KNOWLEDGE IS POWER

Elad Shamir *reports on the importance of understanding and protecting against Kerberos*

Log4Shell, ProxyLogon, and ProxyShell vulnerabilities have dominated cybersecurity news over the past few weeks. A recent joint Cybersecurity Advisory from the CISA, NSA, FBI, ASCS, CCS and NZ NCSC, and NCSC-UK notes 'Kerberoasting' as a potential method for malicious escalation of privilege.

The infamous Kerberoasting attack holds the dubious honour of being the most common method threat actors use to acquire higher privileges. Issues with authentication coercion and delegation add further layers of risk.

Why is Kerberos one of the most frequently targeted components of Active Directory? Despite its ubiquity, Kerberos is probably one of the least understood and most maligned creatures in the AD forest. Although the technology is relatively straightforward on the surface, its close integration with Active Directory can make configuration an absolute nightmare. Semperis' 2022 Purple Knight Report indicates that Kerberos security is especially challenging for healthcare organisations, which scored just 59 percent on Purple Knight's health check of their Active Directory security.

Many Active Directory environments have more domain administrators than necessary. Orphaned admin accounts and service accounts that have excess permissions and weak or non-expiring passwords are disasters waiting to happen. Even group Managed Service Accounts (gMSAs), which were introduced to solve some of the most egregious service-account password issues, can fall prey to Kerberoasting if attackers gain the right privileges.

Threat actors love a path of least resistance. A significant part of hardening Active Directory simply involves creating as many digital hurdles as possible. And when we're dealing with Kerberoasting, mitigating and combatting these attacks starts with understanding precisely how it is that Kerberos works.

Most Kerberos discussions are bogged down by technical explanations and authentication flow diagrams. I'm not a fan. They're boring, they're confusing, and they fail to really explain the basics. Instead, I'd like to tell you a story.

A significant part of hardening Active Directory involves creating as many digital hurdles as possible

Picture an entrepreneur named Bill who's opened an amusement park. Eventually, he notices a lot of people lie about their age or misrepresent their height to get access to rides they aren't allowed on. Bill isn't happy about that, so he decides to come up with a solution.

He establishes a new and improved model where everyone must become a member of an exclusive club to access the park. The park keeps the details of members on file – name, date of birth, height and group memberships. Everyone also gets a secret authentication code.

Now, let's say someone – Alice – wants to get on a ride. First, Alice must visit the ticket office to pay and authenticate using her secret code. The office then pulls her data and issues her a day pass, encrypted using a secret key that only the ticket office knows.

Finally, Alice presents the day pass to the ticket office with the name of the ride. The office then issues her an encrypted ride ticket, which she can present to the ride operator for access. She can only go on whichever ride she's been authenticated for – she cannot, for example, ride the Ferris wheel if she's only authenticated for the rollercoaster.

Now map that story to Kerberos:

From amusement park to Kerberos

Amusement Park	Kerberos
Secret code and payment	Pre-authentication
Ticket office	Domain controller (KDC, AS)
Day pass	Ticket granting ticket (TGT)
Ride ticket	Service ticket (TGS)
Operator	Service account
Ticket office password/key	KRBTGT account password/key
Operator password/key	Service account password/key
Ride name	Service principal name
Bill	Domain admins
Visitors	Users
Visitor details in ticket (but no signatures)	Privilege attribute certificate (PAC)

So, to continue the analogy, let's say that someone steals a ride ticket and then figures out the cipher. They've effectively performed the equivalent of a Kerberoasting attack. This involves acquiring a ticket and cracking the encryption to find a password match for the encryption key.

Within Active Directory, the Kerberoasting process is as follows:

The attacker runs an LDAP query, identifying all normal user accounts whose service principal names attribute is not empty.

The attacker then evaluates each account to determine if cracking it will give them anything worthwhile.

Once they've chosen and cracked an account, the attacker can then take control, enabling them to: access services with that account's privileges; modify existing service tickets, also referred to as silver tickets'; and forge new service tickets.

If the attacker manages to gain control over an Active Directory Key Distribution Service Account (KRBTGT), they can then access anything connected to Active Directory by forging ticket-granting tickets – also known as 'golden tickets'.

The success of a Kerberoasting attack depends on weak or crackable passwords. Active Directory

KERBEROS IS PROBABLY ONE OF THE MOST MALIGNED CREATURES IN THE AD FOREST

has a built-in feature designed to solve this: group Managed Service Accounts, or gMSAs. These accounts have randomly generated passwords that are rotated automatically every 30 days.

The use of group Managed Service Accounts and password rotation seems, at first glance, to run directly counter to well-established advice on password management. "According to NIST and Microsoft, you generally shouldn't rotate passwords for typical user accounts," says Sean Deuby, Semperis' Director of Services. "There's no benefit, and complex password rotation can actually compromise both security and productivity. Unfortunately, we see many businesses erroneously apply this advice to highly privileged accounts, which are subject to a different set of rules."

