Carlos García - Pentesting Active Directory Forests [rooted2019]

- 1.
- 2.

  ciyinet CARLOS GARCÍA GARCÍA ComputerScience Eng. OSCP Penetration Testing Hack&Beers, Qurtuba… Organizer Co-author book Hacking Windows: Ataques a Sistemas y redes Microsoft PS C:> WHOAMI 2

- 3.

  ciyinet WHAT ARE WE GOING TOTALK ABOUT? - Introduction to Active Directory Forests and Trusts - Why Pentesting Trusts? - Authentication Protocols across Trusts - Trusts enumeration - Common Attacks & Techniques - Reconnaissance across Trusts - Conclusions 3

- 4.

  ciyinet FORESTS - Domains arestructured into trees and forests - A tree is a collection of related domains - A forest is a collection of trees that trust each others - Only one “Enterprise Admins” group per forest - Exists in root domain only - Non-existing in child domains - Added as local admin in child domain’s DCs 4

- 5.

  ciyinet TRUSTS - Allow authenticationtraffic to flow between two domains - Establish the ability for users in one domain to authenticate to resources in another domain 5

- 6.

  ciyinet TRUST DIRECTION - One-way -Domain B trusts A - Users in Domain A can access resources in Domain B. Users in domain B cannot access domain A - Two-way - Domain A trusts B, domain B trusts A - Authentication requests can be passed between the two domains in both directions 6

- 7.

  ciyinet TRUST TRANSITIVITY Determines ifa trust can be extended outside of the two domains - Transitive - Extends trust relationship with other domains - Let a trusted domain pass through to a third domain - Non-transitive - Denies trust relationship with other domains 7

- 8.

  ciyinet TYPE OF TRUSTS TypeDirection Transitivity Description Parent-Child 2-way Transitive Automatically established when a new domain is created in a tree Tree-Root 2-way Transitive Automatically established when a new tree is added to a forest. Between the new tree root and the forest root domain External 1-way or 2-way Non-transitive Manually created between a domain in a forest and another domain in a different forest that does not have a forest trust established Forest 1-way or 2-way Transitive Manually created between one forest root domain

and another forest root domain Shortcut 1-way or 2-way Transitive Manually created between domains in the same forest that is used to shorten the trust path in a large and complex domain tree or forest and improve authentication times Realm 1-way or 2-way Transitive or Non-transitive Manually created between an AD domain and a non-Windows Kerberos V5 realm References: https://blogs.msmvps.com/acefekay/2016/11/02/active-directory-trusts 8

- 9.

  ciyinet TRUSTS - All trustswithin the same forest are two-way and transitive - This is why all domains within a forest trust each other - Users from any domain can access resources in any other domain within the forest as long as: - They have the proper permissions assigned at the resource - They have network access 9

- 10.
- 11.

  ciyinet DIRECTION OF TRUSTVS ACCESS Domain A Trusted domain (inbound) Domain B Trustring domain (outbound) Direction of access Direction of trust 11

- 12.
- 13.

  ciyinet WHY PENTESTING TRUSTS? -Environments with trusts that were created many years ago without security in mind - Sometimes domain trusts introduce unintended access paths - Some domains (i.e. testing, development…) are not well maintained, controlled or monitored 13

- 14.

  ciyinet WHY PENTESTING TRUSTS? Orsimply, what if your target is in a different domain? Reconnaissance Weaponisation and Exploitation Privilege Escalation & Lateral Movement Action on Targets Installation and Command & Control ▪ Email harvesting ▪ Social Networking ▪ IP Discovery ▪ Port Scanning ▪ Identify vulnerabilities ▪ Build and deliver malware via phishing, web, USB drive, network… ▪ Exploit a vulnerability to compromise the victim's system ▪ Install malware ▪ Stablish persistence inside the environment ▪ Command channel for remote access ▪ Obtain more credentials ▪ Access other systems ▪ Escalate privileges ▪ Identify critical assets ▪ Data exfiltration ▪ Encryption of critical assets ▪ Service disruption ▪ Money $$$ References: Kroll Proactive Security Team 14

