1. Który z poniższych etapów łańcucha cyberzabójstw nie odpowiada etapowi Ataku i Wyzysku w procesie testów penetracyjnych?

A. Uzbrojenie

B. Rekonesans

C. Instalacja

D. Działania na rzecz celów

2. Niedawno Robert przeprowadził atak phishingowy na cel testów penetracyjnych, próbując zebrać dane uwierzytelniające, które mógłby wykorzystać w późniejszych atakach. Na jakim etapie procesu testów penetracyjnych znajduje się Robert?

A. Planowanie i ustalanie zakresu

B. Atakowanie i wykorzystywanie

C. Zbieranie informacji i identyfikacja podatności

D. Wyniki raportowania i komunikacji

3. Które z poniższych narzędzi oceny bezpieczeństwa nie jest powszechnie używane podczas fazy zbierania informacji i identyfikacji luk w testach penetracyjnych?

A. Nmap

B. Nessusa

C. Metasploit

D. Nslookup

4. Na jakim etapie łańcucha cyberzabójstw osoba atakująca kradnie informacje, korzysta z zasobów komputerowych lub zmienia informacje bez pozwolenia?

A. Uzbrojenie

B. Instalacja

C. Działania na rzecz celów

D. Dowodzenie i kontrola

5. Robert prowadzi śledztwo w sprawie incydentu związanego z bezpieczeństwem, w którym napastnicy zostawili dyski USB zawierające zainfekowane pliki na parkingu budynku biurowego. Na jakim etapie łańcucha cyberzabójstw opisano to działanie?

A. Uzbrojenie

B. Instalacja

C. Dostawa

D. Dowodzenie i kontrola

6. Które z poniższych nie jest narzędziem do gromadzenia danych wywiadowczych typu open source?

A. WHOIS

B. Nslookup

C. Nessusa

D. FOCA

7. Które z poniższych narzędzi jest platformą eksploatacji powszechnie używaną przez testerów penetracyjnych?

A. Metasplot

B. Wireshark

C. Aircrack-ng

D. SET

8. Co zazwyczaj obejmuje MSA?

A. Warunki, które będą regulować przyszłe umowy

B. Wzajemne wsparcie podczas ocen

C. Architektura mikrousług

D. Dopuszczalny minimalny poziom usług level

9. Podczas wykonywania testu penetracyjnego na miejscu Robert podłącza swój laptop do dostępnego gniazda sieciowego. Jednak gdy próbuje się połączyć, nie otrzymuje adresu IP i nie ma połączenia z siecią. Wie, że port działał wcześniej. Jaką technologię najprawdopodobniej zastosował jego cel?

A. Jack whitelisting

B. Jack blacklisting

C. NAC

D. 802.15

10. Jaki rodzaj testu penetracyjnego nie ma na celu zidentyfikowania jak największej liczby podatności, a zamiast tego koncentruje się na podatnościach, które konkretnie odpowiadają celom uzyskania kontroli nad konkretnymi systemami lub danymi?

A. Ocena oparta na celach

B. Ocena oparta na zgodności

C. Ocena czarnej drużyny

D. Ocena zespołu czerwonego

11. Podczas testu penetracyjnego na miejscu, jaki element określania zakresu ma kluczowe znaczenie dla oceny sieci bezprzewodowych podczas pracy w budynkach współdzielonych?

A. Typ szyfrowania

B. Częstotliwość bezprzewodowa

C. Identyfikatory SSID

D. Wstępnie współdzielone klucze

12. Jaki typ przeciwnika najprawdopodobniej użyje do swoich ataków tylko gotowych narzędzi?

A. APT

B. Script kiddies

C. Haktywiści

D. Przestępczość zorganizowana

13. Podczas testu penetracyjnego, którego zakres obejmuje pojedynczą aplikację internetową, Robert odkrywa, że serwer sieciowy zawiera również listę haseł do innych serwerów w lokalizacji docelowej. Po powiadomieniu klienta proszą go o użycie ich do weryfikacji tych serwerów, a on przystępuje do testowania tych haseł na innych serwerach. Co się stało?

A. Nadużycia

B. Obracanie

C. Pełzanie zakresu

D. Ekspansja docelowa

14. Robert został zatrudniony do przeprowadzenia testu penetracyjnego organizacji obsługującej karty kredytowe. Jego praca będzie przebiegać zgodnie z zaleceniami PCI DSS. Jaki rodzaj oceny przeprowadza Lucas?

A. Ocena oparta na celach

B. Ocena zespołu czerwonego

C. Ocena czarnej drużyny

D. Ocena oparta na zgodności

15. Jaki jest pełny zakres portów, na których może działać usługa UDP?

A. 1–1024

B. 1–16 383

C. 1-32 767

D. 1–65 535

16. Robert pracuje z nieuprzywilejowanego konta użytkownika, które zostało uzyskane w ramach testu penetracyjnego. Odkrył, że host, na którym się znajduje, ma zainstalowany Nmap i chce przeskanować inne hosty w swojej podsieci, aby zidentyfikować potencjalne cele w ramach próby obrotu. Jakiej flagi Nmap będzie musiał użyć, aby pomyślnie przeskanować hosty z tego konta?

A. -sV

B. -u

C. -oA

D. -sT

17. Które z poniższych narzędzi dostarcza informacji o rejestratorze domeny i fizycznej lokalizacji?

A. Nslookup

B. Host

C. KTOIS

D. Traceroute

18. Robert przeprowadza skanowanie Nmapem sieci 10.10.0.0/16, której jego pracodawca używa jako zakresu sieci wewnętrznej dla całej organizacji. Jeśli użyje flagi - T0, jaki problem może napotkać?

