Informationssammlung

NETWORKING ACADEMY DAY 2017

REGENSTAUF 31.3.2017

Bestandsaufnahme

Cyberthreat Real-Time Map

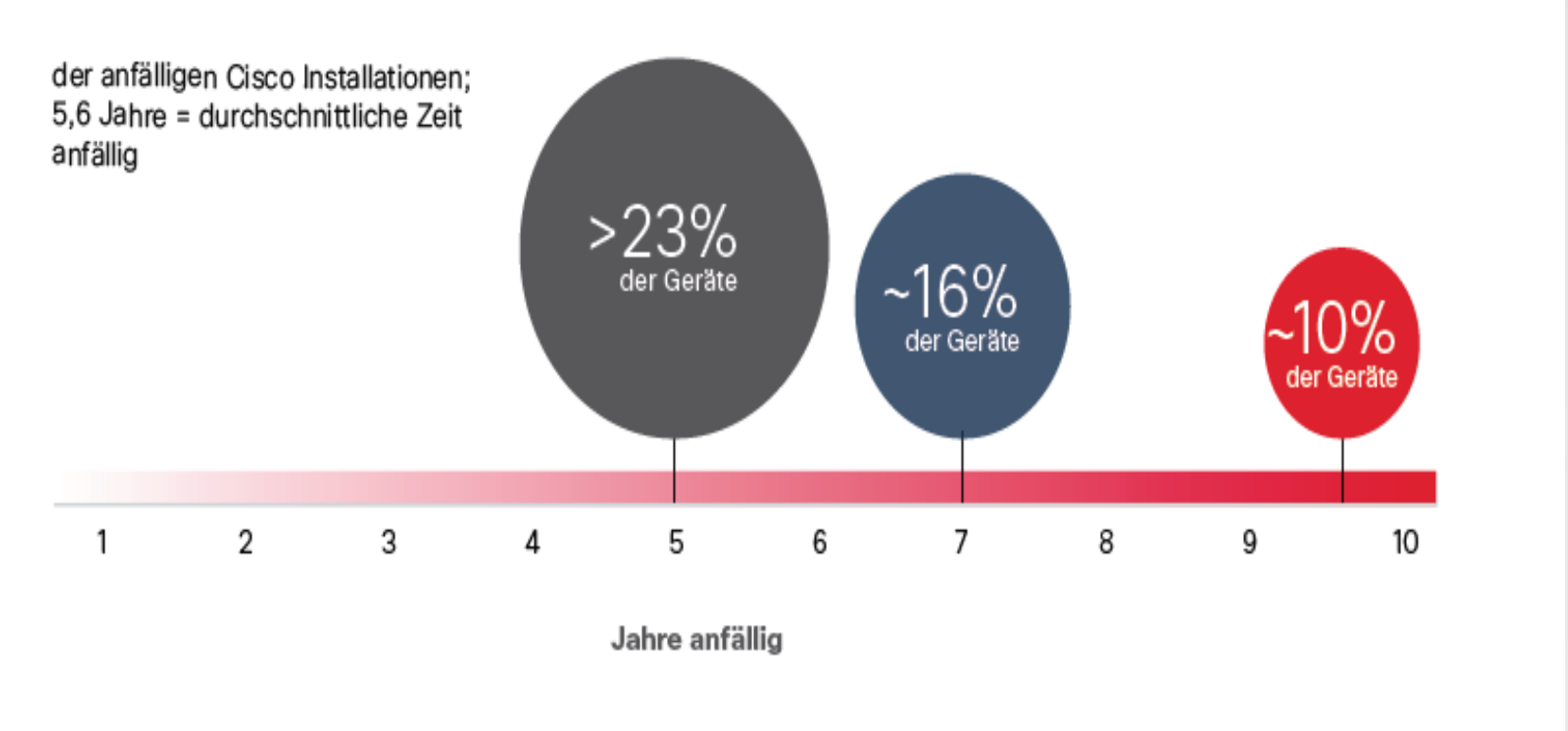
Die größten Datenlecks

Netzanalyse

- 2015 untersuchte Cisco 115.000 Geräte, um auf die Risiken von unzureichend gepflegter, veralteter Infrastruktur und nicht behobener Sicherheitslücken im IOS aufmerksam zu machen.
- 106.000 Geräte **(92 Prozent)** verwendeten Software mit bekannten Sicherheitslücken.
- 2016 wurde bei einer Stichprobe von Cisco Geräten geprüft, inwieweit auf zentralen Infrastrukturelementen (Router und Switches) vorhandene bekannte Sicherheitslücken zurückdatieren.
- Insgesamt wurden bei 103.121 an das Internet angebundenen Geräten bekannte CVEs (Common Vulnerabilities and Exposures) aus den Jahren 2002 bis 2016 entdeckt**. Jedes Gerät** wies dabei im Durchschnitt 28 bekannte Sicherheitslücken auf.

Quelle: Cisco Midyear Cybersecurity Report 2016

Geräte



Quelle: Cisco Midyear Cybersecurity Report 2016

Folge: Viele Cisco-Geräte sind gefährdet.
Der Angreifer muss sie nur ausfindig machen

Angriffsvorbereitung

- Im Folgenden wird gezeigt, wie man Informationen sammelt, um diese für Angriffe zu nutzen.

- Beispiel: Ein Angreifer sucht Geräte mit offenem Telnet-Port im Internet

Warum sind so viele Geräte nicht aktualisiert?

Ursachen

- Obwohl Patches für erkannte Sicherheitslücken schnell verfügbar sind, werden diese vielfach nicht installiert.
- Folge: Es entsteht ein unbeschränktes Zeitfenster, in dem Angreifer Exploits (Angriffsskripte) gegen diese Komponenten ausführen können, d.h. die Kenntnis von CVEs (Common Vulnerabilities and Exposures) ist extrem nützlich

Warum werden keine Updates vorgenommen?

Nachlässigkeit

- Abwarten bis Infrastruktur erneuert wird
- Update aufschieben, weil mühevoll – Folge: Ablauf des Supports, keine Aktualisierung möglich
- Cisco-Geräte sind Teil kritischer Infrastrukturen ohne Redundanz!! Jeder prüfe seinen Access-Bereich. Daher können sie ohne Netzausfall nicht aktualisiert werden

Wie werden angreifbare Systeme entdeckt?

