Date: 13th February-2026

ACTIVE DIRECTORY (AD)GA YO‘NALTIRILGAN ASOSIY TAHDIDLAR

Tashmatova Shaxnoza Sabirovna
TDTU Katta oqituvchi
Erkinov Shohjahon Sherali o‘g‘li
Xayriddinov Shaxboz Shavkatovich
Ravshanov Amirshox Inoyatovich
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: Ushbu maqolada Active Directory (AD) tizimiga yo‘naltirilgan asosiy kiberxavfsizlik tahdidlari tahlil qilinadi. Active Directory korporativ tarmoqlarda autentifikatsiya va avtorizatsiyani ta’minlovchi markaziy infratuzilma bo‘lgani sababli, u kiberjinoyatchilar uchun asosiy nishon hisoblanadi. Maqolada parolga asoslangan hujumlar (Password Spraying, Brute Force), Kerberos protokolidagi zaifliklardan foydalanish (Kerberoasting, Golden Ticket), NTLM relay hujumlari, privilegiyalarni oshirish (Privilege Escalation), lateral harakat (Lateral Movement) va domen nazoratchilariga qaratilgan hujumlar yoritiladi.

Kalt so‘zlar: Active Directory, Kerberoasting, Golden Ticket, NTLM relay, Password Spraying, Brute Force, privilegiyalarni oshirish, lateral harakat, domen nazoratchisi, kiberxavfsizlik.

Active Directory (AD) korporativ tarmoqlarda markazlashgan autentifikatsiya va avtorizatsiya tizimi sifatida ishlaydi. U foydalanuvchilarni tekshiradi, ularga resurslardan foydalanish huquqini beradi, xavfsizlik siyosatlarini boshqaradi hamda domen infratuzilmasining yaxlitligini ta’minlaydi. Shu sababli AD tashkilotning eng muhim axborot infratuzilma komponentlaridan biri hisoblanadi.

Amaliyot shuni ko‘rsatadiki, zamonaviy kiberhujumlarning aksariyati aynan Active Directory ni nishonga oladi. Sababi oddiy: agar hujumchi AD ustidan nazoratni qo‘lga kiritsa, u butun domenni, barcha foydalanuvchilarni va tarmoq resurslarini boshqarish imkoniyatiga ega bo‘ladi. Shuning uchun AD ga qaratilgan tahdidlarni chuqur o‘rganish va ularni tahlil qilish muhim ilmiy va amaliy ahamiyatga ega.

Credential (hisob ma’lumotlari) asosidagi tahdidlar

Active Directory ga yo‘naltirilgan eng keng tarqalgan tahdid turi — bu foydalanuvchi autentifikatsiya ma’lumotlarini qo‘lga kiritishdir. AD tizimi login va parol asosida ishlaganligi sababli, credential o‘g‘irlash hujumchiga dastlabki kirish nuqtasini beradi.

Hujumchilar ko‘pincha phishing xatlari, zararli dasturlar yoki ichki tarmoqda joylashgan zararli skriptlar orqali foydalanuvchi login va parollarini qo‘lga kiritadi. Bundan tashqari, Windows tizimida LSASS (Local Security Authority Subsystem Service) jarayoni xotirasidan parol hashlarini olish usuli ham keng qo‘llaniladi. Maxsus vositalar, masalan, Mimikatz, credential dumping jarayonini avtomatlashtiradi.

Credential asosidagi hujumlarning xavfi shundaki, ular ko‘pincha aniqlanishi qiyin bo‘lgan lateral harakatlarga olib keladi. Hujumchi bir foydalanuvchi hisobini qo‘lga kiritgach, boshqa tizimlarga ham kirish imkoniyatini izlaydi va bosqichma-bosqich yuqori huquqlarga ega bo‘ladi.

Quyidagi 1.1- jadvalda credential hujumlarning asosiy ko‘rinishlarini ko‘rsatadi:

Hujum turi	**Mazmuni**	**Xavfi**
Pass-the-Hash	NTLM hash orqali autentifikatsiya	Parolsiz kirish
Pass-the-Ticket	Kerberos ticketni qayta ishlatish	Tarmoq resursiga noqonuniy kirish
Credential Dumping	LSASS dan parollarni olish	Administrator huquqini egallash
Brute Force	Parolni taxmin qilish	Hisob bloklanishi yoki buzilishi

Yana bir xavfli hujum turi — Golden Ticket. Bu hujumda hujumchi KRBTGT hisobining hash qiymatini qo‘lga kiritadi va soxta autentifikatsiya ticketi yaratadi. Natijada u domen ichida istalgan foydalanuvchi sifatida harakatlana oladi. Bu deyarli to‘liq domen nazoratini anglatadi.

Kerberos asosidagi asosiy tahdidlar quyidagi 1.2-jadvaldan iborat:

Hujum nomi	**Tavsifi**	**Natijasi**
Kerberoasting	Service account hashni olish	Parolni buzish
AS-REP Roasting	Pre-auth o‘chirilgan hisobni nishonga olish	Hisob kompрometatsiyasi
Golden Ticket	Soxta TGT yaratish	To‘liq domen nazorati
Silver Ticket	Soxta xizmat ticketi	Mahalliy resursga kirish

Privilege Escalation — bu hujumchining past darajadagi foydalanuvchi huquqidan administrator darajasiga ko‘tarilish jarayonidir. AD infratuzilmasida noto‘g‘ri sozlangan ruxsatlar, zaif ACL (Access Control List) yoki noto‘g‘ri guruh konfiguratsiyasi huquqni oshirish imkonini beradi.

