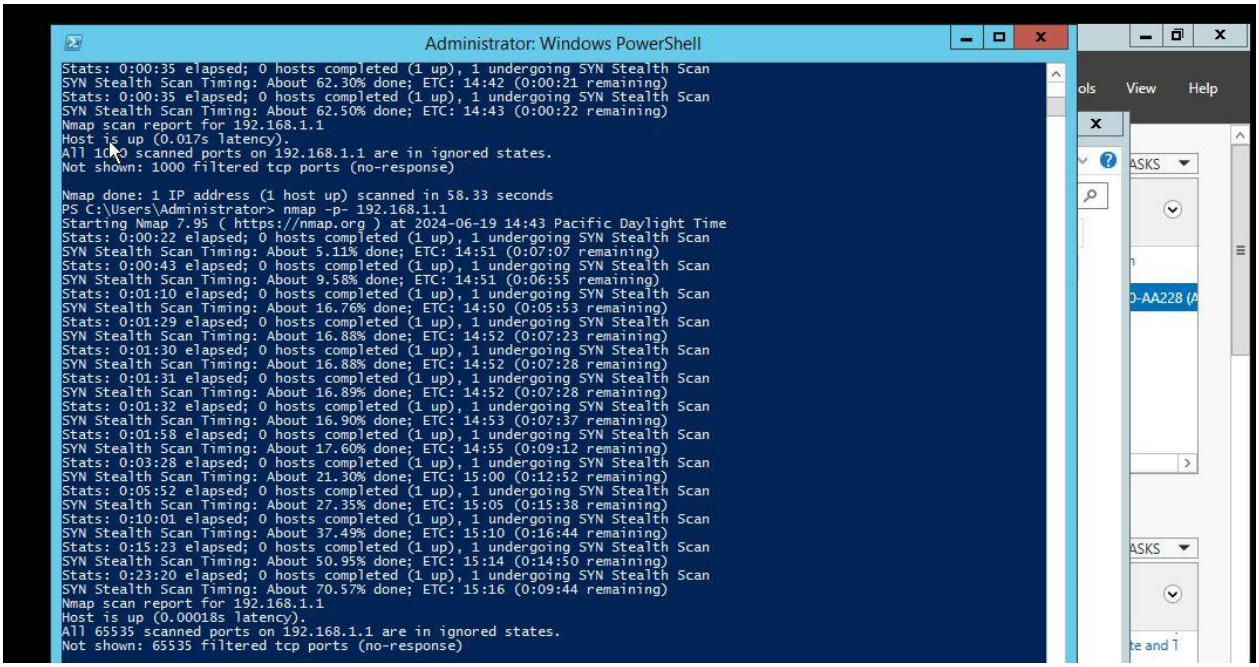
Kao zaključak praktičnog dijela rada bi se dalo izvest da ove nabrojene ranjivosti kao EternalBlue, Kerberos tiket i LDAP Injection predstavlja velike sigurnosne izazove za starije verzije Windows Servera, uključujući Windows Server 2008 R2 koju sam koristila za ispitivanje ranjivosti. Kako bi se ranjivosti spriječile, treba implementirati odgovarajuće sigurnosne mjere kako bi zaštitili Active Directory i cijelu infrastrukturu organizacije od potencijalnih napada i neovlaštenog pristupa.

U okviru ovog projekta sam izvela osnovno mrežno skeniranje i skeniranje svih portova pomoću alata Nmap u PowerShellu, a u nastavku su opisani koraci poduzeti tijekom ovog postupka uz rezultate skeniranje. Prvi korak je bilo preuzimanje i instalacija alata Nmap. Instalacijski paket sam preuzela sa službene stranice, te sam nakon preuzimanja slijedila upute za instalaciju i uspješno instalirala Nmap na svoj sustav. Nakon toga sam pokrenula PowerShell, te sam prvo provjerila da li sam spojena na mrežu, te nakon toga sam pokrenula osnovno mrežno skeniranje naredbom „nmap 192.168.1.1“. Ta naredba skenira IP adresu koja je navedene i prikazuje rezultate sa informacijama o portovima koji su otvoreni i aktivnim servisima na toj IP adresi. Prvo mrežno skeniranje je pokazalo da je uređaj sa IP adresom aktivan, ali da su svi portovi bili u „igored“ stanju, što znači da su filtrirani ili blokirani.



