Windows

1. Czym się różnią zdarzenia logowania od zdarzeń logowania na kontach?
2. Czy po zalogowaniu resetuje się licznik nieudanych logowań?
3. Czym się różnią grupy „użytkownicy”, „użytkownicy uwierzytelnieni” oraz grupa „Everyone” („Wszyscy”) ?
4. Dany jest SID: S-1-5-21-3568558243-2807218454-1792209693-1001. Jaki jest RID?
5. Czy jest możliwe, by usługa miała taki sam SID na dwóch różnych maszynach?
6. Do czego służy polecenie user2sid? Co robi whoami /groups? Polecenie psexec -s , psexec -l?
7. Co znajduje się w bazie danych SAM (Security Accounts Manager)?
8. Czy hasło „0aA!” spełnia politykę silnych haseł w systemie Windows, bez zaznaczenia innych opcji?
9. Gdzie zobaczyć, kiedy ostatnio logował się JamesBond?
10. Podaj przykład dynamicznych grup w Windows.
11. Co to jest mechanizm impersonacji?
12. Czy proces z niskim poziomem obowiązkowości może czytać dane zapisane w pliku z wysokim poziomem obowiązkowości?
13. Na czym polega polityka „no write up” ?
14. Na czym polega mechanizm wirtualizacji systemu plików w Windowsach (wirtualizacji UAC)?
15. Czy wszystkie gałęzie rejestru podlegają wirtualizacji?
16. Na czym polega mechanizm „split token” i „token elevation”? Czy dotyczy wszystkich użytkowników?
17. Na czym polega mechanizm UAC (User Access control)? Na czym polega mechanizm pytania na „bezpiecznym desktopie”?
18. Co to jest ASLR (advanced space layour randomization) protection?
19. Które z poleceń poniżej służy do zmiany hasła:

net user jbond *	wmic passwd modify jbond	net accounts jbond pass-modify

20. Które z poniższych poziomów integralności wymyśliłem ja, a które naprawdę istnieją? Untrusted, Low, AppContainer, Installer, Medium, High, System.
21. Czy można (domyślnie) uruchamiać procesy poleceniem runas dla użytkowników bez hasła?
22. Na jakim poziomie integralności działają domyślnie konta z grupy administratorów?
23. Gdzie przechowywany jest FEK (file encryption key) szyfrujący plik? Jak zaszyfrowany jest ten plik?
24. Jakie polecenie służy do pokazania, które pliki są zaszyfrowane? Jak sprawdzić, jakim algorytmem?
25. Jak wygenerować certyfikat dla użyt kownika do użytku dla EFS?
26. Do czego służy Agent Odzyskiwania Danych? Jak go utworzyć? (certmgr, efsinfo /r)
27. Jakie warunki musi spełnić użytkownik, by móc obejrzeć zaszyfrowany plik?
28. Czy utworzenie Agenta DRA powoduje, że natychmiast uzyskuje on dostęp do wszystkich wcześniej zaszyfrowanych plików?

29. Jak umożliwić odszyfrowanie pliku innemu użytkownikowi tego samego systemu?
30. Jak wyświetlić alternatywne strumienie danych? Do czego używa ich Internet Explorer? Jak ZoneId wpływa na działanie ściągniętych plików w systemie?
31. Czy zmiana zawartości ADS pliku spowoduje zmianę sumy kontrolnej wyliczonej np. przez md5sum?
32. NTFS ACL: Jakie prawa przydzieli system użytkownikowi Bob, któremu odmówiono prawa zapisu obiektu O, ale należy ten użytkownik do grupy G, która ma prawo do zapisu obiektu O?
33. Jakie prawa otrzyma użytkownik Alice, który nie ma prawa zapisu do obiektu O, ale należy do grupy G, która ma prawo do zapisu obiektu O?
34. Co jeżeli użytkownik Ziutek ma jawnie nadane prawo zapisu do obiekt O, ale należy d grupy G, której jawnie odmówiono tego prawa do obiektu O?
35. Do czego służy przywilej Bypass Traverse Checking (SeChangeNotifyPrivilege)?
36. Czy icacls /grant dodaje (dołącza) uprawnienia, czy nadaje (ustawia tylko takie, jak wymienione)?
37. Czy można w windows utworzyć plik niemożliwy do skasowania przez właściciela katalogu? A katalog?
38. Jakie udziały są udostępniane domyślnie?
39. Jakim poleceniem wyświetlić udziały? Jak stworzyć udział?
40. Jakim poleceniem można ustawiać reguły dla firewalla?
41. Dlaczego wszystkie predefiniowane reguły filtracji ruchu sieciowego w Windows mają domyślną akcję „zezwalaj”?
42. Co robią poniższe polecenia:

```
netsh advfirewall firewall add rule name="All ICMPv4" protocol=icmpv4 dir=in
profile=private action=block
```

```
netsh advfirewall reset
netsh advfirewall firewall add rule name="All ICMP V4" dir=in action=block protocol=icmpv4
netsh advfirewall firewall add rule name="Open SQL Server Port 1433" dir=in action=allow protocol=TCP localport=1433
netsh advfirewall firewall add rule name="Allow Messenger" dir=in action=allow program="C:\programfiles\messenger\msnmsgr.exe"
netsh advfirewall firewall add rule name="netcat" program="C:\windows\tools\netcat.exe" action=allow dir=in protocol=tcp localport=9000
```

