Microsoft

Security: Microsoft Defender for Identity - Fundamentals

Liju Varghese
Cloud Solutions Architect
Microsoft Canada

About

- 3-day engagement to demo MDI as a UEBA platform.
    - Workshop
    - MDI demo and walkthrough
    - Deployment in production environment

- On-premises AD DS still an authoritative identity store.
- MDI as a detection solution helps identify indicators of threat and compromise.
- User and Entity Behavioral Analytics builds baseline behavioral profiles and then identify anomalous activity.

Agenda

Day	Agenda	Duration
Aug 22	Introductory meeting	1 hr
	Knowledge Sharing 1: Understanding Credential Attacks	2 hrs
	Knowledge Sharing 2: MDI Overview and MDI Deep-Dive	3 hrs
	Knowledge Sharing 3: Importance of Response Planning	2 hrs
Aug 23	Deploy MDI to the customer isolated lab environment	*All day*
Aug 24	Deploy MDI to the customer isolated lab environment (contd.)	
	MDI Solution demonstration	4 hrs

Security, Identity and Cybersecurity Services

Microsoft Defender for Identity (MDI)

Understanding Credential Attacks

Liju Varghese
Cloud Solutions Architect

Microsoft

Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see Use of Microsoft Copyrighted Content at

http://www.microsoft.com/en-us/legal/intellectualproperty/Permissions/default.aspx

DirectX, Hyper-V, Internet Explorer, Microsoft, Outlook, OneDrive, SQL Server, Windows, Microsoft Azure, Windows PowerShell, Windows Server, Windows Vista, and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Objectives

After completing this module, you will be able to explain the following credential theft attacks:

- Pass-the-Hash (PtH)
- Pass-the-Ticket (PtT)
- Overpass-the-Hash
- Golden Ticket
- Remote Code Execution
- Brute force attack

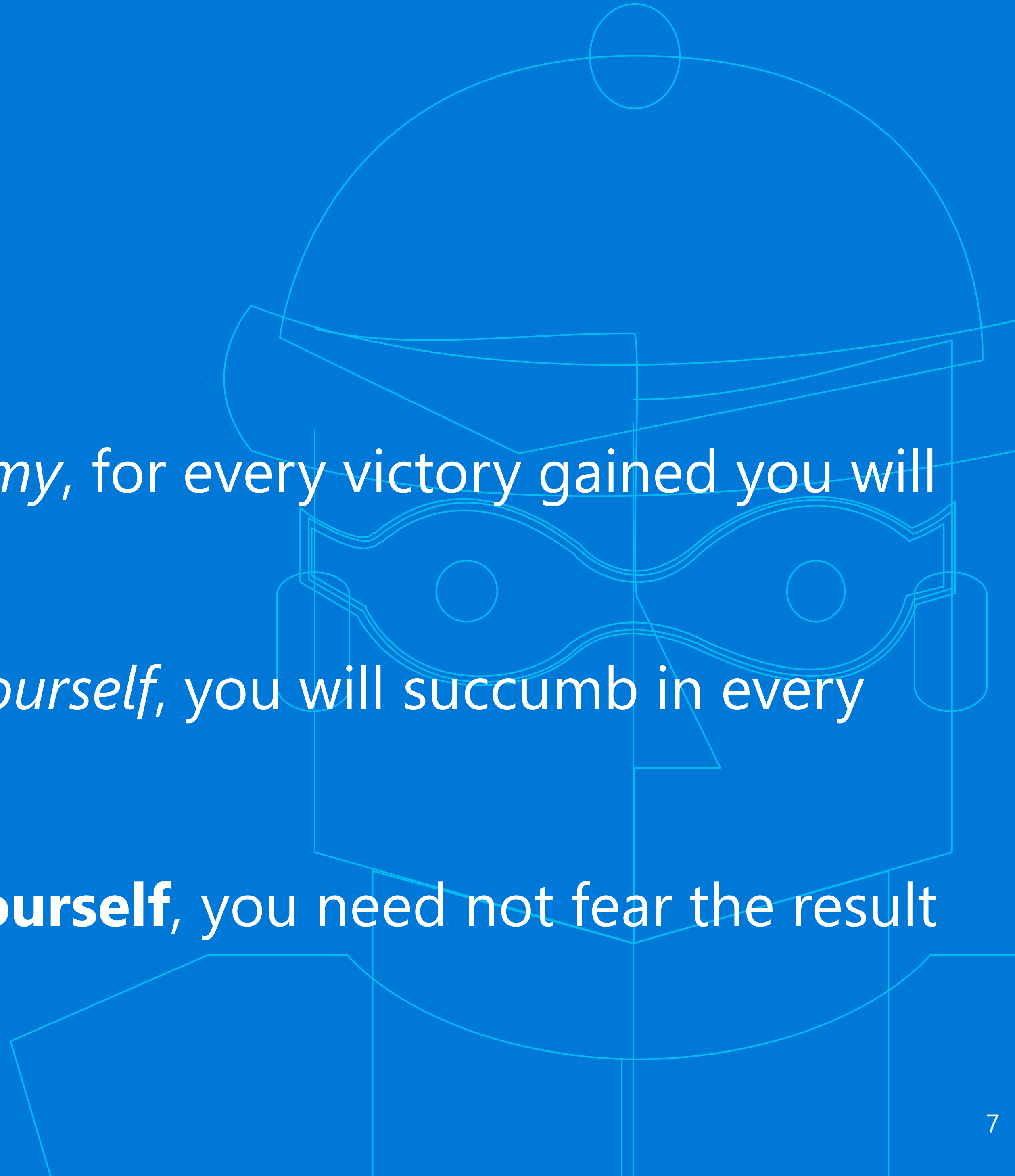
The threat landscape

…the era of cloud computing is here
in a time of war-like constant hostility:

