SharkFest '16 Europe

Common Packets in a Windows / Active Directory Environment

2016-10-18

#sf16eu

Uli Heilmeier

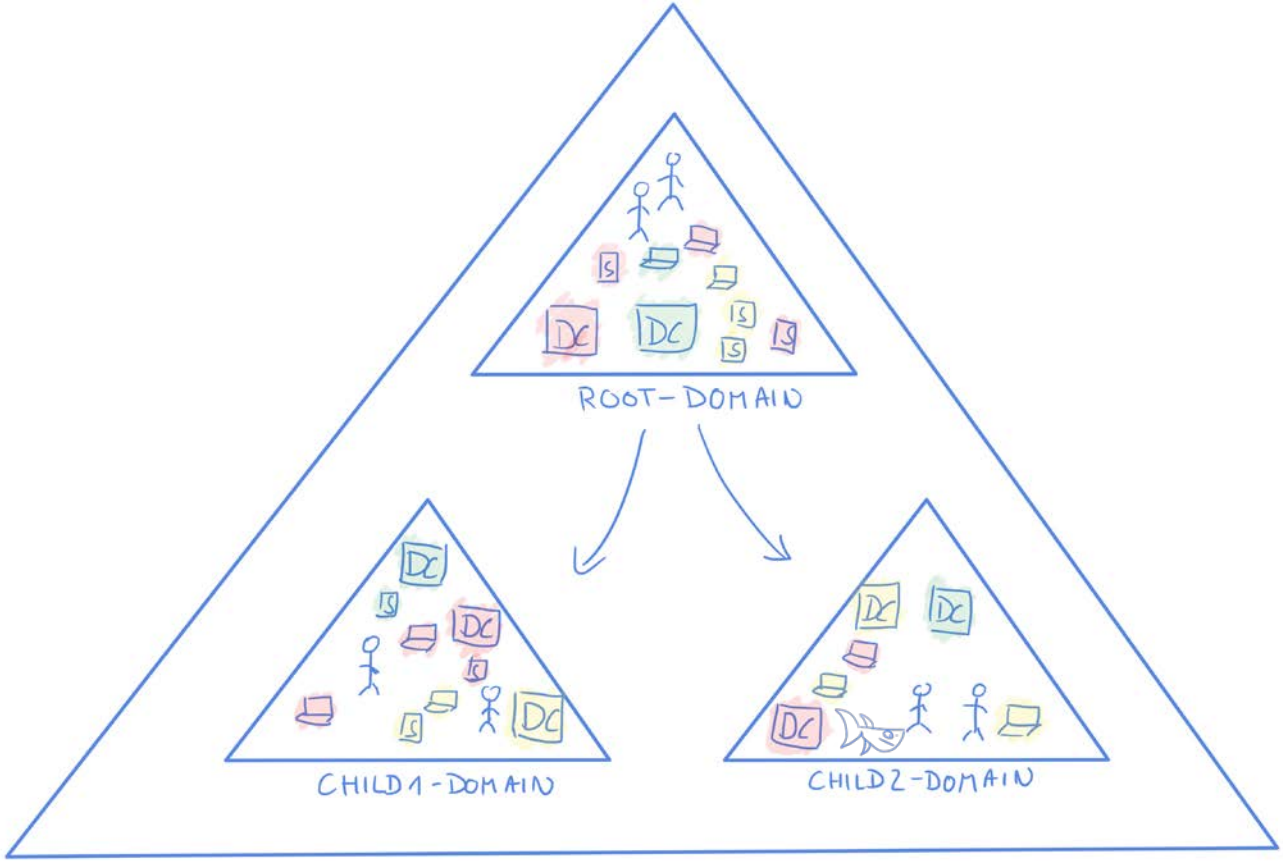
Goals

Goals

- Overview of protocols used by Windows clients
  - DHCP
  - DC and Site discovery
  - Directory information
  - Authentication
  - PXE