Entdeckung durch

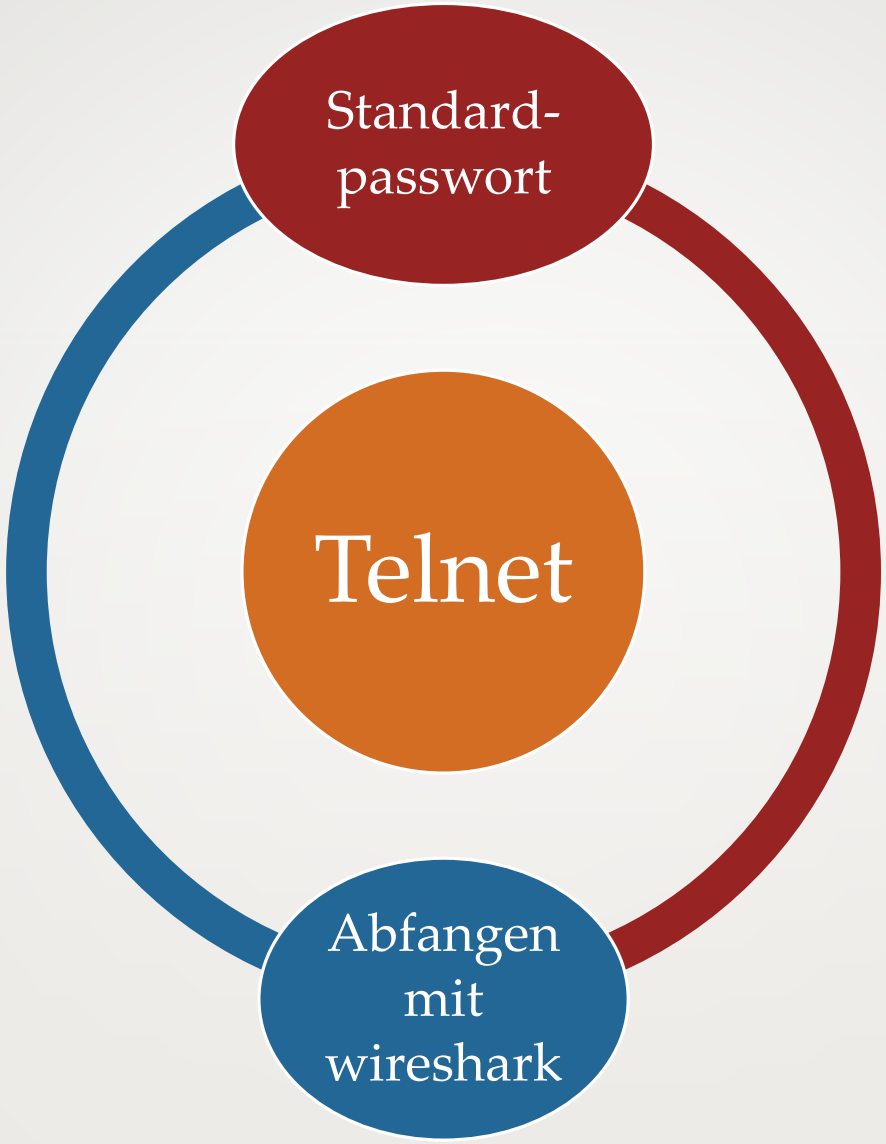
- Einbruch
- Scannen

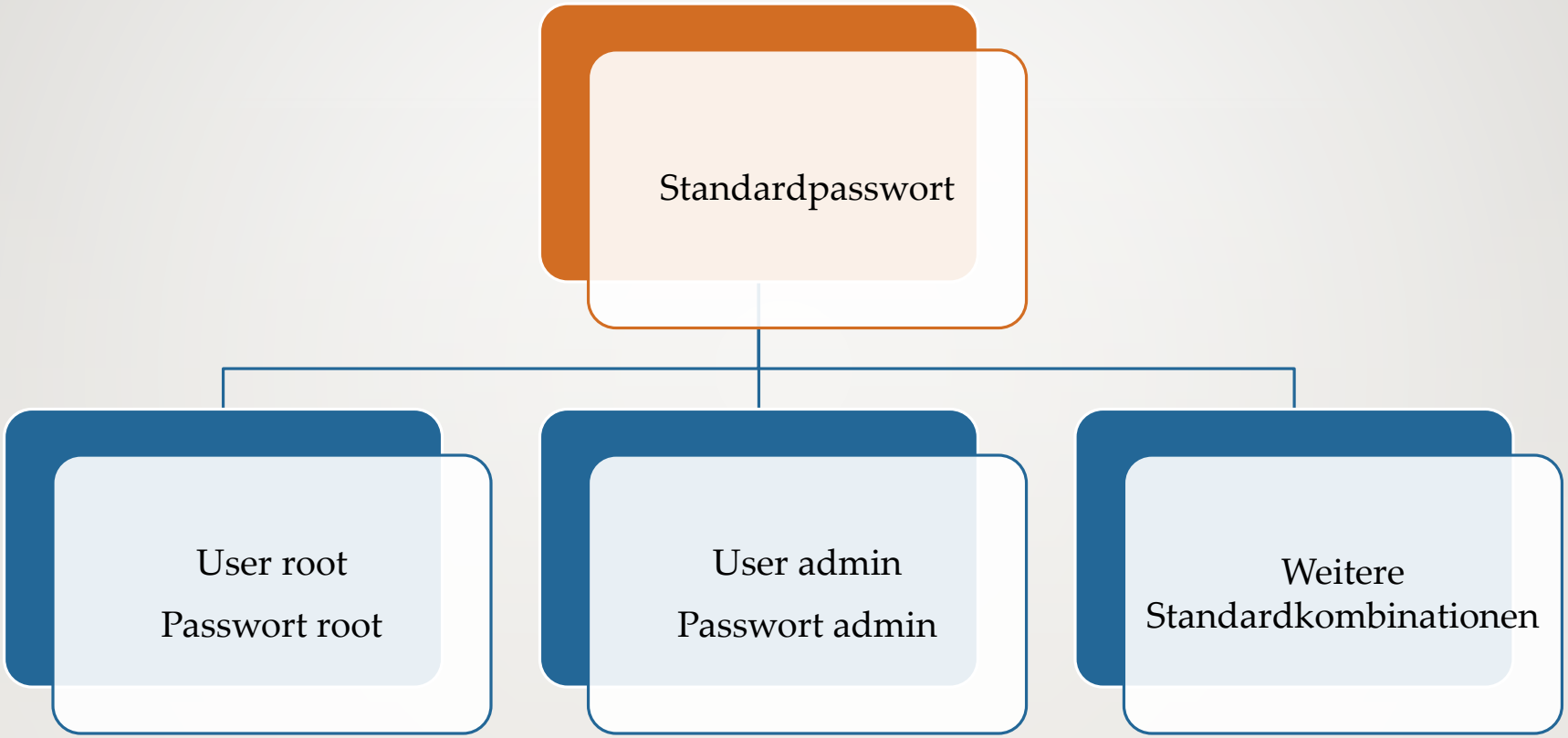
Einbruch

- Werkzeug: Datenbank
  - Shodan

Shodan mit Einträgen bzgl. Systeme des Internets der Dinge

Im Suchfeld "default password telnet“ einfügen,
um Telnet-Ports von Cisco-Routern zu finden
oder HTTP-Server mit Cisco Switch port:"80" product:"Cisco IOS http config"
oder aktiviertes CDP

