



Open Source Day **2011**

## Przegląd nowych mechanizmów bezpieczeństwa w RHEL6

**Leszek Miś**

**Senior Technology Engineer, Linux Polska**

**RHC{E,X}, RHCVA**

**22.03.2011r.**

# Agenda

- Wprowadzenie
- Minimalna platforma instalacyjna
- LUKS
- SELinux:
  - sVirt (pokaz)
  - sandboxing
- Stack Smashing Protection dla GCC, kernela i pakietów
- SSSD
- SNI oraz mod\_ssl
- Inne niemniej istotne



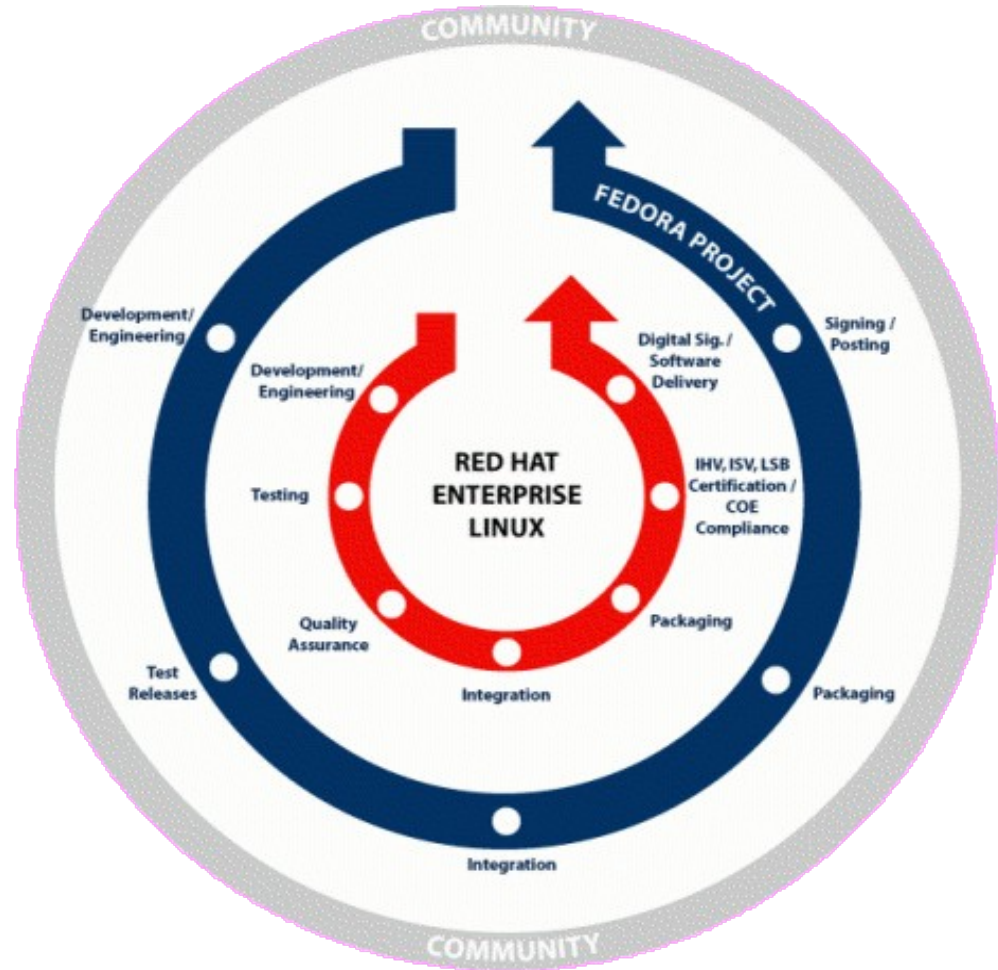
Open Source Day **2011**



# Wprowadzenie

## Red Hat Development Cycle:

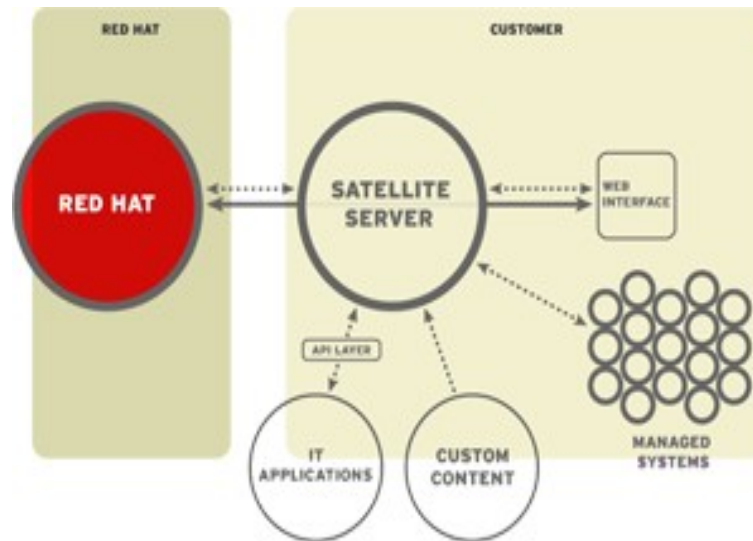
- Stabilność
- Certyfikacje H&S
- Bezpieczeństwo
- 7-10 letni okres utrzymania



Open Source Day **2011**

# Wprowadzenie

- Wbudowane w system operacyjny mechanizmy bezpieczeństwa to kluczowy aspekt wyboru dostawcy oprogramowania
- Publiczne repozytoria vs Red Hat Network



Open Source Day **2011**

# Wprowadzenie

- Niepewna przyszłość darmowych dystrybucji opartych o RHEL
- Duże opóźnienia czasowe przy wydawaniu nowych wersji systemów
- Brak informacji o statusie aktualnych prac
- Brak oficjalnego wsparcia technicznego



Open Source Day **2011**



# Wprowadzenie

- Cykl rozwojowy:  
Testowa Fedora-> produkcyjny RHEL daje rezultaty
- Problemy innych dostawców związane z bezpieczeństwem systemów operacyjnych



Open Source Day **2011**



# Wprowadzenie

- Red Hat Security Response Team
- Akredytacje:
  - EAL4+, Labeled Security Protection Profile, CAPP, RBACPP
  - STIG
- RHEL6 w trakcie certyfikacji CC również dla wirtualizacji (RHEL5+RHEL6)
- Rozwój technologii IT powinien pociągać za sobą rozwój mechanizmów bezpieczeństwa



Open Source Day **2011**





# Minimalna platforma instalacyjna

- Minimalizacja ryzyka
- Zmniejszenie liczby potencjalnie występujących podatności poprzez domyślne usunięcie zbędnych usług/pakietów to podstawowy element szerokopojętego hardeningu systemowego.