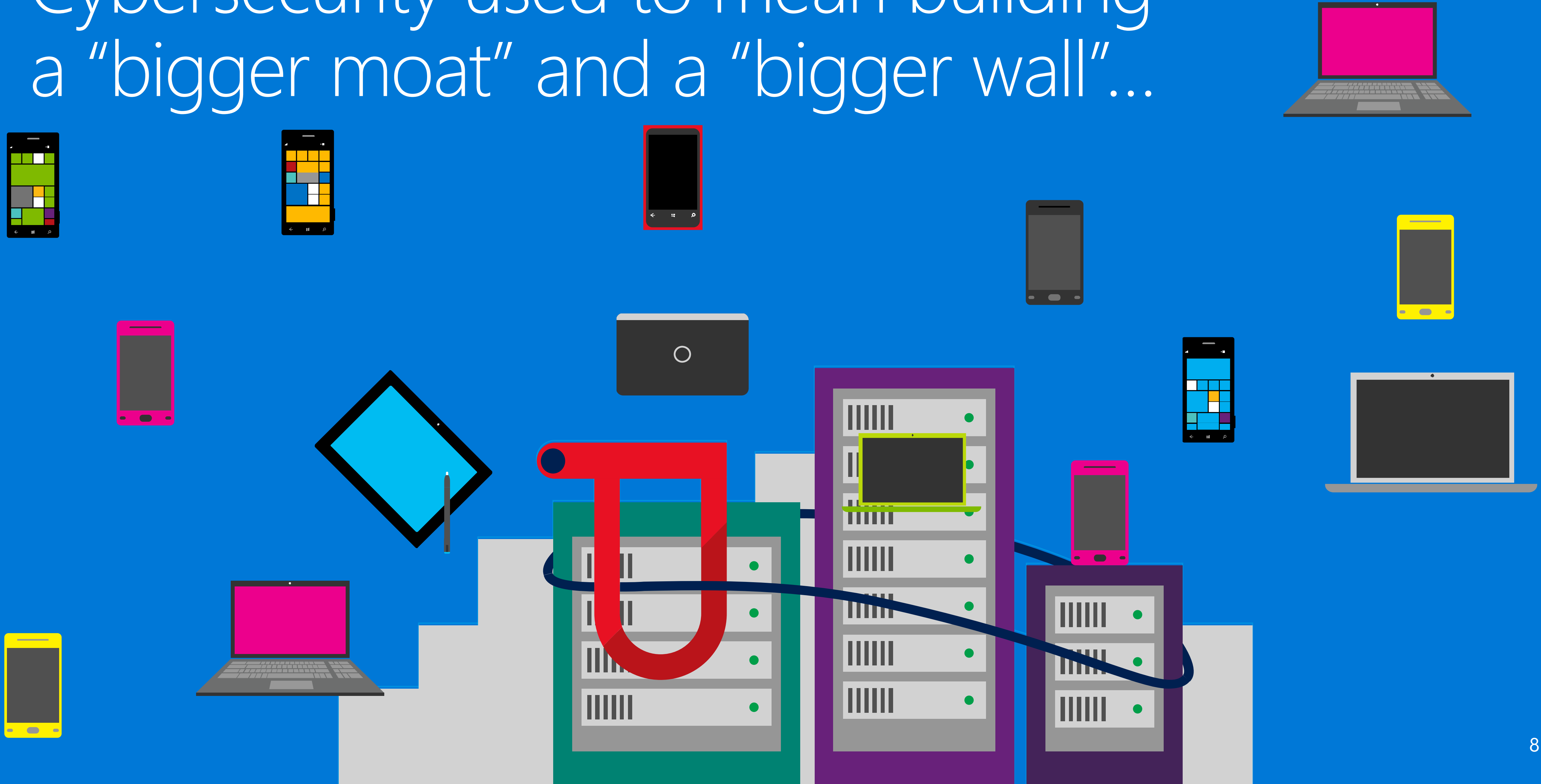
"If you **know yourself** *but not the enemy*, for every victory gained you will also suffer a defeat"

know neither *the enemy nor yourself*, you will succumb in every battle"

know the enemy *and* **know yourself**, you need not fear the result of a hundred battles"