43. Czy można zablokować urządzenie loopback w firewallu windows? Dlaczego tak jest?
44. Dlaczego zablokowanie adresu IPv4 dla danej strony (np. facebook.com) może nie zablokować możliwości połączenia się z tą stroną?
45. Jakie polecenie wyświetla informacje o komunikacji sieciowej?
46. Jaką rolę pełni protokół ESP oraz AH?

47. Jakie są różnice między trybem tunelowym a transportowym dla ESP i AH?
48. ICV (integrity control value) dla protokołu AH jest wyliczane dla jakich części pakietu? A dla jakich części dla protokołu ESP? Jak na to wpływa fragmentacja pakietów IP?
49. Dlaczego w trybie transportowym nie da się wykorzystywać protokołu AH z NATem (network adress translation)
50. Jaką rolę pełni „klucz wstępny" w protokole IPSec?
51. Wymień możliwe metody uwierzytelnienia asocjacji SA w systemie Windows
52. Do czego służą numery sekwencyjne w protokole IPSec?
53. Czy IPSec wykorzystuje mechanizm okna (sliding window)?
54. Co to jest Perfect Forward Secrecy w kontekście Ipsec?

LINUX

55. Na jakiej warstwie działa filtracja dostępu przy pomocy TCP wrappera?
56. W jakiej kolejności są przetwarzane reguły TCP wrappera?
57. Jeżeli w pliku hosts.allow mamy regułę
    service : 10.8.0.0/255.255.255.0 EXCEPT 10.8.0.2 : ALLOW
    ALL : ALL : DENY
    ALL : 150.254. 192.168. unixlab.cs.put.poznan.pl
    a w hosts.deny regułę:
    ALL : 10.8.0.4 : DENY

To czy komputer 10.8.0.2 może uzyskać dostęp do usługi service? A komputer z IP 150.254.30.30?

58. Jaka jest różnica między dyrektywami twist a spawn przy użyciu w hosts.allow?
59. Jaki jest efekt zapisu poniżej?
    Hosts.allow: ALL : ALL
    host.deny ALL : ALL
60. Czy coś zmieni, jeżeli dla xinetd wpiszę dyrektywę only_from = 192.168.30.40 ?
61. Dla nadchodzących połączeń, które reguły będą miały pierwszeństwo : firewalla (iptables) czy tcp_wrappera?
62. Czy aplikacja musi mieć wkompilowane wsparcie dla tcp.wrappera, by można nią było zarządzać z poziomu tcpwrappera?
63. Czy można w /etc/hosts.allow zabronić dostępu do danej usługi?
64. Do czego służy opcja PARANOID w plikach konfiguracyjnych tcp_wrappera?
65. Jaki będzie efekt następujących ustawień w plikach konfiguracyjnych tcp_wrappera?

