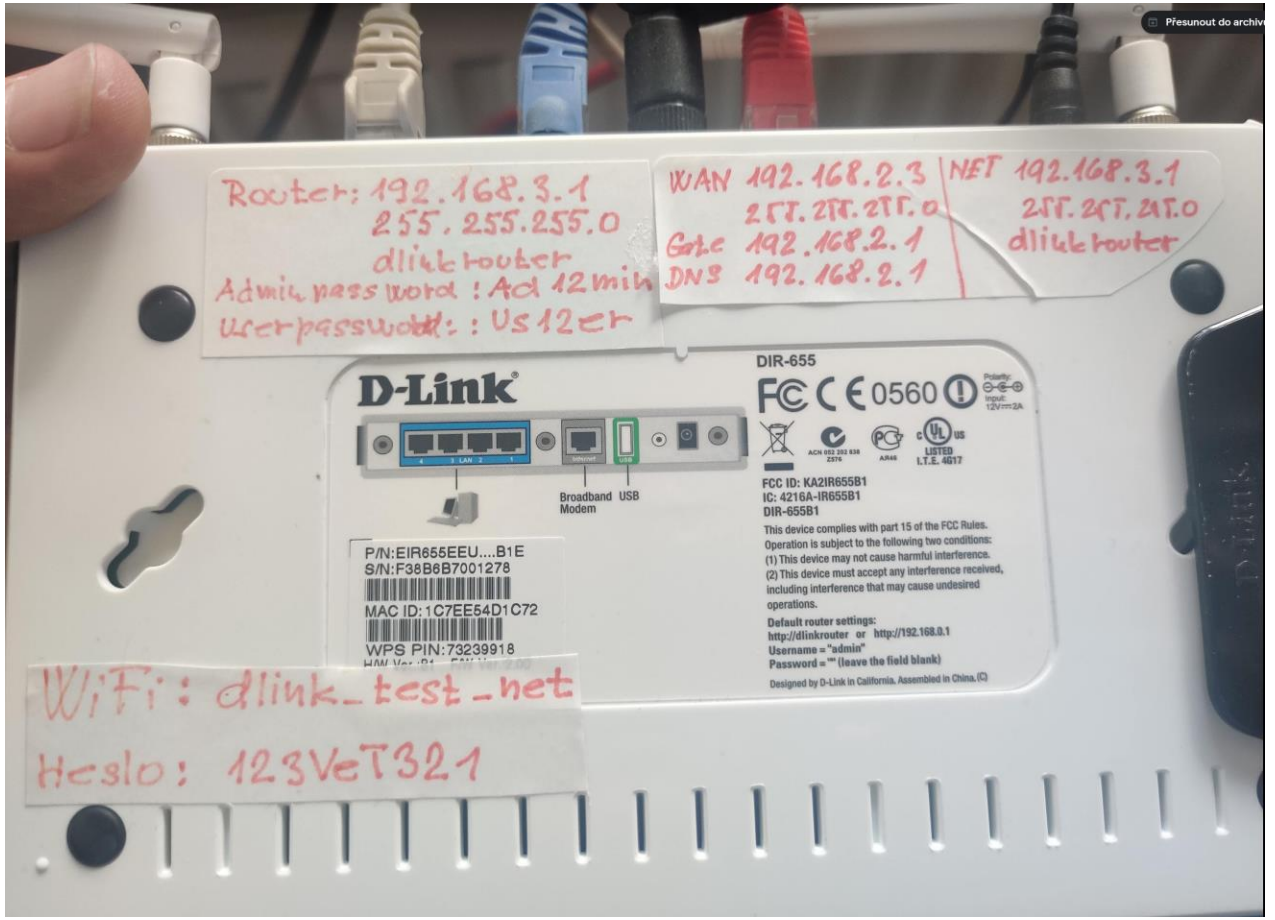
Automatizace skenování zranitelností a penetračního testování