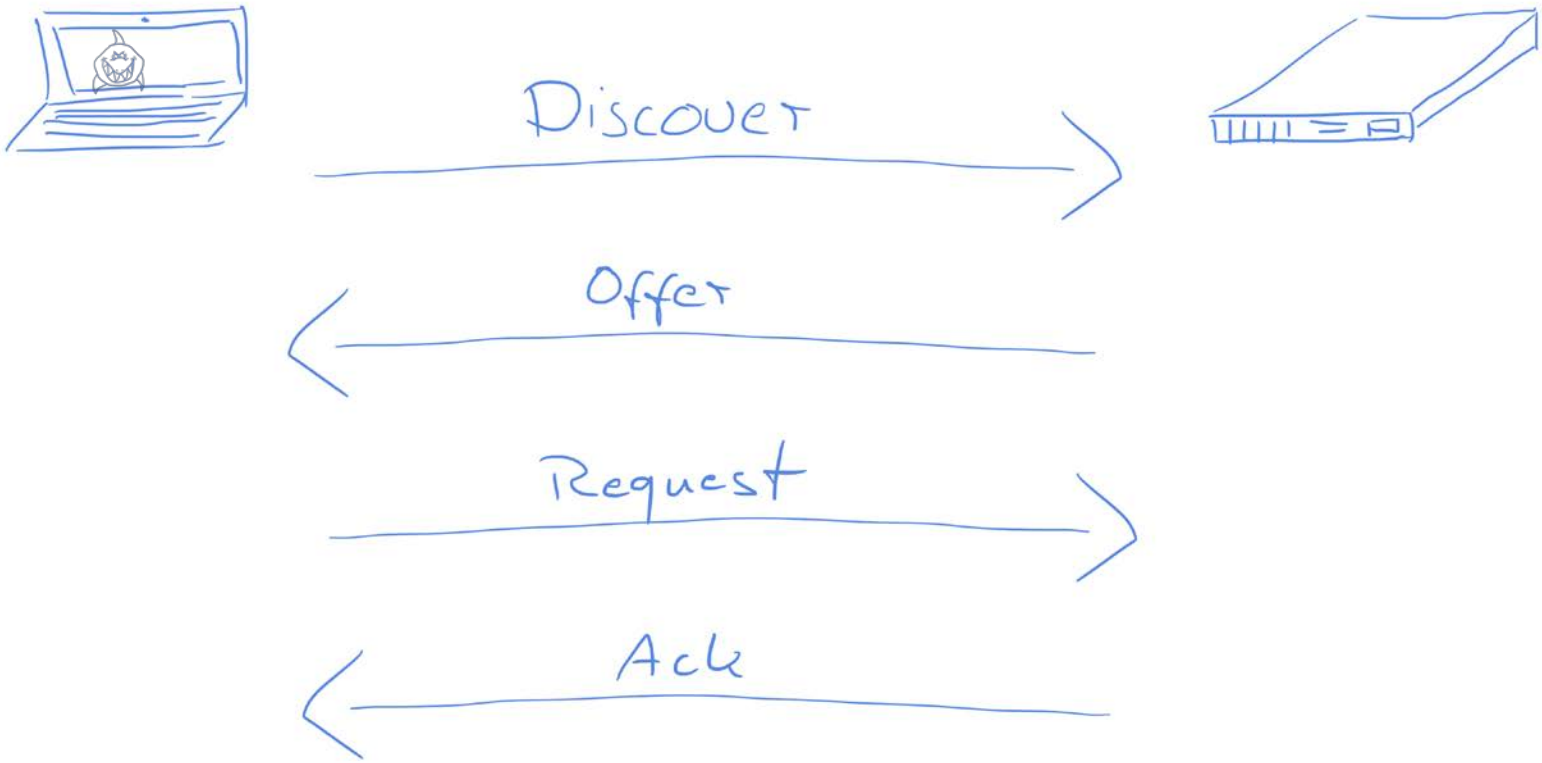
Terms

- **Active Directory (AD):** Distributed multi-master database with user, computer, groups, etc. objects
- **Domain:** A set of users, groups, computers sharing a common directory database, security objects, trust relationship
- **Domain Controller:** A server running different services to control a AD
- **Forest:** Top level container houses domains
- **Site:** Groups of geo locations