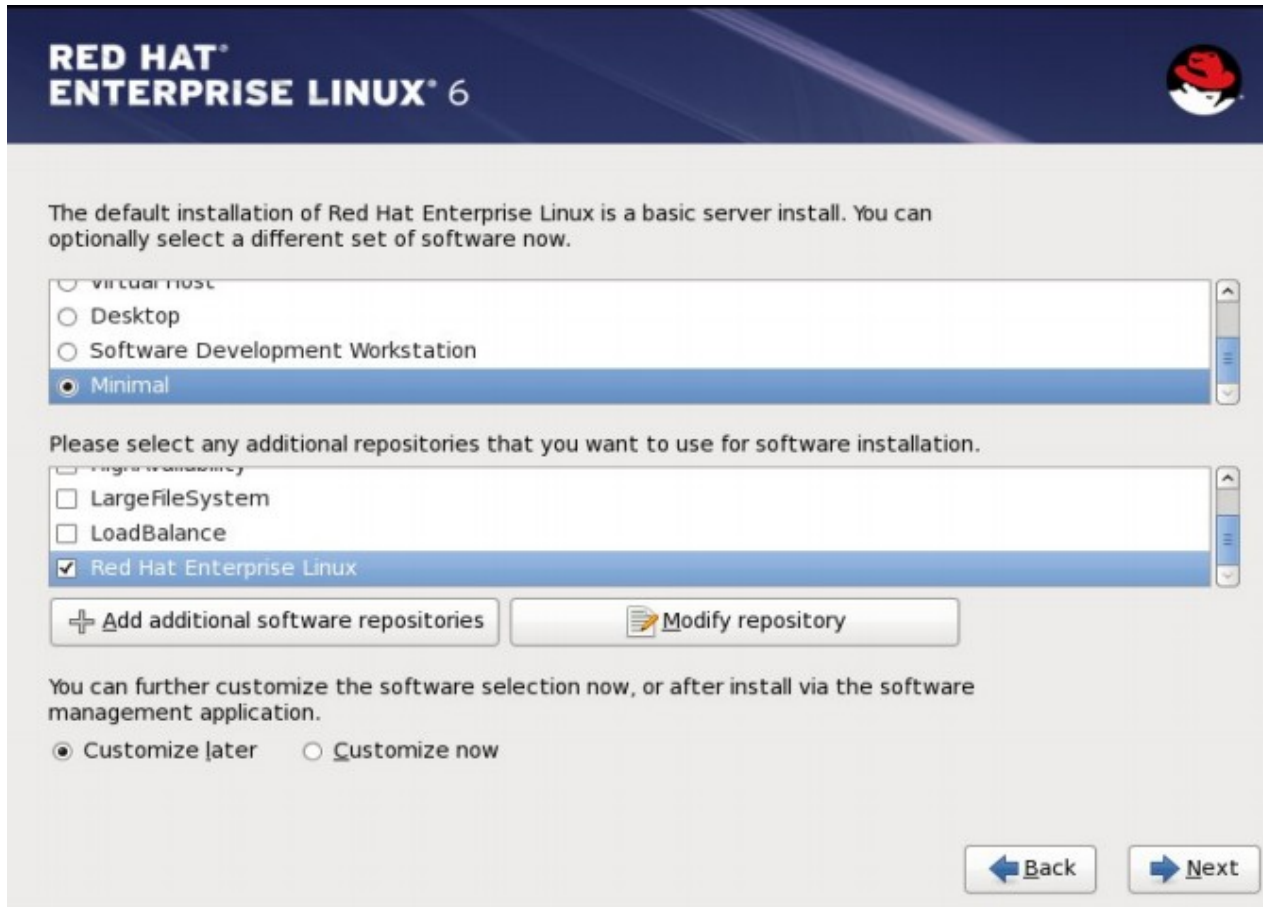


Open Source Day 2011





# Minimalna platforma instalacyjna



**RED HAT®  
ENTERPRISE LINUX® 6**

The default installation of Red Hat Enterprise Linux is a basic server install. You can optionally select a different set of software now.

☐ Virtual Host  
☐ Desktop  
☐ Software Development Workstation  
☒ Minimal

Please select any additional repositories that you want to use for software installation.

☐ LargeFileSystem  
☐ LoadBalance  
☒ Red Hat Enterprise Linux

[+ Add additional software repositories](#) [Modify repository](#)

You can further customize the software selection now, or after install via the software management application.

☒ Customize later ☐ Customize now

[Back](#) [Next](#)



Open Source Day **2011**

# Minimalna platforma instalacyjna

- Zainstalowane pakiety: **223**
- Autostartujące demony: **5** (rsyslogd, sshd, auditd, crond, udevd, postfix)
- SetUID: **7**
- SetGID: **22**
- LibCAP-ng – capabilities

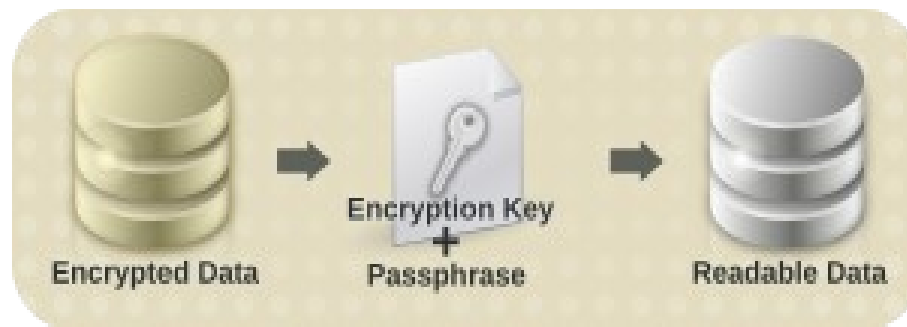


Open Source Day **2011**



# LUKS czyli szyfrowane dane

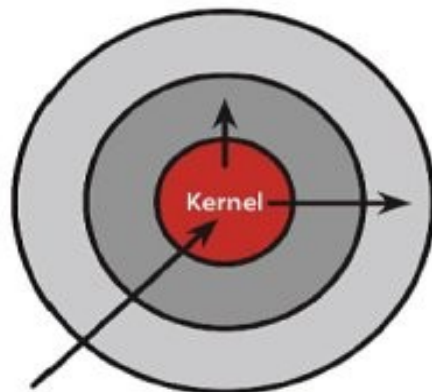
- LUKS czyli Linux Unified Key Setup
- Natywne wsparcie w RHEL6
- Bezpieczeństwo danych składowanych na laptopach
- Bezpieczeństwo danych składowanych na serwerach w odległych datacenter