Cybersecurity used to mean building a “bigger moat” and a “bigger wall”…

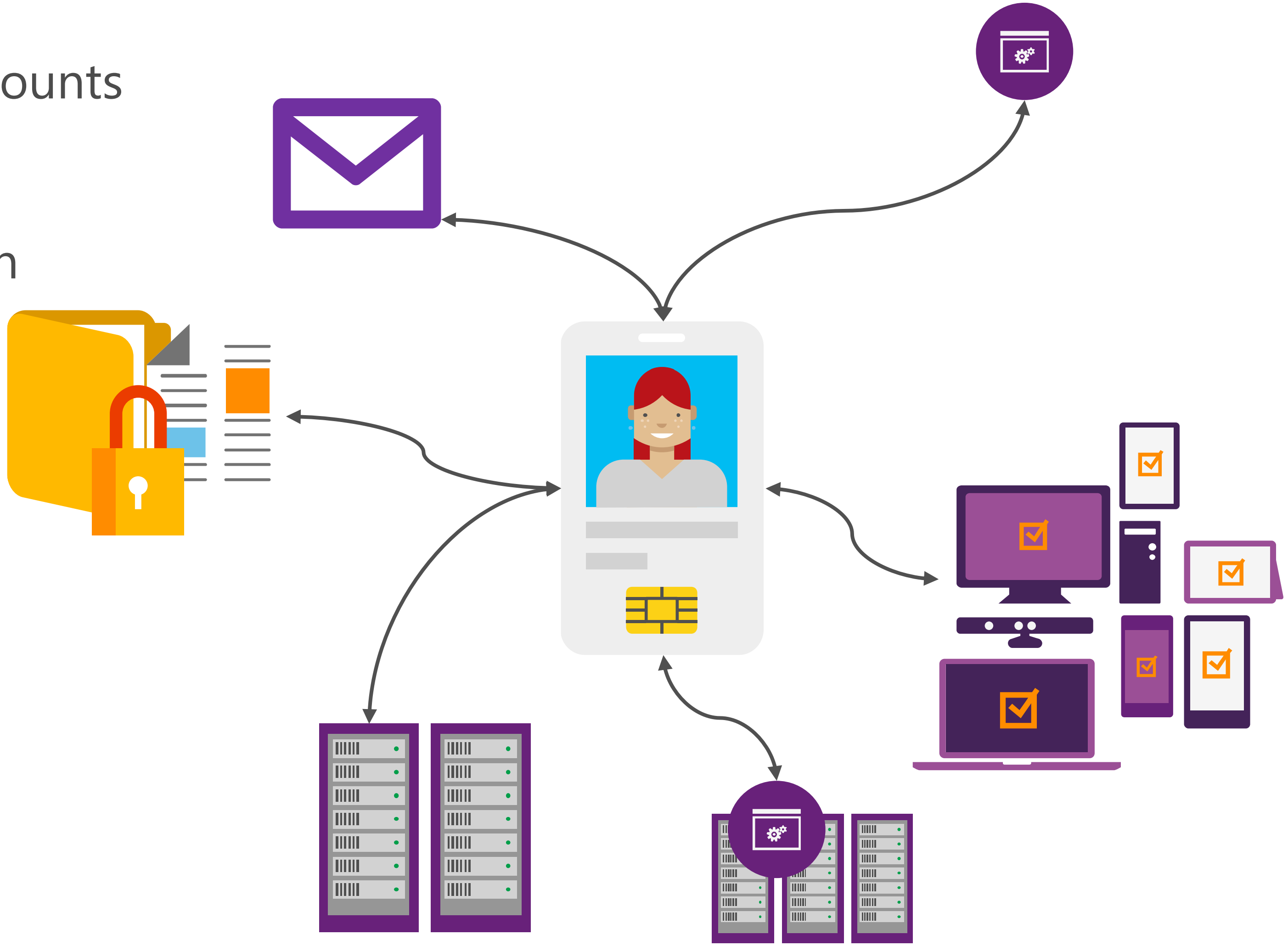


Role of directory and identity in security

Foundation of security assurances for all information assets in the organization:

- Authenticates all user and computer accounts within the on-premises Active Directory infrastructure
- Centralized delegation and authorization mechanism for many resources.

Modern cyber-attackers actively target directories to get intellectual property and corporate assets



What is credential theft, and why is it important?

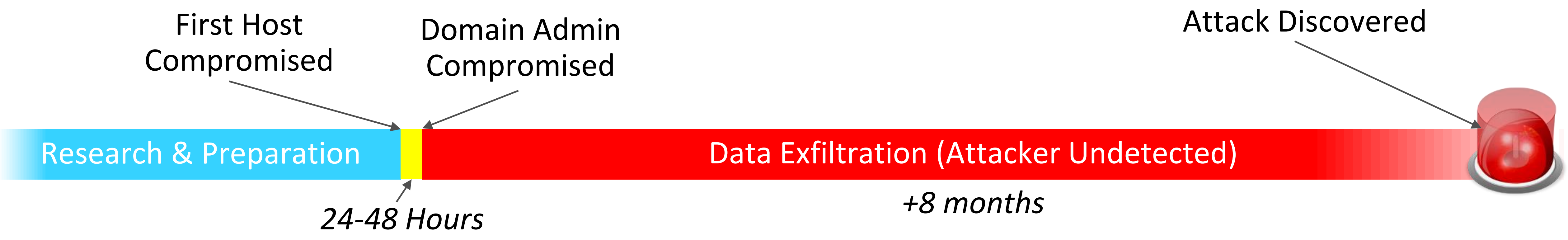
Credential theft is a technique in which **an attacker captures account credentials** from a compromised computer.

The attacker then uses these credentials to authenticate and access other network resources.

Why is it important?

Once the attacker gets in, Credential Theft is the technique they use to **spread their access throughout the network**

Typical attack timeline and observations



First Host Compromised

Domain Admin Compromised

Attack Discovered

Research & Preparation

Data Exfiltration (Attacker Undetected)

24-48 Hours

+8 months

Attack Sophistication
Attack operators will exploit any weakness
Target information on any device or service

Exploiting Credentials
On-premises Active Directory controls access to business assets
Attackers commonly target AD DS and IT Admins

Attacks not detected
Current detection tools miss most attacks
You may be under attack (or compromised)

Response and Recovery
Response requires advanced expertise and tools.
Expensive and challenging to successfully recover from.