Pavel Gadžuk

Co je HiraGuard

- Automatizovaná platforma pro skenování zranitelností a penetrační testování
  - Provádí pravidelné automatizované testy
- Automatizace testovacích procesů
  - Integrace s nástroji pro skenování sítí a vyhodnocování zranitelností
  - Integrace na ofenzivní nástroje pro vyhodnocování rizika zneužití nalezených zranitelností
  - Jednotlivé nástroje jsou spouštěny automaticky na základě rozhodovacího stromu
- Výsledky jsou agregovány a prezentovány jako celek
  - Samoobslužné cloudové rozhraní pro správu výsledků testů (Azure)
    - Není nutné manuálně srovnávat výsledky – vše je v jednom dashboardu

Realita



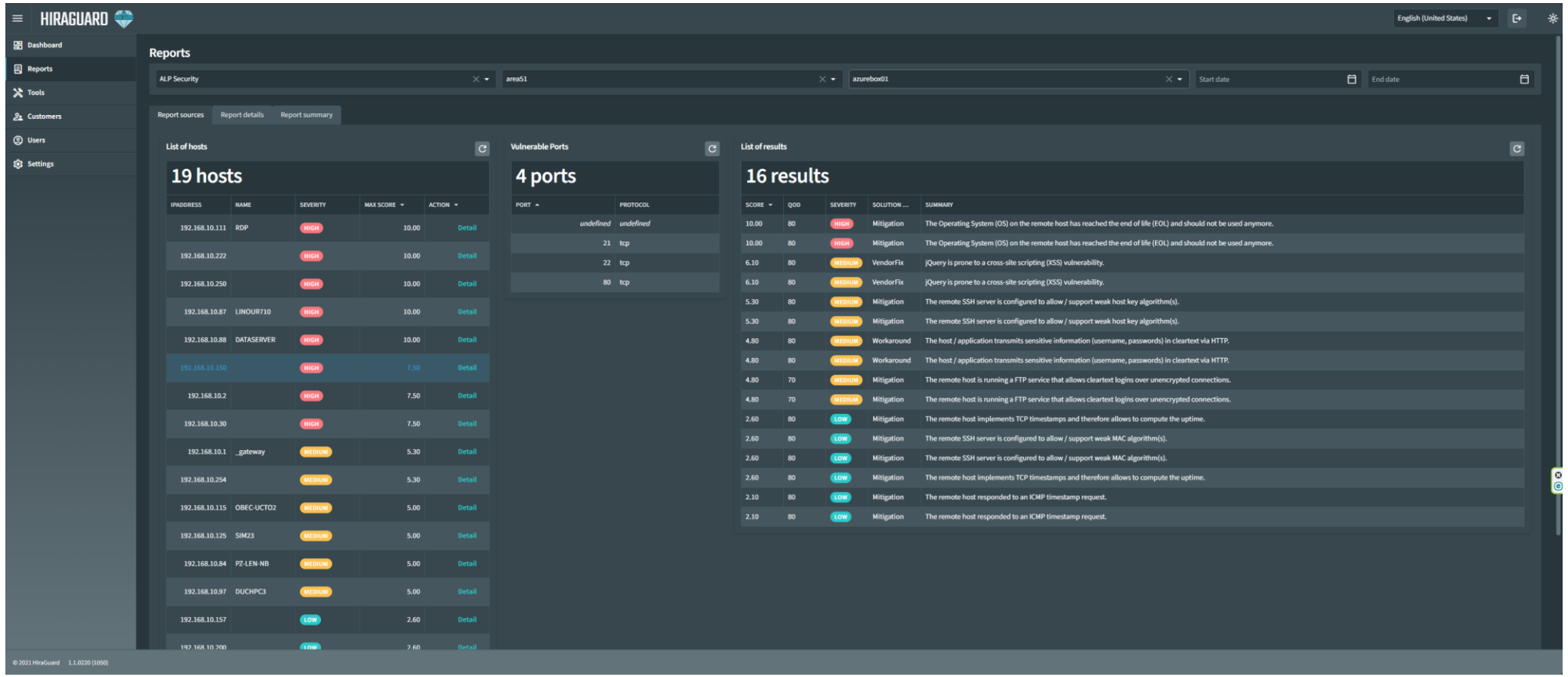
Jihočeský kraj chce efektivněji ochránit nemocnice

- Přes dosud neexistující právní rámec pro řešení kybernetických hrozeb například Jihočeský kraj vzal iniciativu do svých rukou a založil vlastní centrum kybernetické bezpečnosti. Do projektu investoval přes 100 milionů korun a slibuje si od něj lepší ochranu nemocnic, úřadů, škol a dalších krajských institucí.
- „Když jsme si udělali analýzu, ukázalo se, že jednotlivé nemocnice jsou schopny přípravu realizovat, ale jen do míry odpovídající jejich velikosti a ekonomické síle," zdůvodnil rozhodnutí o založení centra jihočeský hejtman MARTIN KUBA. Centrum má posílit obranu a předcházet tím ztrátám dat a paralyzování chodu klíčových institucí.