Masalan, agar oddiy foydalanuvchi noto‘g‘ri sozlangan obyekt ustidan yozish huquqiga ega bo‘lsa, u o‘zini yuqori darajadagi guruhga qo‘shishi mumkin. Shuningdek, xizmat hisoblaridagi noto‘g‘ri delegatsiya sozlamalari ham xavf tug‘diradi.

Privilege Escalation tahdidi juda xavfli, chunki u ko‘pincha tizim ichida yashirin ravishda amalga oshiriladi va uzoq vaqt aniqlanmasligi mumkin.

Replikatsiya va DCSync hujumlari

Active Directory multi-master replikatsiya asosida ishlaydi. Bu degani, har bir Domain Controller ma’lumotlar bazasining nusxasiga ega va ular o‘zaro sinxronlashtiriladi.

DCSync hujumi davomida hujumchi o‘zini Domain Controller sifatida ko‘rsatadi va replikatsiya protokoli orqali foydalanuvchilarning hash qiymatlarini so‘rab oladi. Agar hujumchi bu huquqqa ega bo‘lsa, u administrator parollarini qo‘lga kiritishi mumkin.

DCShadow esa soxta Domain Controller yaratish va zararli o‘zgarishlarni katalogga kiritishga asoslanadi. Bu hujum AD yaxlitligini buzadi va aniqlash qiyin bo‘lgan tahdid hisoblanadi.

LDAP va Enumeration hujumlari

Hujumchilar ko‘pincha bevosita buzishdan oldin tizim haqida ma’lumot to‘playdi. Bu jarayon “enumeration” deb ataladi. LDAP protokoli orqali domen tuzilmasi, foydalanuvchi ro‘yxati, administrator guruhlari va xizmat hisoblari haqida ma’lumot olish mumkin.

Enumeration jarayoni o‘zi mustaqil hujum emas, ammo keyingi bosqichdagi hujumlar uchun tayyorgarlik vazifasini bajaradi. Shu sababli LDAP so‘rovlarini monitoring qilish muhimdir.

Group Policy va konfiguratsiya manipulyatsiyasi

Group Policy Active Directory ning markazlashgan boshqaruv mexanizmi hisoblanadi. Agar hujumchi GPO ustidan nazorat o‘rnatsa, u butun domen bo‘yicha zararli skriptlarni ishga tushirishi yoki xavfsizlik siyosatini o‘zgartirishi mumkin. Masalan, antivirusni o‘chirib qo‘yish, firewall sozlamalarini o‘zgartirish yoki foydalanuvchilarga zararli dastur o‘rnatish imkoniyati yuzaga keladi. Bu tahdid ayniqsa ichki hujumlar (insider threat) uchun xosdir.

Domain Controller kompрometatsiyasi

Domain Controller — AD ning eng muhim elementi. Agar DC egallansa, butun domen xavf ostida qoladi. DC kompрometatsiyasi quyidagi oqibatlarga olib keladi:

- Barcha foydalanuvchi hashlarini qo‘lga kiritish
- Xavfsizlik siyosatini o‘zgartirish
- Soxta foydalanuvchilar yaratish
- Tarmoqni to‘liq boshqarish

Shu sababli DC serverlar alohida segmentda joylashtirilishi, kuchli monitoring ostida bo‘lishi va minimal ruxsat tamoyiliga amal qilinishi lozim. AD ga yo‘naltirilgan tahdidlar odatda bir bosqichli emas, balki ko‘p bosqichli hujum zanjiri ko‘rinishida amalga oshiriladi. Dastlab credential qo‘lga kiritiladi, so‘ng huquq oshiriladi, keyin replikatsiya mexanizmi ekspluatatsiya qilinadi va oxir-oqibat Domain Controller ustidan nazorat o‘rnatiladi. Bu jarayon ko‘pincha MITRE ATT&CK modeli bosqichlariga mos keladi va uzoq muddatli, yashirin harakatlar orqali amalga oshiriladi. Active Directory ga yo‘naltirilgan tahdidlar zamonaviy kiberxavfsizlik muhitida eng xavfli va murakkab tahdidlar qatoriga kiradi. Credential o‘g‘irlash, Kerberos ekspluatatsiyasi, huquqni oshirish, replikatsiya hujumlari va Domain Controller kompрometatsiyasi AD infratuzilmasining asosiy zaif nuqtalarini tashkil etadi. AD xavfsizligini ta’minlash uchun kuchli autentifikatsiya mexanizmlari, muntazam audit, Kerberos monitoringi, SIEM integratsiyasi va Threat Intelligence asosida proaktiv himoya choralari joriy etilishi zarur.

XULOSA

Xulosa qilib aytganda, *Active Directory* korporativ tarmoqning “yuragi” bo‘lib, uning zaiflashuvi butun infratuzilmaning xavf ostida qolishiga olib keladi. AD’ga

yo‘naltirilgan asosiy tahdidlar ko‘pincha autentifikatsiya mexanizmlaridagi zaifliklar, noto‘g‘ri sozlamalar yoki ortiqcha privilegiyalardan foydalanish orqali amalga oshiriladi.

Hujumchilar odatda dastlab oddiy foydalanuvchi hisobini qo‘lga kiritadi, so‘ng lateral harakat orqali yuqori darajadagi huquqlarga ega bo‘lishga intiladi va yakunda domen nazoratchisini egallashga harakat qiladi. Golden Ticket yoki Kerberoasting kabi usullar orqali uzoq muddatli yashirin kirish (persistence) ta’minlanishi mumkin.

ADABIYOTLAR RO‘YXATI

1. Active Directory Security Cookbook. – Packt Publishing, 2020.
2. Microsoft Corporation. Active Directory Security Best Practices.
3. MITRE Corporation. ATT&CK Framework – Enterprise Techniques.
4. SANS Institute. Securing Active Directory in Modern Enterprise.
5. ENISA. Cybersecurity Threat Landscape Reports.