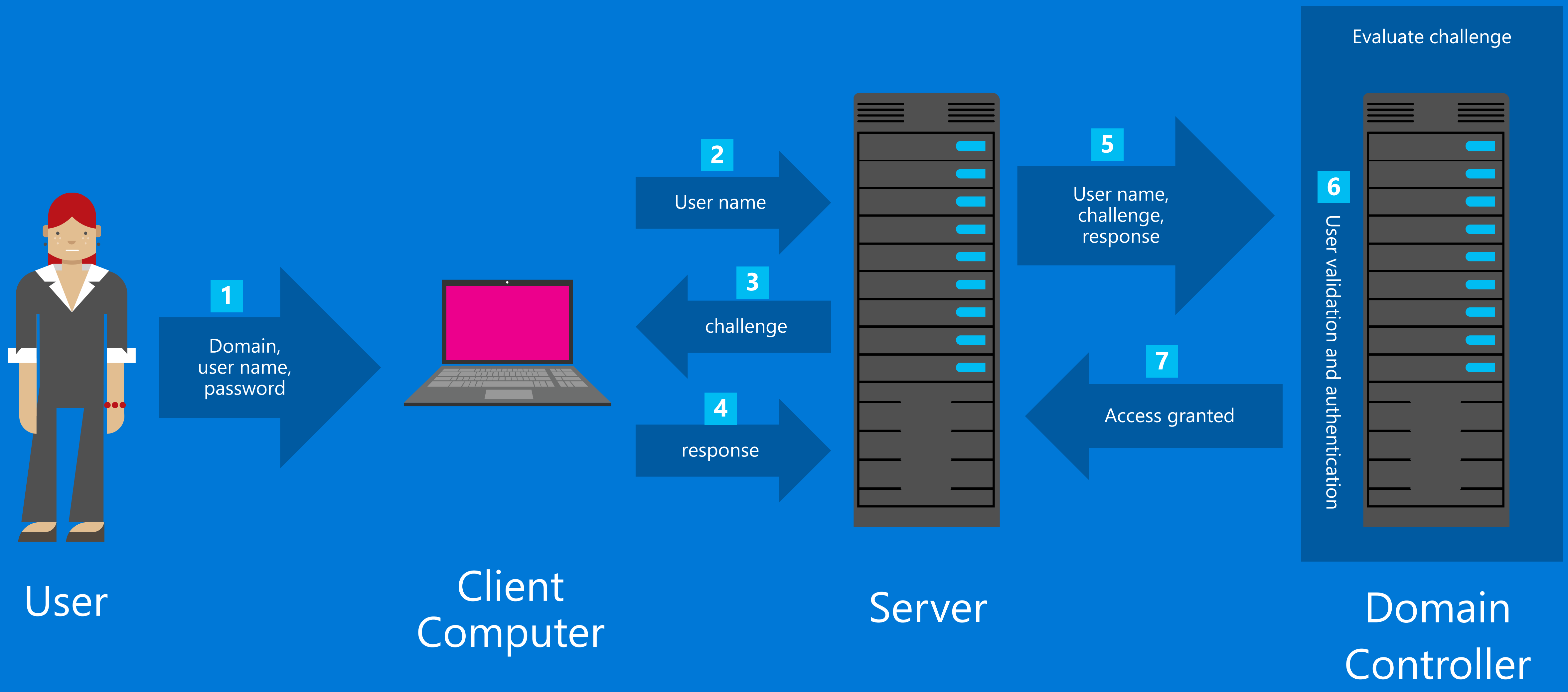
Understanding credential theft attacks

What is NT LAN manager (NTLM)?

- NTLM is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users

- NTLM replaced LAN Manager authentication in Windows. NTLMv2 was introduced in WinNT4.0 SP4

How NTLM works



NTLM weaknesses

No mutual authentication

Service validates user, user does not validate the service

Service =
Protocol + Server

Authentication is not service bound

NTLM does not validate the Server

NTLM does not “know” the encapsulating protocol (e.g. SMB, LDAP,..)

Pass-the-hash (PtH)

The **What**:
PtH allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or Lan Manager hash (LMHash) of a user's password, instead of requiring the associated plaintext password as is normally the case

Attacker uses a tool to replace their username/hash with target account hash in memory. Tools to do this are freely available on the web!

The **How**:

1. Attacker sends spear phishing email and gets access to a system
2. Once on the system, attacker uses tools to grab hashes of logged on users or local admin
3. Attacker moves laterally to a PC where domain admin logs in
4. Attacker grabs domain admin’s hash