Hosts.allow:	Hosts.deny
daytime : ALL : ALLOW	daytime: 192.168.1.101
daytime: ALL EXCEPT 192.168.1.101 : DENY	
in.rlogind: ALL : spawn /usr/bin/echo „spadaj"	
in.rlogind: ALL : twist /usr/bin/echo „spadaj"	

Daytime : ALL : DENY	Daytime : ALL :ALLOW
	Daytime: ALL: ALLOW
	Daytime: 192.168.1.101
Rlogin : 192.168. EXCEPT 192.168.1.101: DENY ALL : ALL	ALL :ALL

66. Która z poniższych konfiguracji uniemożliwi dostęp tylko do usługi rlogin? (a nie wszystkim usługom)

	Hosts.allow	Hosts.deny
A	Rlogin: ALL : ALLOW	Rlogin: ALL : DENY
B		ALL:ALL
C		Rlogin : ALL
D	ALL EXCEPT rlogin : ALL	ALL: ALL

67. Do czego służy opcja NAMEINARGS(argument dla pola flags w ustawieniach usługi w pliku konfiguracyjnym xinetd)

68. Która z poniższych konfiguracji zapewni domyślną odmowę dostępu, z dopuszczeniem usługi rlogin?

	Hosts.allow	Hosts.deny
A	ALL: ALL	Rlogin : ALL: ALLOW
B	Rlogin : ALL: ALLOW	ALL: ALL
C	ALL EXCEPT rlogin : ALL: ALLOW	
D	<puste>	<puste>

69. Co określa standard x509? Pkcs#7 PKCS#12? PEM? S/MIME?
70. Jak generowany jest podpis cyfrowy?
71. Jak szyfrowana jest wiadomość email?
72. Skąd jest brany klucz potrzebny do weryfikacji podpisu? Do odszyfrowania wiadomości?
73. Czym się różni web of trust PGP od certyfikatów?
74. Na czym polega proces podpisania certyfikatu?
75. Jak unieważnić swoje klucze w systemie PGP?
76. Czym się różnią limity soft od hard w linuksie?
77. Jakie polecenie ustawia limity w linuksie?
78. Dlaczego w parametrach polecenia do ustawienia limitów nie ma ograniczania przestrzeni dyskowej przyznanej jednemu użytkownikowi?
79. Jeżeli proces macierzysty ma ustawione limity, czy są one propagowane na jego procesy potomne (a) przy ich uruchomieniu (b) później, podczas ich pracy?
80. Jakim narzędziem edytuje się politykę sudo?

81. Jakiego hasła domyślnie (o ile się nie skonfiguruje inaczej) domaga się sudo? Jak to zmienić?
82. Co oznacza suid w odniesieniu do pliku wykonywalnego oraz katalogu? Czy są jakieś wyjątki w odniesieniu do plików wykonywalnych (W sensie, z prawem +x ustawionym)?
83. Co oznacza sgid w odniesieniu do pliku wykonywalnego oraz katalogu?

84. Co oznaczają te flagi w odniesieniu do zwykłych, niewykonywalnych plików?
85. Który z programów poniżej wymaga SUID, a który SGID (zakładając, że udostępniamy możliwość ich uruchomienia wybranym lub wszystkim użytkownikom)?

Shadow	write	wall	chmod	passwd
vlock	visudo	ping	find	86.

87. Jakim narzędziem można zlokalizować programy z ustawionym bitem SUID/SGID
88. Czy można pod linuksem utworzyć plik, którego właściciel katalogu nie będzie mógł skasować? Czy będzie można utworzyć katalog, którego właściciel nie będzie mógł skasować?
89. Do czego służy sticky bit w odniesieniu do katalogu?
90. Do czego służy plik core i w jakich okolicznościach można go utworzyć?
91. Jakie narzędzia służą do manipulacji plikami core lub debugowania?
92. Jaki będzie efekt wpisania w pliku sudoers frazy::
    ALL ALL = /sbin/fdisk -l
    student ALL = (root) NOPASSWD: /bin/mount, (ziutek) /bin/echo
    sherlock ALL, !lab-net-14 = (DB) NOPASSWD: SHELLS
    GROUPIES CS = (ALL) ALL

93. Dlaczego nie zaleca się fraz typu „`user ALL = ALL, !polecenie`” ?
94. Co robi flaga NOEXEC w sudoers? Jakim potencjalnym niebezpieczeństwom zapobiega?
95. Jak określany jest algorytm dostępu do plików przy obecności list POSIX ACL?