Slika 7 PowerShell i skeniranje mrežnog prometa

Kako bih dobila detaljni pregled mreža, izvršila sam skeniranje svih portova na toj IP adresi, sa naredbom „nmap -p- 192.168.1.1“ . Ta naredba skenira sve portove (od 1 do 65535) što omogućava da se identificiraju svi potencijalni otvoreni portovi i usluge koje se izvršavaju na toj adresi.



Slika 8 Skenranje svog mrežnog prometa

Rezultati koji pokažu da su portovi na ciljanoj IP adresi u igored stanju pokazuju da su ili filtrirani ili blokirani. Na to utječu različiti faktori, kao što su Firewall postavke, IDS/IPS sustavi, Runtime Application Self-Protection. Kod Firewall postavki IP adresa može imati postavljene neke sigurnosne mjere, kao što je firewall koji blokira ili filtrira pristup određenim portovima, a to je jedna uobičajena praksa za zaštitu mreža od neovlaštenog pristupa. IDS/IPS sustavi ili Intrusion Detection Systems i Intrusion Prevention Systems isto mogu biti aktivni na ciljanoj mreži, a oni mogu detektirati i reagirati na pokušaje neovlaštenog pristupa ili skeniranja, a rezultat toga su upravo filtrirani ili blokirani promet na portovima. RASP ili Runtime Application Self-Protection se koristi u nekim slučajevima dok se promet blokira s obzirom na sigurnosna pravila.

Iako su poznati nedostaci Windows Servera 2008 R2 zbog zastarjelih komponenti ili neispravnih sigurnosnih ažuriranja, ipak se takve situacije daju smanjiti redovitim ažuriranjem i primjenom sigurnostnih popravaka. Zaključak ovog testiranja je da su zapravo sigurnosne mjere i dalje prisutne i djelotvorne u okviru ovog eksperimenta, ali da postoje već istraženi i poznati sigurnosni nedostaci na ovoj verziji. Samo testiranje je pokazalo da unatoč zastarjeloj verziji i dalje postoje aktivne sigurnosne mjere koje su blokirale firewall i skeniranje mrežnog prometa. Samo testiranje me podsjetilo kolika je važna primjena sigurnosnih praksi kao što je konfiguriranje firewalla, praćenja aktivnosti mreže i implementaciji različitih sustava koji bi blokirali ili detektirali potencijalnu prijetnju na vrijeme.

Sam praktični rad mi je pomogao shvatit brojne aspekte sigurnosnih sustava. Unaprijedila sam razumijevanje kako mrežni sustavi štite svoje resurse od neovlaštenog pristupa, dobila praktično iskustvo u VMware Workstationu i Nmapu.

9. ZAKLJUČAK

U današnjem digitalnom okruženju, sigurnost Active Directory-a predstavlja ključni aspekt za održavanje integriteta, dostupnosti i povjerljivosti podataka unutar organizacija. Kroz ovaj rad, istražili smo važnost sigurnosti Active Directory-a, ključne pojmove povezane s njom, tipove napada s kojima se možemo susresti te prakse, politike i tehničke mjere zaštite koje organizacije mogu primijeniti kako bi osigurale svoje Active Directory okruženje.

Upravljanje sigurnošću Active Directory-a nije samo tehnološki izazov, već i organizacijski, zahtijevajući sveobuhvatni pristup koji uključuje obuku osoblja, usklađenost s propisima, redovito ažuriranje sustava, praćenje i detekciju prijetnji te planiranje za hitne slučajeve. Važno je shvatiti da je sigurnost Active Directory-a dinamičan proces koji zahtijeva stalno praćenje, evaluaciju i poboljšanje kako bi se održala korak s evolucijom prijetnji i tehnološkim promjenama.