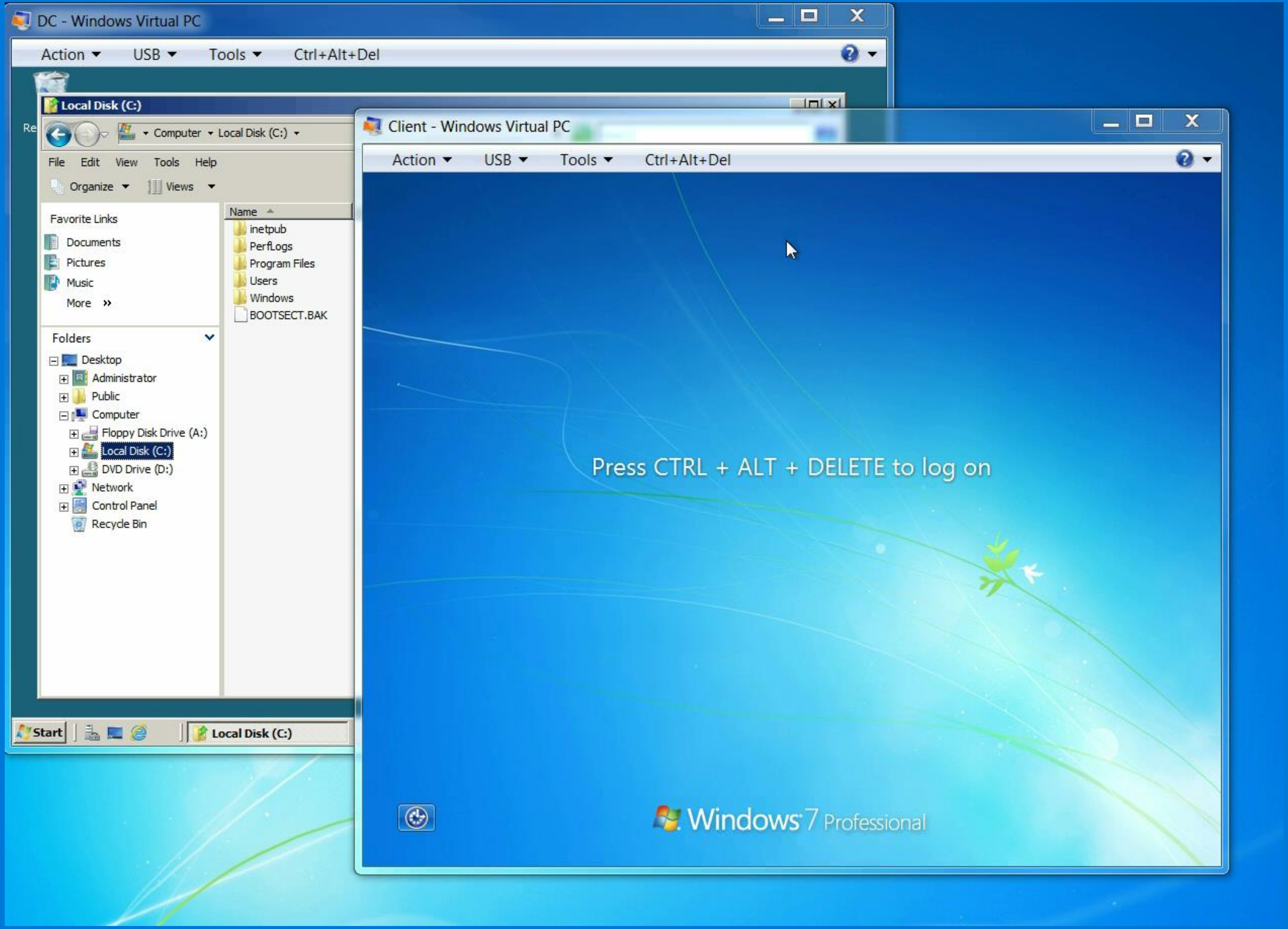
Pass-the-hash (PtH)

Why is it bad?

Because the tools are freely available, this attack is easy to execute

Allows attacker to easily get Domain Admin (DA) rights and roam throughout the network

DA is local admin on every domain joined PC/Server, which typically means admin on any apps or services installed as well



Press CTRL + ALT + DELETE to log on

Overpass-the-hash

The **What**:
OtH is a hacking technique that allows an attacker to use the NTLM hash to obtain a valid user Kerberos ticket request. The user key (NTLM hash when using RC4) is used to encrypt the Pre-Authentication & first data requests

The **How** :

1. Attacker sends spear phishing email and gets access to a system
2. Attacker uses a hacking tool to grab user hash and generates Kerberos request
3. Attacker then authenticates to resources as the user

Overpass-the-hash

Why is it Bad?

1. Authentication (KRB_AS_REQ) is done with the DC, but looks legit because the request is formed using the users hash

2. Again, TGT is good and wont need to be validated for 10 hours (default Kerberos lifetime)

3. And again….All activity appears as the user, so security logs wont help

Additional considerations:

1. These attacks require local administrator privileges on the target endpoint. The tools need admin privileges to access and change LSASS memory

2. This is why it is so important that users are just that, users of the machine, not admins.

3. Spear phishing is pretty common, but web site attacks are possible too

LSASS (Local Security Authority Subsystem Service)

Kerberos

The **What**:

Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

→ **It is all about keys and tickets!**

If you are accessing a resource on a server, you need 3 sets of keys, all stored in AD DS, and all derived from the password

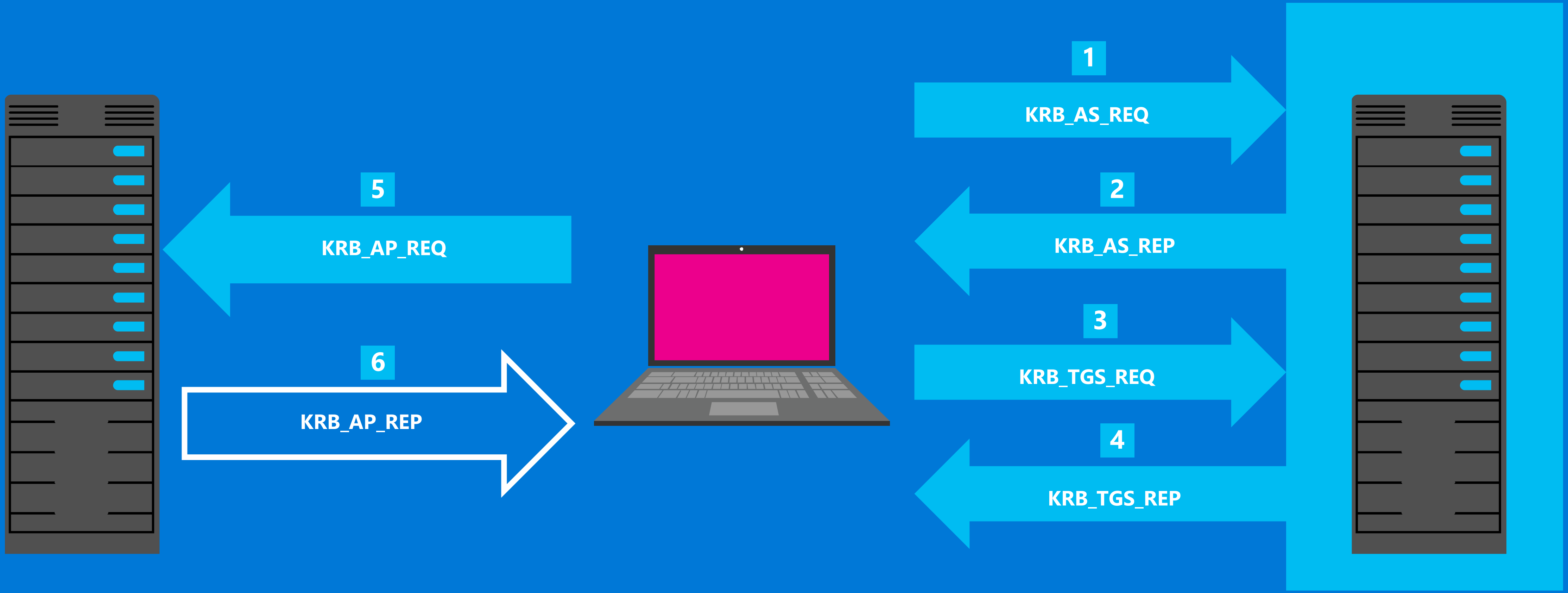
The **How**:

1. **The KDC** (Key Distribution Center) long-term secret key (*domain key*)
    - Under the `krbtgt` account (RC4, AES128, AES256, DES…)
    - Needed to sign Microsoft specific data in "**PAC**", encrypt **TGT**

2. **The Client** long-term secret key (*derived from the password*)
    - Under the user/computer/server account
    - Needed to check **KRB_AS_REQ**, encrypt session key

3. **The Target/Service** long-term secret key (*derived from the password*)
    - Under the computer/server account
    - Needed to countersign data in "**PAC**" of **TGS**, encrypt **TGS**

How kerberos works



Server

Client Computer

Kerberos Domain Controller

Kerberos vulnerabilities

Kerberos KRBTGT

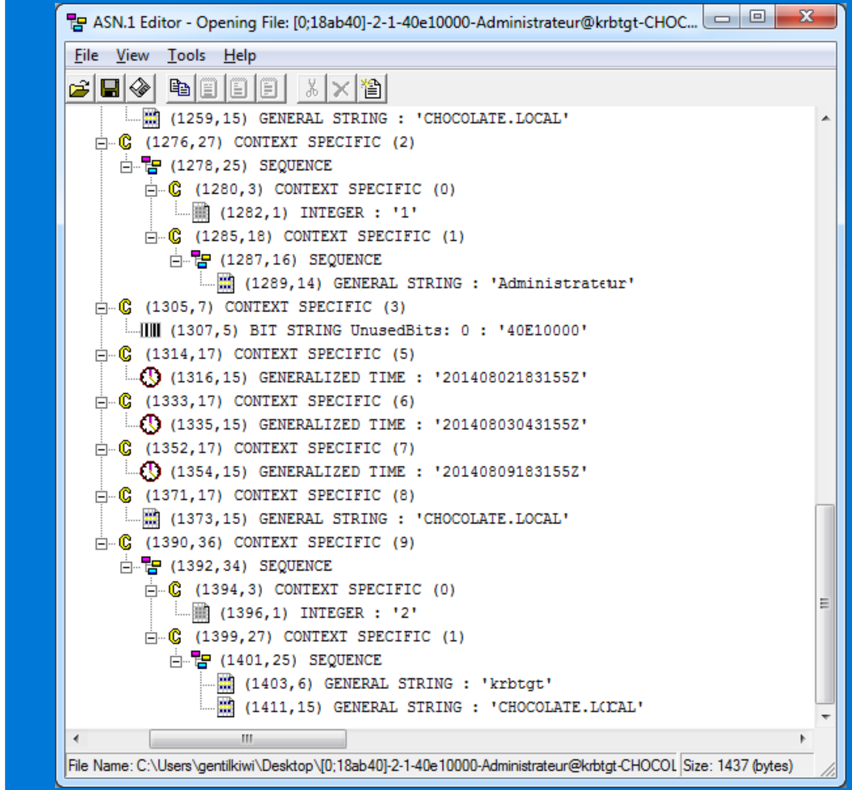
krbtgt account password / hash only changes:

- Upgrade of domain functional level (NT5 to NT6)*
- ~~Bare metal recovery using restore media~~
- Manually changed (compromise recovery)
- In most enterprises this password hasn't changed in YEARS

Kerberos PAC

All of this is not secret!

- Tickets are ASN.1 encoded
  - Use OpenSSL or your favorite tool
- Kerberos ticket (and KRB-CRED format)
  - http://www.ietf.org/rfc/rfc4120.txt
- Microsoft Specific PAC
  - http://msdn.microsoft.com/library/cc237917.aspx