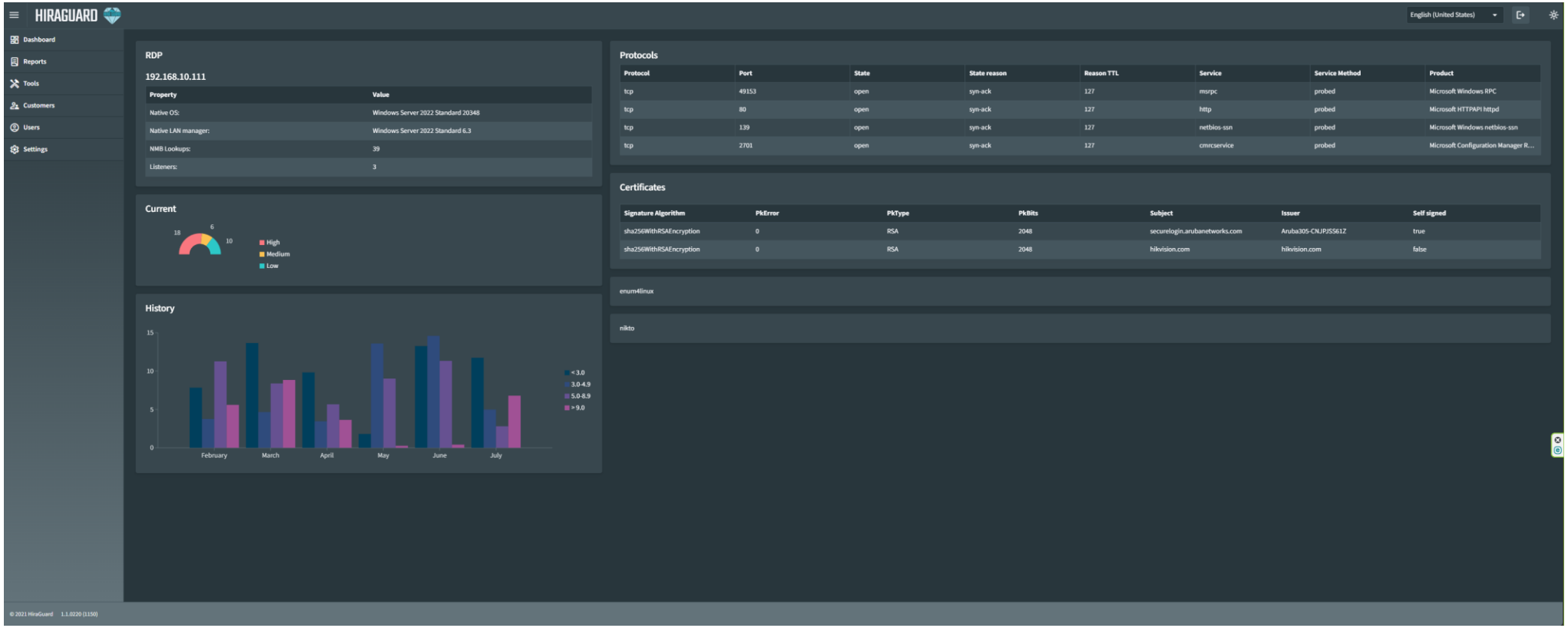
Dashboard

- Prezentace výsledků testů
  - Jednoduché rozhraní
  - Vše je zpracovává automaticky
  - Máte přehled o stavu sítě v čase
  - Vyhodnocování výsledků testů