- 15.
- 16.
- 17.

  ciyinet NTLM ACROSS TRUSTS 1.User requests access and sends DOMAIN-AUSERNAME Client in DOMAIN-A 2. Server sends challenge message 3. Client sends response message 4. Server sends DOMAIN-AUSERNAME challenge and response to DC in DOMAIN-B Server in DOMAIN-B DC in DOMAIN-B DC in DOMAIN-A References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773178(v=ws.10) https://blogs.technet.microsoft.com/askpfeplat/2013/05/05/how-domain-controllers-are-located-across-trusts/ https://blogs.technet.microsoft.com/isrpfeplat/2010/11/05/optimizing-ntlm-authentication-

flow-in-multi-domain-environments/ 8. Server sends authentication result to the client 7. Response to authenticate user 17

- 18.

  ciyinet KERBEROS ACROSS TRUSTS Whena user requests access to a resource in a different domain: - User's DC will not be able to issue a TGS of another domain as TGS can only be built using the target service's password and DC only contain password data from security principals in their own domain - To solve this, the there is a trusts password between two domains in the same AD forest used as a bridge enable Kerberos authentication across trust 18

- 19.

  ciyinet KERBEROS ACROSS TRUSTS Clientin DOMAIN-A 1. Request TGT (AS-REQ) 2. Receive TGT (AS-REP) Server in DOMAIN-B DC in DOMAIN-A DC in DOMAIN-B References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc773178(v=ws.10) https://adsecurity.org/?p=1588 3. Present TGT, request TGS (TGS-REQ) 4. Receive inter-realm TGT (TGS-REP) Client encrypts a timestamp with their secret (hash/key) Client receives a TGT signed with the DOMAIN-A krbtgt account that proves they are who they say they are The TGT is then used to request TGS for specific resources/services on the DOMAIN-B DC sends a TGT for DOMAIN-B signed and encrypted using the inter-realm key DC sends a TGS ticket encrypted using the hash/key of the account that is associated with that service (SPN) The TGT is then used to request service tickets (TGS) for specific services on the domain. TGT I-R TGT TGS 19

- 20.
- 21.

  ciyinet TRUSTS ENUMERATION So weland in the organization; the exploitation path will depend on: - Domain you land on and its trusts - Privileges you manage to get in it - User's privileges in foreign domains ? ? ? 21

- 23.
- 24.

  ciyinet TRUSTS ENUMERATION -NLTEST - Different information depending on where it's executed from quarantined_domain = Filter_sids nltest /domain_trusts nltest /dclist:DOMAIN nltest /server:DC /trusted_domains 24

- 25.

  ciyinet TRUSTS ENUMERATION -POWERVIEW - To enumerate trusts on a foreign domain, you need to able to bind to a DC (usually PDC) on the foreign domain* - Get-DomainTrust –SearchBase "GC://$($ENV:USERDNSDOMAIN)" - Return all forest trusts for the current forest or a specified forest Get-DomainTrust –Domain FOREIGN DOMAIN FQDN Get-ForestTrust –Domain FOREIGN DOMAIN FQDN 25

- 27.
- 28.
- 29.

- 30.

  ciyinet EXPLOITATION PATH Source (attacker's location) Target domain Techniqueto use Trust relationship Root Child • Golden Ticket + Enterprise Admins group Inter-realm (2-way) Child Child • SID History exploitation Inter-realm Parent-Child (2-way) Child Root • SID History exploitation Inter-realm Tree-Root (2-way) Forest A Forest B • Printer bug + Unconstrained Delegation ? Intra-realm Forest or External (2-way) - Having Domain-Admin-level on the current domain: 30 - Not having Domain-Admin-level on the current domain: Reconnaissance + Exploitation (and always depending on type of trusts, direction and transitivity)

- 31.