ROOT-DOMAIN
CHILD1-DOMAIN
CHILD2-DOMAIN

DHCP

PCAP Time


Discover
Offer
Request
Ack

DC and Site discovery

PCAP Time

DC and Site discovery

- DNS
  - SRV _ldap._tcp.dc._msdcs.<domain-name>
  - SRV _ldap._tcp.<site-name>._sites.dc._msdcs.<domain-name>
  - A/AAAA <domain-name>
- CLDAP
  - Netlogon attribute

DC and Site discovery

- Tools
  - nslookup
  - nltest
    - nltest /dsgetsite
    - nltest /dsaddresstosite:<computer-name> or <ip-address>

Directory Information

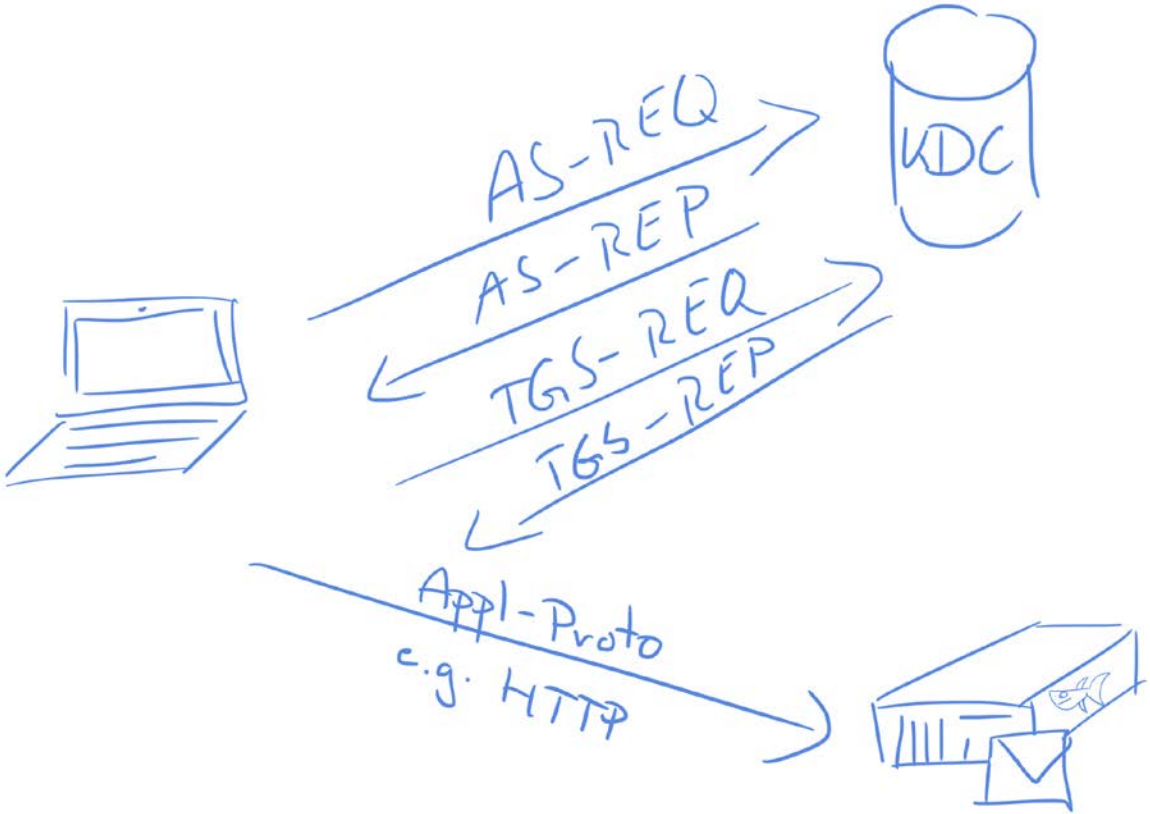
PCAP Time

Directory Information

- LDAP
- SMB
- DCERPC
  - Portmapper
  - UUID-Service

Authentication

PCAP Time


AS-REQ
AS-REP
TGS-REQ
TGS-REP
KDC
Appl-Proto
e.g. HTTP

Authentication

- Kerberos
  - setspn –L <account-name>
- NTLM

PXE

PCAP Time

Questions?

Email: uh@heilmeier.eu
Twitter: @pizza_4u