Dashboard


HIRAGUARD
English (United States)
Dashboard
Reports
Tools
Customers
Users
Settings
Reports
ALP Security
area51
azurebox01
Start date
End date
Report sources
Report details
Report summary
List of hosts
19 hosts
IPADDRESS NAME SEVERITY MAX SCORE ACTION
192.168.10.111 RDP HIGH 10.00 Detail
192.168.10.222 HIGH 10.00 Detail
192.168.10.250 HIGH 10.00 Detail
192.168.10.87 LINOUR710 HIGH 10.00 Detail
192.168.10.88 DATASERVER HIGH 10.00 Detail
192.168.10.150 HIGH 7.50 Detail
192.168.10.2 HIGH 7.50 Detail
192.168.10.30 HIGH 7.50 Detail
192.168.10.1 _gateway MEDIUM 5.30 Detail
192.168.10.254 MEDIUM 5.30 Detail
192.168.10.115 OBEC-UCTO2 MEDIUM 5.00 Detail
192.168.10.125 SIM23 MEDIUM 5.00 Detail
192.168.10.84 PZ-LEN-NB MEDIUM 5.00 Detail
192.168.10.97 DUCHPC3 MEDIUM 5.00 Detail
192.168.10.157 LOW 2.60 Detail
Vulnerable Ports
4 ports
PORT PROTOCOL
undefined undefined
21 tcp
22 tcp
80 tcp
List of results
16 results
SCORE QOD SEVERITY SOLUTION ... SUMMARY
10.00 80 HIGH Mitigation The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.
10.00 80 HIGH Mitigation The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.
6.10 80 MEDIUM VendorFix jQuery is prone to a cross-site scripting (XSS) vulnerability.
6.10 80 MEDIUM VendorFix jQuery is prone to a cross-site scripting (XSS) vulnerability.
5.30 80 MEDIUM Mitigation The remote SSH server is configured to allow / support weak host key algorithm(s).
5.30 80 MEDIUM Mitigation The remote SSH server is configured to allow / support weak host key algorithm(s).
4.80 80 MEDIUM Workaround The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
4.80 80 MEDIUM Workaround The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
4.80 80 MEDIUM Mitigation The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
4.80 70 MEDIUM Mitigation The remote host is running a FTP service that allows cleartext logins over unencrypted connections.
2.60 80 LOW Mitigation The remote host implements TCP timestamps and therefore allows to compute the uptime.
2.60 80 LOW Mitigation The remote SSH server is configured to allow / support weak MAC algorithm(s).
2.60 80 LOW Mitigation The remote SSH server is configured to allow / support weak MAC algorithm(s).
2.60 80 LOW Mitigation The remote host implements TCP timestamps and therefore allows to compute the uptime.
2.10 80 LOW Mitigation The remote host responded to an ICMP timestamp request.
2.10 80 LOW Mitigation The remote host responded to an ICMP timestamp request.
© 2021 HiraGuard 1.1.0220 (1050)

Dashboard


HIRAGUARD
English (United States)
Dashboard
Reports
Tools
Customers
Users
Settings
RDP
192.168.10.111
Property
Value
Native OS:
Windows Server 2022 Standard 20348
Native LAN manager:
Windows Server 2022 Standard 6.3
NMB Lookups:
39
Listeners:
3
Current
18
6
10
High
Medium
Low
History
15
10
5
0
February
March
April
May
June
July
<3.0
3.0-4.9
5.0-8.9
>9.0
Protocols
Protocol
Port
State
State reason
Reason TTL
Service
Service Method
Product
tcp
49153
open
syn-ack
127
msrpc
probed
Microsoft Windows RPC
tcp
80
open
syn-ack
127
http
probed
Microsoft HTTPAPI httpd
tcp
139
open
syn-ack
127
netbios-ssn
probed
Microsoft Windows netbios-ssn
tcp
2701
open
syn-ack
127
cmrcservice
probed
Microsoft Configuration Manager R...
Certificates
Signature Algorithm
PkError
PkType
PkBits
Subject
Issuer
Self signed
sha256WithRSAEncryption
0
RSA
2048
securelogin.arubanetworks.com
Aruba305-CNJPJSS61Z
true
sha256WithRSAEncryption
0
RSA
2048
hikvision.com
hikvision.com
false
enum4linux
nikto
© 2021 HiraGuard
1.1.0220 (1150)

Děkuji za pozornost

Pavel Gadžuk

https://www.hiraguard.com

Powered by