ASN.1 Editor - Opening File: [0;18ab40]-2-1-40e10000-Administrateur@krbtgt-CHOC...
File
View
Tools
Help

```
      (1259,15) GENERAL STRING : 'CHOCOLATE.LOCAL'
  C (1276,27) CONTEXT SPECIFIC (2)
      (1278,25) SEQUENCE
        C (1280,3) CONTEXT SPECIFIC (0)
            (1282,1) INTEGER : '1'
        C (1285,18) CONTEXT SPECIFIC (1)
            (1287,16) SEQUENCE
              (1289,14) GENERAL STRING : 'Administrateur'
  C (1305,7) CONTEXT SPECIFIC (3)
      (1307,5) BIT STRING UnusedBits: 0 : '40E10000'
  C (1314,17) CONTEXT SPECIFIC (5)
      (1316,15) GENERALIZED TIME : '20140802183155Z'
  C (1333,17) CONTEXT SPECIFIC (6)
      (1335,15) GENERALIZED TIME : '20140803043155Z'
  C (1352,17) CONTEXT SPECIFIC (7)
      (1354,15) GENERALIZED TIME : '20140809183155Z'
  C (1371,17) CONTEXT SPECIFIC (8)
      (1373,15) GENERAL STRING : 'CHOCOLATE.LOCAL'
  C (1390,36) CONTEXT SPECIFIC (9)
      (1392,34) SEQUENCE
        C (1394,3) CONTEXT SPECIFIC (0)
            (1396,1) INTEGER : '2'
        C (1399,27) CONTEXT SPECIFIC (1)
            (1401,25) SEQUENCE
              (1403,6) GENERAL STRING : 'krbtgt'
              (1411,15) GENERAL STRING : 'CHOCOLATE.LOCAL'
```

File Name: C:\Users\gentilkiwi\Desktop\[0;18ab40]-2-1-40e10000-Administrateur@krbtgt-CHOCOL Size: 1437 (bytes)

*NT5: Windows 2000 or Windows Server 2003
NT6: Windows 2008 later

Pass-the-ticket (PtT)

The **What**:
PtT allows an attacker to extract an existing, valid Kerberos ticket from one machine and pass it to another one to gain access to resources as that user

Attacker grabs TGT or TGS from target user and replaces in memory, then accesses resources as the users.

The **How**:

1. Attacker sends spear phishing email and gets access to a system
2. Attacker uses a hacking tool to grab user TGT/TGS
3. Attacker then authenticates to resources as the user
4. Attacker can act as user and exfiltrate data, etc. All activity appears to be from that user
5. If domain admin is found, attacker can access anything on the network as domain admin

Pass-the-ticket (PtT)

Why is it bad?

Because the tools are freely available, this attack is easy to execute

Allows attacker to easily get DA and roam throughout the network

DA is local admin on every domain joined PC/Server, which typically means admin on any apps or services installed as well

Golden tickets and silver tickets

The **What**:

A "Golden Ticket", is a homemade ticket
It's done with a lot of effort and a key.

It's not made by the KDC, so:

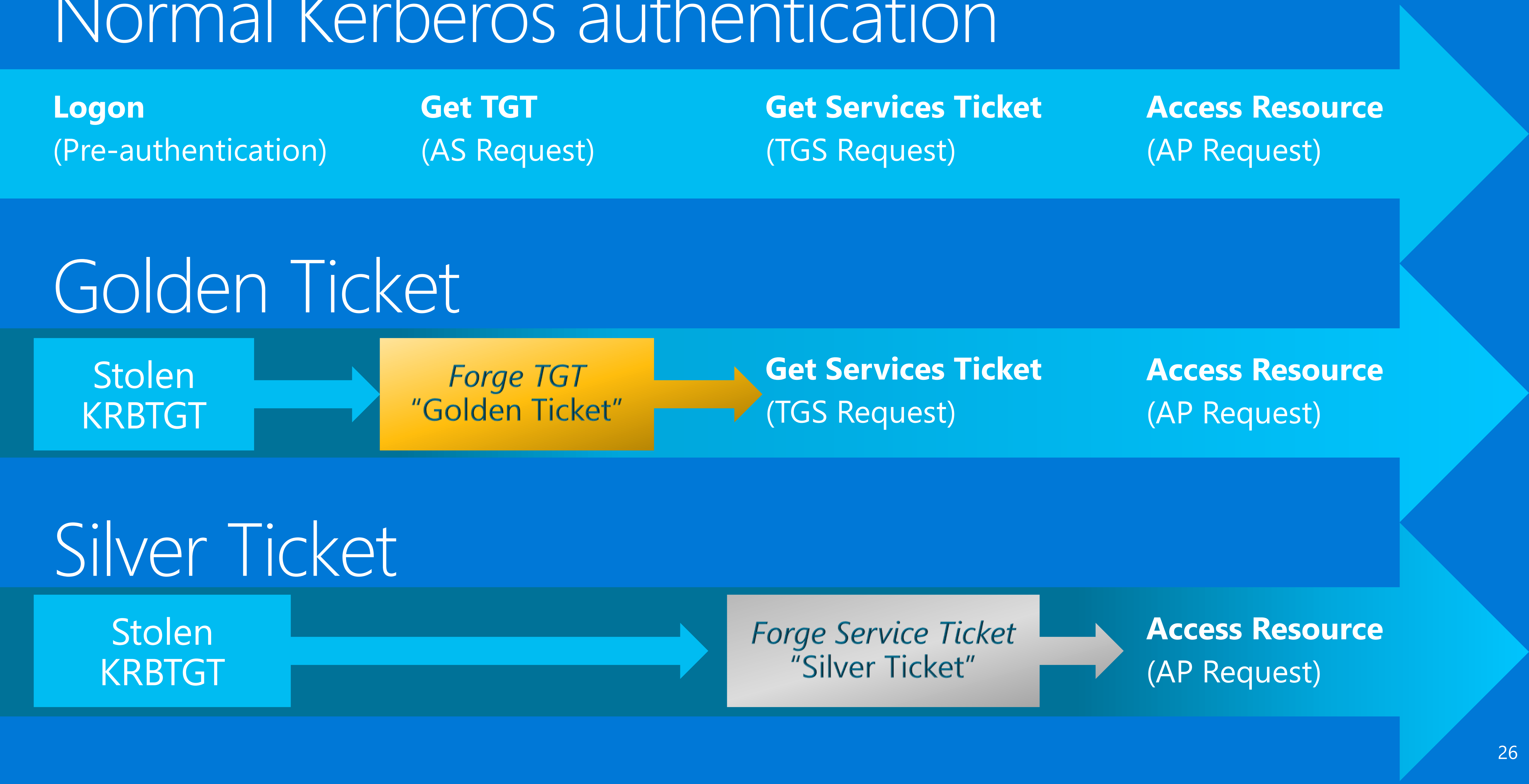
- It's not limited by GPO or others settings ;)
- You can push whatever you want inside
- It's smartcard independent (sorry CISO)

There's more:

A golden ticket is a forged TGT with longer lifespan.