Ključni elementi za uspješno osiguranje Active Directory-a uključuju redovito izvođenje sigurnosnih kopija i planiranje za oporavak u slučaju napada, implementaciju tehničkih mjera sigurnosti poput višerazinske autentikacije i upravljanja pristupom te primjenu alata i tehnika za praćenje i reagiranje na sigurnosne incidente.Naglasili smo važnost preventivnih mjera i politika, kao i obavezno educiranje zaposlenika o sigurnosnim prijetnjama i pravilnom postupanju u slučaju napada. Sve ove aktivnosti ne samo da jačaju sigurnost organizacije već i stvaraju osjećaj povjerenja među zaposlenicima i klijentima.

Kroz kontinuirano ulaganje u sigurnost Active Directory-a, organizacije ne samo da štite svoje poslovanje od potencijalnih prijetnji, već i grade temelje za stabilno, pouzdano i održivo poslovanje u digitalnom svijetu.
Osim toga, važno je istaknuti da sigurnost Active Directory-a nije samo stvar tehnologije, već i ljudi i procesa. Stoga, organizacije trebaju ulagati u edukaciju osoblja o sigurnosnim praksama i promicati svijest o cyber sigurnosti na svim razinama. Osposobljavanje zaposlenika za prepoznavanje sumnjivih aktivnosti i pravilno reagiranje u slučaju incidenata ključno je za cjelovitu zaštitu organizacije.

Uz to, naglašavamo važnost kontinuiranog praćenja novih tehnoloških trendova i razvoja u području cyber sigurnosti te prilagodbu sigurnosnih strategija sukladno tim promjenama. S tehnološkim napretkom dolaze i nove prijetnje, stoga je važno biti proaktivan u identificiranju i suzbijanju potencijalnih rizika.Nadalje, planiranje za hitne situacije i redovito testiranje sigurnosnih planova ključni su za osiguranje brze i učinkovite reakcije u slučaju napada. Kroz simulacije incidenata i analizu njihovih rezultata, organizacije mogu identificirati slabosti u svojim sigurnosnim strategijama i poduzeti potrebne korake za njihovo poboljšanje.

U zaključku, sigurnost Active Directory-a zahtijeva sveobuhvatan i proaktivan pristup koji uključuje tehnološke, organizacijske i ljudske resurse. Kroz kontinuirano ulaganje u sigurnost i suradnju svih relevantnih dionika, organizacije mogu izgraditi stabilno i sigurno okruženje koje će podržati njihovo poslovanje u digitalnom dobu.

9. LITERATURA

1. **"Active Directory Security: Securing Windows Environments with Identity Management"**
   - Autor: Gil Kirkpatrick
   - Izdavač: Addison-Wesley
   - Godina izdavanja: 2005
2. **"Mastering Active Directory for Windows Server 2008"**
   - Autor: John A. Price, Brad Price
   - Izdavač: Sybex
   - Godina izdavanja: 2008
3. **"Active Directory: Designing, Deploying, and Running Active Directory"**
   - Autor: Brian Desmond, Joe Richards, Robbie Allen, Alistair G. Lowe-Norris
   - Izdavač: O'Reilly Media
   - Godina izdavanja: 2013
4. **"Active Directory Cookbook: Solutions for Administrators & Developers"**
   - Autor: Robbie Allen, Laura E. Hunter
   - Izdavač: O'Reilly Media
   - Godina izdavanja: 2008
5. **"The Active Directory Cookbook for Windows Server 2003 and Windows 2000"**
   - Autor: Robbie Allen, Laura E. Hunter
   - Izdavač: O'Reilly Media
   - Godina izdavanja: 2005
6. **"Active Directory Forestry: Investigating and Managing Objects and Attributes for Windows 2000 and Windows Server 2003"**
   - Autor: Gil Kirkpatrick
   - Izdavač: Realtimepublishers
   - Godina izdavanja: 2004
7. **"Security Policies and Implementation Issues (Information Systems Security & Assurance)"**
   - Autor: Michael E. Whitman, Herbert J. Mattord, Andrew Green
   - Izdavač: Cengage Learning
   - Godina izdavanja: 2014
8. **"Active Directory: Structure, Mechanisms, and Risks"**
   - Autor: Martin Oberhofer
   - Izdavač: Vieweg+Teubner Verlag
   - Godina izdavanja: 2015

Popis slika