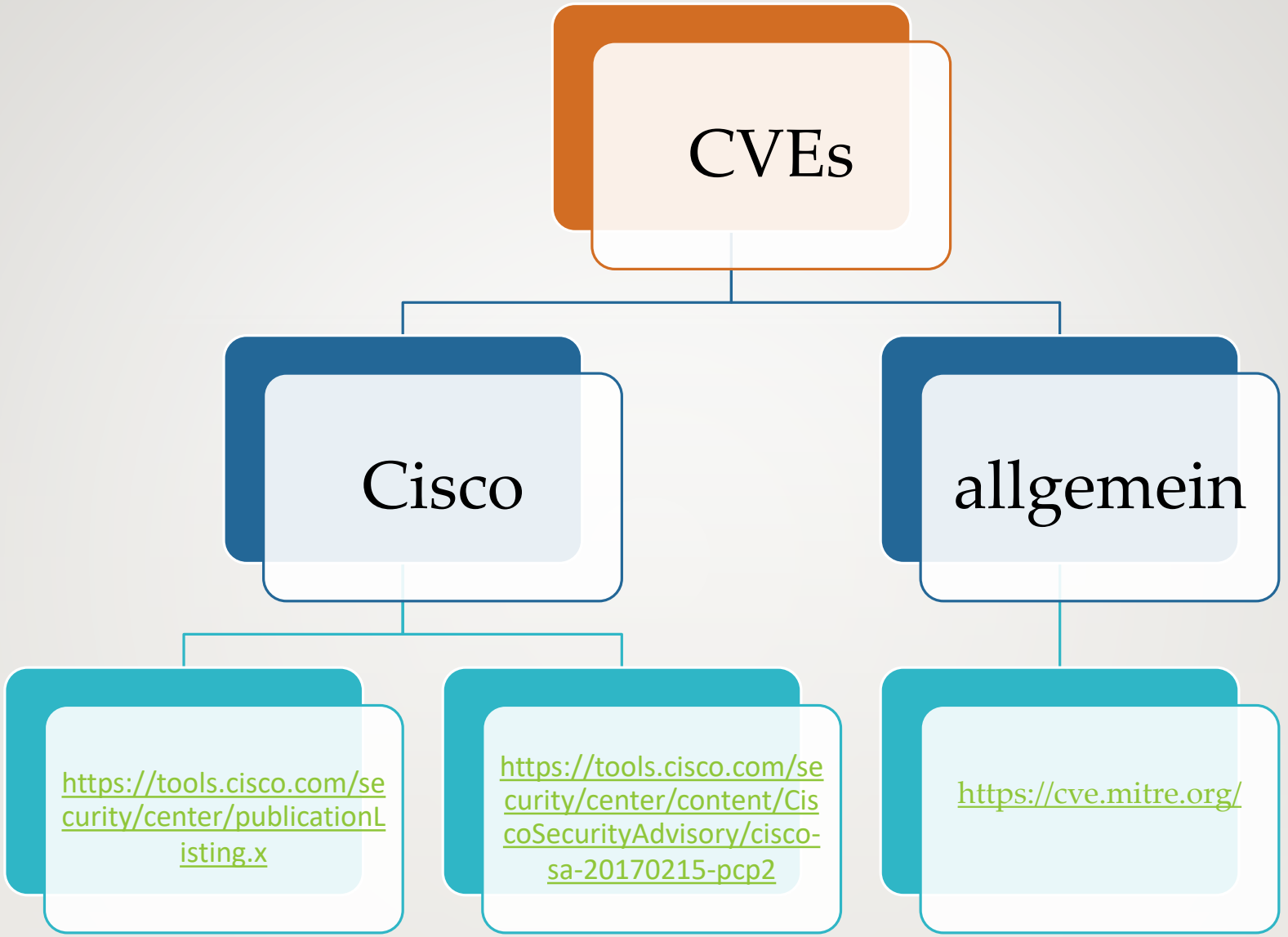

Standard-
passwort
Telnet
Abfangen
mit
wireshark


Standardpasswort
User root
Passwort root
User admin
Passwort admin
Weitere
Standardkombinationen

Bedrohung CDP

- Auf den Cisco-Geräten standardmäßig aktiviert
- Gibt Auskunft über
  - Gerätetyp
  - IP-Adresse
  - IOS-Version
  - Interfaces
- Ausgangspunkt für die Erstellung einer Topologieübersicht

Welche Verwundbarkeiten existieren? Wo sind diese zu finden?


CVEs
Cisco
allgemein
https://tools.cisco.com/security/center/publicationListing.x
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-pcp2
https://cve.mitre.org/

Wo und wie sind angreifbare Systeme zu finden?

Mechanismus

- Netzscan

Grundsatzfrage: Ist überhaupt ein Netzscan möglich?

Wie findet ein Angreifer mögliche Ziele bei 2^{32} IP-Adressen und 2^{16} möglichen Ports?
Existieren damit nicht zu viele Kombinationen von IP-Adresse und Port, um diese gänzlich zu durchsuchen?

Dies war bis 2013 gängige Meinung.
Danach entwarf ein Unbekannter auf Basis des bekannten Tools nmap das „Carna-Botnetz“ und scannte den gesamten IP-Adressraum

Der Datensatz ist unter http://www.scans.io einsehbar.
Die Seite bietet regelmäßige Scans zu den Ports 80 und 443

Nmap-Demo gegen Netz der Hochschule Flensburg als Basis eines internetweiten Scans