- Typically, a TGT has a 10 **hour** lifetime but the attacker can forge with a 10 **year** lifetime
- Attacker can also change group membership, SID, user name

A silver ticket is a forged service ticket.
Once the TGT is forged, Kerberos <u>does not need</u> to complete **KRB_AS_REQ** or **KRB_AS_REP**, ***essentially skipping steps 1 and 2***, and the authentication portion with the Domain Controller.



Normal Kerberos authentication

Logon
(Pre-authentication)

Get TGT
(AS Request)

Get Services Ticket
(TGS Request)

Access Resource
(AP Request)

Golden Ticket

Stolen
KRBTGT

Forge TGT
"Golden Ticket"

Get Services Ticket
(TGS Request)

Access Resource
(AP Request)

Silver Ticket

Stolen
KRBTGT

Forge Service Ticket
"Silver Ticket"

Access Resource
(AP Request)

Golden tickets and silver tickets

Impact of a Stolen KRBTGT Account Key:

Attacker "becomes a DC"

- Can issue TGTs for any account in the domain ("Golden Ticket")
- Can issue Service Tickets for any account/service in the domain ("Silver Ticket")
- Can forge any attributes (group memberships, validity period, etc.)
- Can create tickets for accounts that don't exist

Extremely difficult to detect fake tickets

This is a post-compromise "attack"

- Only possible if Domain/Forest is already compromised
- Recovery must include resetting KRBTGT and many other means of control
- You might have to rebuild your entire on-premises Active Directory forest…

The **How**:

1. Attacker sends spear phishing email and gets access to a system
2. Attacker uses hacker tool to grab domain admin's hash and gains access to DCs (Domain Controllers)
3. Attacker grabs KRBTGT hash and uses hacker tool to create a golden ticket
4. Attacker can act as user and exfiltrate data

Golden tickets and silver tickets

Why is it bad?

No authentication (KRB_AS_REQ) is done with the DC (for example, **10 YEARS**!)

Gives attacker long term access, assuming they maintain remote access persistence

Brute force attacks

The **What**:

Brute force attack is the technique of trial-and-error or rainbow tables to decipher encrypted passwords (hashes)

Typically very slow to crack a password, but GPUs are speeding the process up – "25-GPU cluster cracks every standard Windows password in less than 6 hours"

http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

Attacker needs the hash or NTDS.dit to execute the attack

Software typically runs against the database looking for hashes that match basic or other sample passwords

Attacker needs admin access to get the hash or database, so might be used in longer campaigns

The **How**:

1. Attacker sends spear phishing email and gets access to a system

2. Attacker uses hacker tool to grab DA hash and gains access to DC

3. Attacker exports AD database (NTDS.dit)

4. Attacker can then go offline and Brute force attack the hashes in the database

Brute force attacks

Why is it bad?

Attacker can gain plaintext passwords via Brute force attack

Attacker can run the attack offline and doesn’t alert customer

Once the passwords are discovered attacker can remote in, like users, assuming Username/Password authentication

Remote code execution

The **What**:

Attackers can use vulnerabilities to execute malicious code against a machine and gain control of the machine.

- Typically attackers try to escalate privileges or grab credentials once they are in
- Attackers typically use known vulnerabilities, but the system hasn't been patched
- Zero-days or unknown vulnerabilities are sometimes used as well

The **How**:

1. Attacker sets up attack web site, user drives by or is spear phished to hit the site

2. Web site executes code using a vulnerability in the browser

3. Code allows attacker to take control of the system

4. Attacker now has access, most likely full administrator access, and can execute further steps against the network

Remote code execution

Additional Considerations…

These attacks require local administrator privileges on the target endpoint. The tools need admin privileges to access and change LSASS memory

This is why it is so important that users are just that, users of the machine, not admins.

Spear phishing is pretty common, but web site attacks are possible too

```
C:\Users\NEERDOWELL>_
```

What does all of this mean?

DCs are the keys to the kingdom…

and need to be protected as such

Credential Theft attacks are very hard to detect…

an attack typically looks like normal user authentications at the DC

It’s too costly to monitor endpoints for these attacks…

which means most customers never see them

The bottom line…

Workstations
Servers
Webshells on the perimeter
'Skeleton key' on DCs
VPN server
Network device
Printers

Malware implants

Unauthorized accounts
Stolen credentials
Password guessing based history/DIT
PKI Credentials

Account abuse

Management tool configurations
ACLS on Services
Group Policy Modification
Script Modification
ACLs on AD objects
DNS lookup redirection
Enabling SQL xp_cmdshell

Abuse of systems and configurations

Target AD DS & Identities
On-premises Active Directory controls access to business assets
Attackers commonly target AD DS and IT Admins

Parasitic infected files on shares and user profiles

…others we do not know about yet

Module review

In this module, you learned what credential theft attacks are including:

- Pass-the-Hash (PtH)
- Pass-the-Ticket (PtT)
- Overpass-the-Hash
- Golden Ticket
- Remote Code Execution
- Brute force attack

What questions do you have?

Questions & Answers

Microsoft