  ciyinet Forest CIYILAB ForestTRICIA ciyilab.local dev.ciyilab.local test.dev.ciyilab.local DA-LEVEL TECHNIQUES – ROOT TO CHILD Parent-Child trust Parent-Child trust assuan.local Tree-Root trust tricia.local Forest trust Forest CANETE canete.local External trust Golden ticket + EA group 31

- 32.

  ciyinet ciyilab.local GOLDEN TICKET +ENTERPRISE ADMINS ciyilabciyi dc01 32 mimikatz.exe "kerberos::golden /domain:ROOT_DOMAIN_FQDN /sid:ROOT_DOMAIN_SID /krbtgt:ROOT_DOMAIN_KRBTGT_NT_HASH /user:USERNAME /groups:500,501,513,512,520,518,519 /ptt" Included by default. 519: RID of "Enterprise Admins" group

- 34.
- 35.

  ciyinet SID HISTORY - Usedto migrate users from one domain to another - When a user is migrated, his old SID and all groups' SIDs he's a member of can be added to the attribute sidHistory - When the user tries to access a resource, his SID and the SIDs included in the sidHistory attribute are checked to grant/deny access - sidHistory is normally respected by domains within the forest. For external/forest trusts, they are filtered out by the "SID filtering" protection References: https://www.itprotoday.com/windows-78/exploiting-sidhistory-ad-attribute https://www.harmj0y.net/blog/redteaming/the-trustpocalypse/ https://gallery.technet.microsoft.com/migrate-ad-users-to-new-2e480804/ http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/ 35

- 36.
- 38.
- 39.

  ciyinet EXPLOITATION PATH - HavingDomain-Admin-level in the domain you are: - Not having Domain-Admin-level on the current domain: Reconnaissance + Exploitation (and always depending on type of trusts, direction and transitivy) 39 Source (attacker's location) Target domain Technique to use Trust relationship Root Child • Golden Ticket + Enterprise Admins group Inter-realm (2-way) Child Child • SID History exploitation Inter-realm Parent-Child (2-way) Child Root • SID History exploitation Inter-realm Tree-Root (2-way) Forest A Forest B • Printer bug + Unconstrained Delegation ? Intra-realm Forest or External trust (2-way)

- 40.

ciyinet RECONNAISSANCE 1. Enumerate truststhe current domain has and also trusts the other domains have 2. Enumerate objects: a. Enumerate security principals (i.e. users, groups, computers) in the current domain that have access to resources in another domain b. Enumerate groups that have users from another domain 3. Map exploitation path: what accounts need to be compromised to move from the current position to the target 40 References: http://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/

- 41.
- 43.
- 44.

ciyinet 2. OBJECT ENUMERATION Securityprincipals (users/groups) can be configured to have access to resources in another domain as: - Members of a local group in foreign machines - Look for foreign local group membership - Members of a domain group in a foreign domain - Look for foreign domain group membership - Principals in ACEs in a DACL - Look for foreign security principals in ACE in a foreign domain 44

- 45.

ciyinet TYPE OF GROUPS GroupVisibility (available to) Can have members from Same domain Other domains in same forest Domains outside the forest (forest or external trust) Functional memberships Local Local • Users • Computers • Domain local groups • Global groups • Universal groups • Users • Computers • Global groups • Universal groups • Users • Computers • Global groups • Users in the same forest • Users in other forests (foreign security principals) AD Domain local Domain (Cannot be used outside the domain they've been created in) • Users • Computers • Other Domain local groups • Global groups • Universal groups • Users • Computers • Global groups • Universal groups • Users • Computers • Global groups • Users in the same forest • Users in other forests (foreign security principals) AD Global Forest(s) • Users • Computers • Other Global groups None None Cannot have users of other domains AD Universal Forest(s) (Stored within the Global Catalog) • Users • Computers • Global groups • Other Universal groups • Users • Computers • Global groups • Other Universal groups None Users in the same forest References: https://www.youtube.com/watch?v=aPh8_RB8XEU 45