96. Jakie polecenia są używane do nadawania i wyświetlania POSIX ACL?

97. Czy poleceniem seffacl można ustawić konkretne prawa, czy też są one dodawane/doklejane?
98. Jaką rolę pełni maska uprawnień mechanizmu POSIX ACL?
99. Wobec których użytkowników stosowana jest maska POSIX ACL?
100. W jaki sposób i kiedy wyliczana jest maska POSIX ACL?
101. Czy można wymusić brak wyliczania maski przy poleceniu setfacl?
102. Jaką funkcję pełnią uprawnienia domyślne POSIX ACL?
103. Jakim obiektom można nadawać uprawnienia domyślne POSIX ACL?
104. Załóżmy prawa do katalogu KAT jak poniżej. Nadajemy następujące uprawnienia domyślne:. Jakie są wartości wartości domyślnych katalogu?
    chmod u=rx,g=r,o=w KAT
    setfacl -m u:ziutek:r KAT
    setfacl -m d:u:tester:w KAT

105. Załóżmy, że mamy następujące uprawnienia domyślne dla katalogu Szuflada. Zakładamy katalog Podszufla, a w nim plik Barnaba. Jakie prawa będą dla pliku Barnaba, a jakie dla katalogu Podszufla?
Default:user::r-x
Default:group::rwx
Default:other::r--
Default:user:tester:rwx

106. W jaki sposób można przekopiować uprawnienia z jednej listy ACL do innej (tylko opisać jak, bez polecenia)?

107. Załóżmy wykonanie następujących poleceń jak poniżej. Czy użytkownik ziutek należący do grup users będzie miał prawo do odczytu do pliku? Dlaczego? Plik należy do boryny, do grupy users.

```
setfacl -m u:ziutek:r plik
chmod g=- plik
```

108. Załóżmy, że ls wyświetla prawa do plików jak poniżej. Czy można na tej podstawie odpowiedzieć, jakie są prawa dla grupy do plików, oraz jaka jest maska ACL?

-rwxrw-r-x+ 1 students users 0 Jan 25 PLIK

109. Jakie uprawnienia musi mieć użytkownik, by móc zmienić listy ACL dla obiektów w Linuksie?
110. Czy flaga SGID wpływa na efekty maski ACL, uprawnień domyślnych albo listy ACL?
111. Czy można utworzyć plik w katalogu obcego użytkownika, którego obcy użytkownik nie będzie mógł: odczytać, zmodyfikować, skasować? Jak to się zmienia dla katalogów?

112. Gdzie znajdują się klucze publiczne zdalnych systemów, pozyskane podczas logowania przez SSH na te systemy?

113. Co powoduje polecenie ssh -l ziutek obcy.system.pl cat /home/ziutek/plik?
114. Jakie metody uwierzytelnienia dopuszcza protokół ssh?
115. Jak generować pary kluczy do użycia przez protokół ssh?
116. Co należy uczynić, by móc zalogować się na zdalny system bez hasła?
117. Załóżmy, że ustawiliśmy tunelowanie ssh typu DynamicForward na komputerze A, a w firefoksie na komputerze B ustawiliśmy odpowiednio opcje dla proxy aplikacyjnego (SOCKS Proxy). Czyje IP będą widzieć obce strony odwiedzane przez przeglądarkę, komputera A czy też B?
118. Na komputerze GAT wydano polecenie ssh jak w tabelce poniżej. Następnie na komputerze BOB wykonano polecenie jak w tabelce. Na komputerze ALICE działa netcat -l 1024. Między którymi komputerami połączenie jest szyfrowane? Z kim połączy się BOB?

GAT:	BOB

ssh -L 9090:ALICE:1024 SER	netcat GAT 9090
ssh -R 9090:ALICE:1024 SER	Netcat SER 9090

119. Czy można utworzyć tunel VPN przy pomocy ssh?
120. Jakim kluczem szyfrowane jest połączenie ssh? Jak ssh zapewnia integralność komunikatów?
121. Jakimi metodami można uwierzytelniać strony komunikacji przy użyciu openVPN?
122. Na jakim protokole opiera się narzędzie openVPN?
123. Jakim kluczem jest szyfrowane połączenie w tunelu openVPN? (symetrycznym/asymetrycznym)?
124. Jaka jest różnica między urządzeniami tun i tap?
125. Czy przy użyciu współdzielonego wstępnie klucza do serwera może podłączyć się wielu klientów?