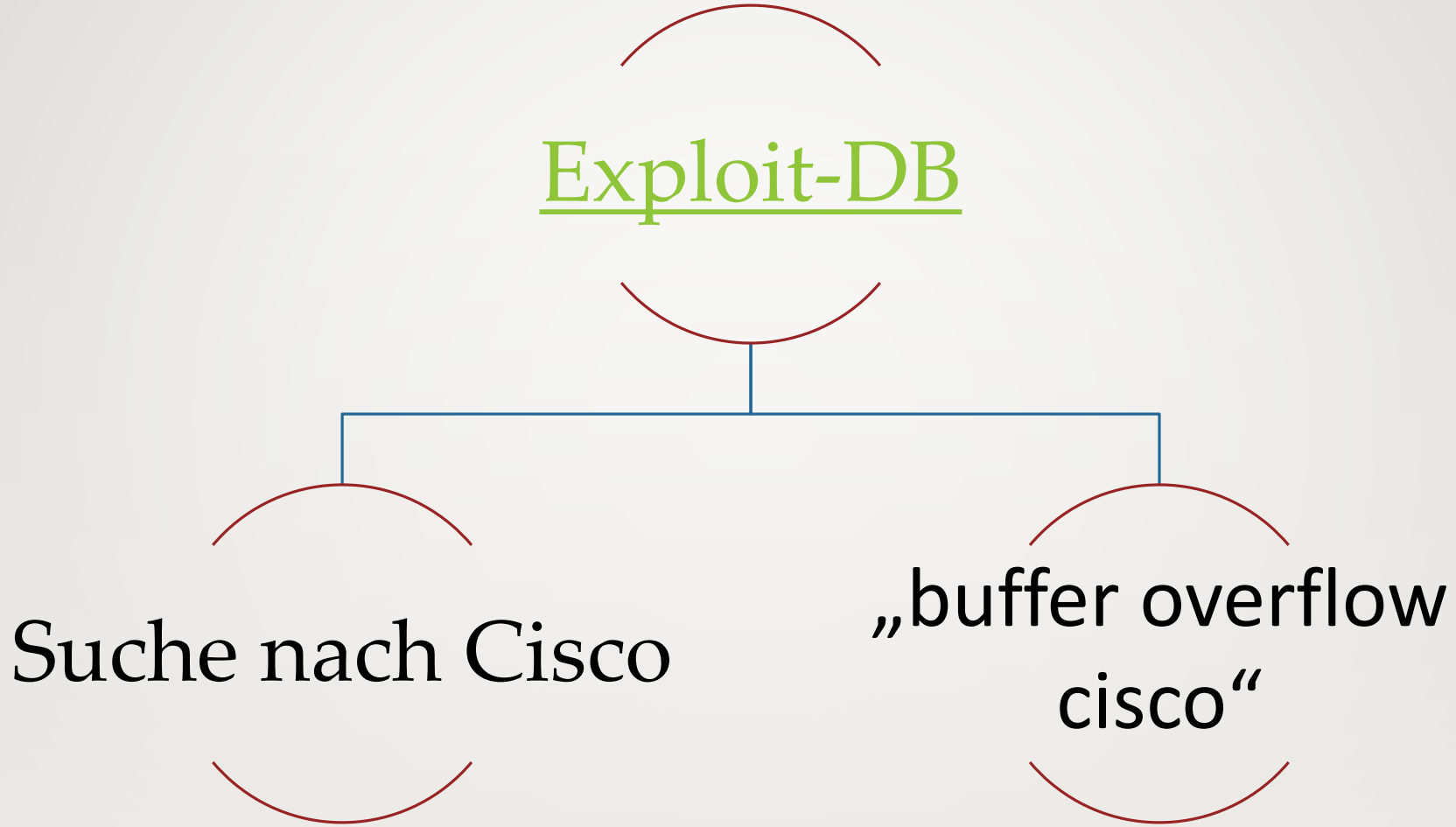
Werkzeuge

- Mit
  - Zmap (Universität Michigan)
  - Masscan

existieren mittlerweile zwei weitere Tools für einen internetweiten Scan.

Folge: bei der Vergabe von Subnetzen für IPv6 **keine fortlaufende Nummerierung** verwenden!!

Gibt es Exploits, die sich gegen CVEs richten?


Exploit-DB
Suche nach Cisco
„buffer overflow cisco“

Weitere Informationsbeschaffung

Pre-Pentest-Phase

- Die Vorbereitung eines Penetration-Tests besteht in der Informationssammlung über das Zielobjekt. Dazu können eine Vielzahl weiterer Tools verwendet werden.

Network Scanner

- SoftPerfect Network Scanner liefert Infos zu:
  - IP-Adressbereich,
  - DHCP-Server,
  - SNMP-Devices,
  - doppelte IP-Adressen,
  - Netzwerkfreigaben

Robtex

- Die Webseite www.robtex.com zeigt u.a.
  - DNS-Einbindung,
  - weitere Domains
  - Mail-Server
  - Autonome Systeme
  - Domain-Server

als Graphik mit IP-Adresse 193.175.191.141 (durch ping in Erfahrung bringen)

Portscanner

- nmap –sP –PR IP-Adressbereich arbeitet als ARP-Scanner
- nmap -v –script=targets-ipv6-multicast* nmap-Skripte, die im Namen den String „targets-ipv6-multicast“ aufweisen
- nmap -sV -p 445 –script=smb-check-vulns 193.174.250.0/24 Test einer Schwachstelle über einen Netzwerkbereich
- nmap -6 fe80::f442:baa2:56e7:6681%eth0 scan auf ipv6 link-local-Adresse
- Networktrafficview-x64 zeigt den Datenverkehr des lokalen Rechners

NetworkTrafficView.exe

Vielen Dank!