- 46.

ciyinet FOREIGN LOCAL GROUPMEMBERSHIP - Remote SAM (SAMR) or GPO correlation - Depending on current configuration (i.e. Windows firewall), in some cases we might need local admin privs on target to enumerate its local groups PowerView: Get-NetLocalGroup –ComputerName HOSTNAME Get-NetLocalGroupMemeber –ComputerName HOSTNAME -GroupName GROUP References: http://www.harmj0y.net/blog/redteaming/local-group-enumeration/ 46

- 47.
- 49.
- 50.
- 52.
- 53.
- 54.

ciyinet FOREIGN USER MEMBERSHIP Enumerateusers in groups outside of the user's domain. This can be used within the same forest PowerView: *Only Universal groups membership will be reflected Get-DomainForeignUser –Domain FOREIGN DOMAIN FQDN 54

- 56.

ciyinet FOREIGN GROUP MEMBERSHIP Enumeratgroups in the target domain that contains users that are not from the target domain. This can be used against domain within the same forest or through a external/forest trust PowerView: Get-DomainForeignGroupMember –Domain FOREIGN DOMAIN FQDN 56

- 57.

ciyinet FOREIGN ACL PRINCIPALS 1.Enumerate DACLs (and their ACE entries) of all objects in domains that trusts yours 2. Only analyze ACE entries with foreign security principals This can be used against domain within the same forest or through a external/forest trust PowerView to list ACE entries with security principals from our domain: Get-DomainObjectAcl –Domain FOREIGN DOMAIN FQDN –ResolveGUIDs | Where-Object {$_.SecurityIdentifier –like 'CURRENT_DOMAIN_SID*'} 57

- 58.

ciyinet 3. MAPPING EXPLOITATIONPATH – OBJECT ENUMERATION WITH BLOODHOUND BloodHound can enumerate trusts and objects in foreign domains (local and domain groups membership, ACLs, etc.) Invoke-BloodHound –SearchForest Invoke-BloodHound –Domain FOREIGN DOMAIN FQDN 58

- 59.
- 62.
- 64.
- 66.
- 67.

ciyinet WRAPPING UP –"METHODOLOGY" 1. Enumerate trusts the current domain has and also trusts the other domains have 2. Is the target within the same forest? Yes: step 3 No: steps 4 and 5 3. Got DA-level privileges in the current domain? Yes: use DA-level techniques No: steps 4 and 5 4. Enumerate objects: a. Security principals (i.e. user, groups, computers) in the current domain that have access to resources in another domain b. Groups that have users from another domain c. Foreign security principals in ACE in foreign domains 5. Map exploitation path What accounts need to be compromised to move from the current position to the target 67

- 68.
- 69.

ciyinet CONCLUSIONS - If otherdomain trusts our domain, we can query their AD information - Trusts can introduce unintended access paths - Domain trust boundaries are not security boundaries - Losing control of the KRBTGT account password hash of any domain equates to losing control of the entire forest - You must reset KRBTGT (twice) in every domain in the forest! 69

- 70.

ciyinet BUSINESS RISK Compromise ofjust one Domain Admin account in the Active Directory forest exposes the entire organization to risk. The attacker would have unrestricted access to all resources managed by all domains, users, servers, workstations and data. Moreover, the attacker could instantly establish persistence in the Active Directory environment, which is difficult to notice and cannot be efficiently remediated with guarantees. “Once Domain Admin, always Domain Admin” “Once any Domain Admin, always Enterprise Admin” 70

- 71.

ciyinet ACKNOWLEDGMENT & REFERENCES -My brother (Happy B-DAY!!!) - Francisco Tocino - Nikhil Mittal (@nikhil_mitt) - Will Schroeder (@harmj0y) - Andrew Robbins (@_wald0) - Benjamin Delpy (@gentilkiwi) - Sean Metcalf (@PyroTek3) 71

- 72.
- 73.
- 74.
- 75.