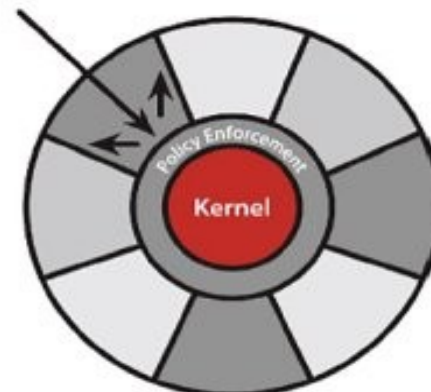
Open Source Day **2011**

# SELinux

Koncepcją polityki bezpieczeństwa SELinux jest określenie jak najmniejszej ilości uprawnień dla danego obiektu (demona, binarki) potrzebnych do jego prawidłowego funkcjonowania. Jest to swego rodzaju firewall aplikacyjny (efekt jaila).



**Discretionary Access Control**  
Once a security exploit gains access to privileged system component, the entire system is compromised.



**Mandatory Access Control**  
Kernel policy defines application rights, firewalling applications from compromising the entire system.

# SELinux

Aplikacja ograniczona polityką MAC może wykonać tylko operacje zdefiniowane w globalnej polityce. Cała reszta operacji jest domyślnie zabroniona.

**Efektywna ochrona przed atakami typu 0-day**

**Rozliczalność użytkowników oraz administratorów**

**Ograniczenie uprawnień użytkowników (czułość, kategorie)**

**Podział uprawnień dla administratorów poszczególnych usług**



Open Source Day **2011**



# SELinux

## RHEL6 – rozszerzona polityka

	Typy	Klasy	Role	Użytkownicy	Bools	
RHEL5	1785	61	6	3	172	
RHEL6	3083	77	13	9	257	



Open Source Day **2011**



# SELinux

- `semanage boolean -l`
- `semanage dontaudit [ on | off ]`
- `semanage module [--enable|--disable] mod`



Open Source Day **2011**





# SELinux - sVirt

- sVirt to zmodyfikowana biblioteka libvirt zintegrowana z mechanizmem SELinux.
- Bezpieczeństwo wirtualizacji osiągnięte poprzez separację uruchomionych maszyn wirtualnych za pomocą mechanizmu MCS.



Open Source Day **2011**



# SELinux - MCS

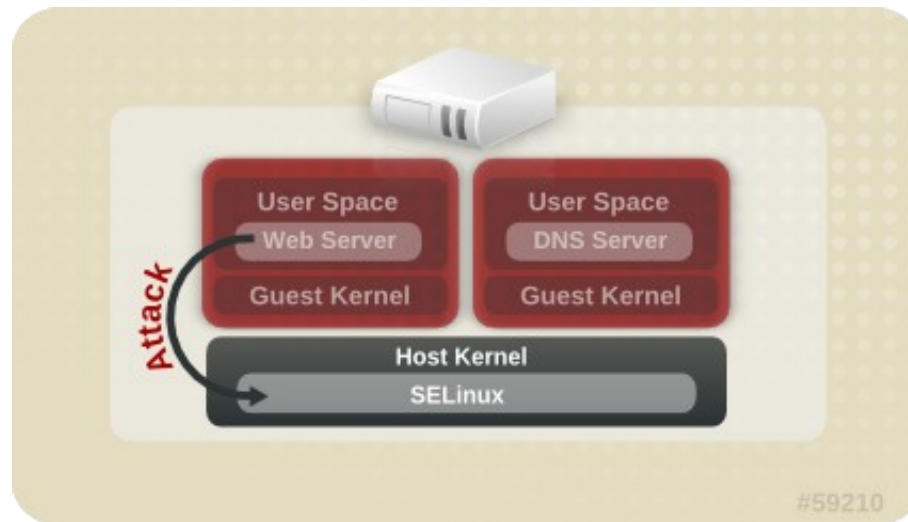
## Multi Category Security:

- przypisywanie kategorii do zasobów systemowych (także do użytkowników)



# SELinux - sVirt

- Dedykowany dla hypervisora KVM
- Każda maszyna wirtualna to pojedynczy proces widzialny w systemie typu host.
- Unikalne oznaczenie kategorią dla systemów VM i ich zasobów



Open Source Day **2011**

# SELinux - sVirt

Pokaz.