Kerberoasting enables a service ticket with cryptographic material to be taken offline. The ticket can then be cracked far more efficiently and without oversight. Without password rotation, the threat actor will eventually succeed.

"Service accounts are unlike typical user accounts," continues Deuby. "For highly privileged accounts, you'll want to use a password generator to create highly entropic passwords you know will be difficult to crack. Rotating them regularly further defeats efforts to compromise them, especially with the KRBTGT account." Still, the use of gMSAs alone is not enough to defeat determined attackers.

If an attacker can compromise a service account or host configured for unconstrained delegation, they can take over any user or computer that authenticates to that host.

"Unconstrained delegation really seems to hearken back to the fact that Active Directory has been around for more than 20 years." explains Deuby. "It's essentially the compiled sins of those decades. Maybe 10 or 15 years ago someone had to do something in a hurry, so they set up unconstrained delegation to make things easier – without thinking about how vulnerable that could make Active Directory."

Unconstrained delegation leaves a business vulnerable to authentication coercion – a method of attack that goes beyond watering hole attacks and social engineering. Authentication coercion is at the core of several of AD's most significant vulnerabilities. You've probably heard of techniques using authentication coercion like PetitPotam and ShadowCoerce.

Those two types of attack are publicly disclosed, but attackers and red teams know of many other undisclosed types of authentication coercion. This is what makes unconstrained delegation one of the most dangerous configurations in Active Directory. There are many ways it can be exploited, and many of those tactics are largely unknown.

One excellent tactic for defeating Kerberoasting is the honeypot. You know what attackers are looking for in a Kerberoastable account. Their end goal is to use service tickets to gain access to increasingly higher privileges, potentially even gaining access to administrative rights. Given that attackers inevitably choose the path of least resistance, they aren't likely to pass up the opportunity to skip straight to administrative rights.

KERBEROS SECURITY IS ESPECIALLY CHALLENGING FOR HEALTHCARE ORGANISATIONS

Create a fake account that's part of the domain admins group and make sure it's noticeable. That account should be equipped with a particularly strong password and ideally shouldn't be used for anything. If you see that account generating tickets, you'll know immediately that you have malicious activity within your network.

Beyond disabling unconstrained delegation and implementing better password policies, there are other ways you can protect Kerberos. First, upgrade your domain controllers to the latest version of Windows Server. Doing so ensures that service tickets issued to users always use the highest encryption level possible. It also prevents attackers from downgrading the cipher to make it easier to crack.

Second, disable NTLM. If attackers intercept an NTLM exchange, they can potentially crack the hash on that exchange within 24 hours. Sign every channel, bind every service, and implement micro-segmentation.

Third, keeping an eye on security indicators – both indicators of exposure and indicators of compromise – can aid monitoring efforts and improve the efficacy of Active Directory security controls. When combined with the ability to undo changes and perform vulnerability assessments that flag user accounts with risky controls, it reduces the likelihood of malicious behaviour impacting AD and going undetected.

LOSING BATTLE

Unfortunately, trying to watch manually for security indicators is a losing battle. A smarter solution is a security solution built specifically for Active Directory and armed with the most current threat information. For example, at Semperis, the Research Team regularly updates the list of threat indicators to enable enterprises to spot Active Directory security holes – both indicators of exposure (IOEs) and indicators of compromise (IOCs).

Identifying IOEs enables security teams to shut down vulnerabilities before attackers can take advantage of them. And IOCs – modifications such as changes to the default domain policy, say, or Group Policy objects (GPOs) related to the default domain controller's policy – can be signs that attackers are active in your environment. GPOs that control security settings can be a gateway to privileged access. Changes to default security descriptor attributes on schema object classes can indicate that attackers are using newly created objects to gain such access.

Beyond spotting IOCs, look for solutions that also offer auto-remediation of critical changes. This capability enables you to stop suspicious activity in its tracks, whenever and wherever it happens. Security admins can then review the suspicious changes, allowing them if they turn out to be legit and preventing further damage if they don't. Many attacks circumvent logging, so this automatic rollback capability is vital.

With a carefully thought-out incident response plan and assessment and protection tools built to protect Kerberos and Active Directory (such as Semperis' Purple Knight and Directory Services Protector), organisations can reduce the likelihood of a successful Kerberoasting attack ●

Elad Shamir is Director, Breach Preparedness and Response, Semperis. He has over 15 years of experience across the different domains of information security and spent most of his career focusing on security research and delivering offensive security services, such as red team adversary simulations and penetration tests.

Complex password rotation can actually compromise both security and productivity

Picture credit: shutterstock.com