Open Source Day **2011**



# SELinux - sandbox

Do czego służy sandbox?

- Tworzenie i uruchamianie aplikacji w odseparowanym środowisku:
  - Generowanie nowej kategorii MCSX
  - Oznaczanie katalogów jako sandbox\_file\_t:MCSX
  - Uruchamianie aplikacji w „piaskownicy” (setexeccon)
- Sandbox -X



Open Source Day **2011**



# SELinux - sandbox

```
$ sandbox `which sshc`
```

```
cannot parse config file /home/crony/.ssh/ssh_connector.conf
```

```
type=AVC msg=audit(1299164978.485:875): avc: denied  
{ open } for pid=13381 comm="ssh_connector"  
name="ssh_connector.conf" dev=dm-11 ino=93657  
scontext=unconfined_u:unconfined_r:sandbox_t:s0:c199,c812  
tcontext=unconfined_u:object_r:home_ssh_t:s0 tclass=file
```

- Xguest – kiosk mode



Open Source Day **2011**



# SSP

## Kernel RHEL6:

- Hybryda wersji 2.6.{32,33,34}
- Domyślnie skompilowany z obsługą Stack Smashing Protection (gcc >=4.2.x)
- ASLR domyślnie włączony
- FORTIFY\_SOURCE dla C++

Kolejny sposób na **utrudnienie** atakującemu procesu exploitowania błędu.



Open Source Day **2011**





# SSP

.config - Linux Kernel v2.6.32 Configuration

Enable -fstack-protector buffer overflow detection

CONFIG\_CC\_STACKPROTECTOR:

This option turns on the -fstack-protector GCC feature. This feature puts, at the beginning of functions, a canary value on the stack just before the return address, and validates the value just before actually returning. Stack based buffer overflows (that need to overwrite this return address) now also overwrite the canary, which gets detected and the attack is then neutralized via a kernel panic.

This feature requires gcc version 4.2 or above, or a distribution gcc with the feature backported. Older versions are automatically detected and for those versions, this configuration option is ignored. (and a warning is printed during bootup)

Symbol: CC\_STACKPROTECTOR [=y]

Prompt: Enable -fstack-protector buffer overflow detection (EXPERIMENTAL)

Defined at arch/x86/Kconfig:1463

Location:

-> Processor type and features



Open Source Day 2011



# SSSD

System Security Services Daemon:

- Zamiennik nss\_Idap
- Offline'owe uwierzytelnienie
- Redukcja obciążenia serwerów katalogowych
- Wsparcie dla wielu domen
- Integracja z IPA Server



Open Source Day **2011**



# Inne

system-config-firewall:

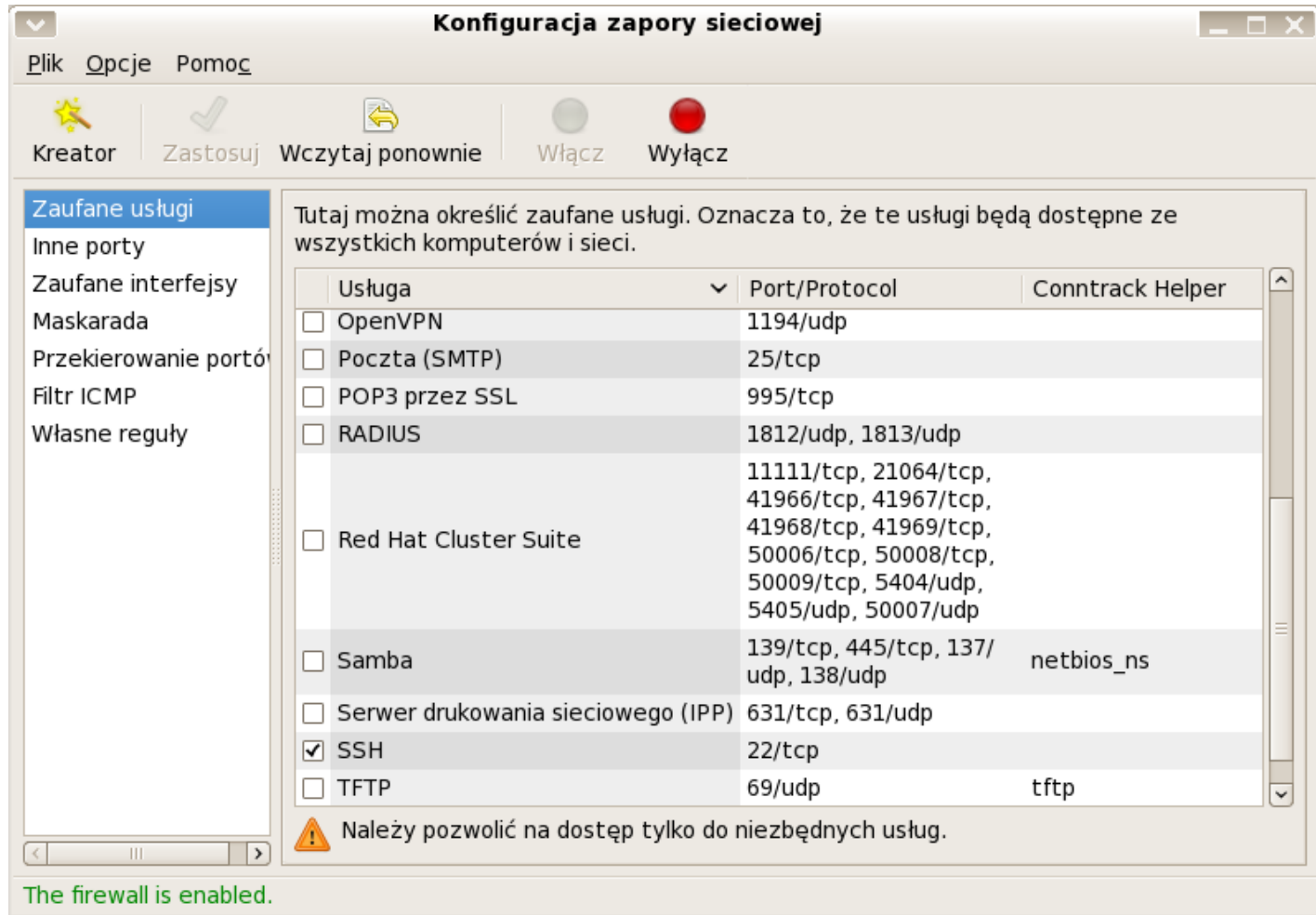
- Rozbudowane możliwości „klikalnego” firewalla:
  - zaufane interfejsy
  - maskarada
  - port forwarding
  - filtrowanie ICMP
- Grupowanie portów per usługa - np. Red Hat Cluster Suite czy też CIFS



Open Source Day **2011**



# system-config-firewall



Open Source Day 2011

# Inne

- SHA256 dla RPM
- rsyslog – zamiennik wysłużonego syslogd
- scrub – bezpieczne kasowanie danych
- sysctl kernel.modules\_disabled=1 (LKMOFF)
- Integracja NetworkManager i Openswan
- Narzędzia do obsługi TPM
- sectool (w RHEL 6.0 jeszcze niedostępny)



Open Source Day **2011**



# Inne - SNI

## httpd 2.2.15 + mod\_ssl - wsparcie dla mechanizmu SNI(Server Name Indication)

```
# strings /usr/lib64/httpd/modules/mod_ssl.so | grep -i sni
```

```
SSLStrictSNIVHostCheck
```

```
Strict SNI virtual host checking
```

```
Non-default virtual host with SSLVerify set to 'require' and VirtualHost-specific CA certificate list is only available to clients with TLS server name indication (SNI) support
```

```
Hostname %s provided via SNI, but no hostname provided in HTTP request
```

```
Hostname %s provided via SNI and hostname %s provided via HTTP are different
```

```
No hostname was provided via SNI for a name based virtual host
```

```
SSL_TLS_SNI
```



Open Source Day **2011**

# Inne

## Sectool:

- Wbudowane narzędzie do testowania systemu pod kątem typowych błędów konfiguracyjnych
- Audytowi konfiguracji poddawane są następujące elementy systemu:

filesystem, firewall, suid, permissions, selinux, exec-shield, vsftpd, openssh, openvpn, removedlibs, shadow, password, group, bootloader, pam, logfiles, cron, routing, integrity,



Open Source Day **2011**





# Pytania?



Dziękuję za uwagę!



Open Source Day **2011**