A. Skanowanie zakończy się, gdy liczba hostów osiągnie 0.

B. Skanowanie nie będzie skanować adresów IP w sieci .0.

C. Skanowanie będzie przebiegać bardzo wolno.

D. Skanowanie będzie skanować tylko w poszukiwaniu usług TCP.

19. Który z poniższych formatów wyjściowych Nmapa prawdopodobnie nie będzie przydatny dla testera penetracyjnego?

A. -oA

B. -oS

C. -oG

D. -oX

20. We wczesnej fazie testu penetracyjnego Robert odzyskuje binarny plik wykonywalny, który chce szybko przeanalizować pod kątem przydatnych informacji. Które z poniższych narzędzi szybko da mu wgląd w potencjalnie przydatne informacje w pliku binarnym?

A. NETCAT

B. strings

C. Hashmod

D. Eclipse

21. Robert konfiguruje swoje rozwiązanie do zarządzania lukami w zabezpieczeniach, aby wykonywać uwierzytelnione skany serwerów w swojej sieci. Jakie konto powinien dostarczyć do skanera?

A. Administrator domeny

B. Administrator lokalny

C. Root

D. Tylko do odczytu

22. Robert pisze raport na temat potencjalnej luki w zabezpieczeniach oprogramowania i chce użyć ustandaryzowanych nazw produktów, aby zapewnić, że inni analitycy bezpieczeństwa zrozumieją raport. Do którego komponentu SCAP może zwrócić się Robert o pomoc?

A. CVSS

B. CVE

C. CPE

D. OVAL

23. Robert planuje przeprowadzić skanowanie podatności organizacji w ramach testu penetracyjnego. Przeprowadza test czarnej skrzynki. Kiedy należałoby przeprowadzić wewnętrzne skanowanie sieci?

A. Na etapie planowania testu

B. Natychmiast po podpisaniu umowy

C. Po uzyskaniu zgody administratora

D. Po skompromitowaniu hosta wewnętrznego

24. Który typ organizacji najprawdopodobniej stanie przed wymogiem regulacyjnym przeprowadzenia skanowania podatności?

B. Bank

B. Szpital

C. Agencja rządowa

D. Gabinet lekarski

25. Która z poniższych kategorii systemów najprawdopodobniej zostanie zakłócona podczas skanowania luk w zabezpieczeniach?

A. Zewnętrzny serwer WWW

B. Wewnętrzny serwer WWW

C. Urządzenie IoT

D. Zapora sieciowa

26. Jaki termin opisuje gotowość organizacji do tolerowania ryzyka w swoim środowisku komputerowym?

A. Krajobraz ryzyka

B. Apetyt na ryzyko

C. Poziom ryzyka

D. Adaptacja do ryzyka

27. Który z poniższych czynników ma najmniejszy wpływ na harmonogramy skanowania podatności?

A. Wymagania prawne

B. Ograniczenia techniczne

C. Ograniczenia biznesowe

D. Dostępność personelu

28. Robert niedawno przeanalizował wyniki raportu skanowania luk w zabezpieczeniach i stwierdził, że luka zgłoszona przez skaner nie istnieje, ponieważ system został załatany zgodnie z opisem. Jaki rodzaj błędu wystąpił?

A. Fałszywie pozytywne

B. Fałszywie negatywne

C. Prawdziwie pozytywne

D. Prawdziwie negatywne

29. Które z poniższych nie jest powszechnym źródłem informacji, które mogą być skorelowane z wynikami skanowania narażenia na atak?

A. Dzienniki

B. Tabele bazy danych

C. SIEM

D. System zarządzania konfiguracją

30. Którego z poniższych systemów operacyjnych należy unikać w sieciach produkcyjnych?

A. Windows Server 2003

B. Red Hat Enterprise Linux 7

C. CentOS 7

D. Ubuntu 16

31. W jakim typie ataku atakujący umieszcza więcej informacji w lokalizacji pamięci, niż jest przydzielone do tego celu?

A. Wstrzyknięcie SQL

B. Wstrzyknięcie LDAP

C. Skrypty między witrynami

D. Przepełnienie bufora

32. Atak Dirty COW jest przykładem jakiego rodzaju podatności?

A. Złośliwy kod

B. Eskalacja uprawnień

C. Przepełnienie bufora

D. Wstrzyknięcie LDAP

33. Którego z poniższych protokołów nigdy nie należy używać w sieci publicznej?

A. SSH

B. HTTPS

C. SFTP

D. Telnet

34. Kilka dni po wykorzystaniu celu z ładunkiem Metasploit Meterpreter Robert traci dostęp do zdalnego hosta. Skan podatności pokazuje, że luka, której użył do wykorzystania systemu, jest nadal otwarta. Co się najprawdopodobniej wydarzyło?

A. Skanowanie złośliwego oprogramowania wykryło Meterpretera i usunęło go.

B. System został załatany.

C. System został ponownie uruchomiony.

D. Meterpreter uległ awarii.

35. Robert chce uruchomić John the Ripper przeciwko zaszyfrowanemu plikowi haseł, który uzyskał w wyniku kompromitacji. Jakie informacje musi znać, aby skutecznie złamać plik?

A. Przykładowa lista słów

B. Użyty skrót

C. Liczba haseł

D. Żadne z powyższych

36. Robert cross kompiluje kod swojego exploita, a następnie go wdraża. Dlaczego miałby skompilować kod?

A. Aby działał na wielu platformach

B. Aby dodać dodatkowe biblioteki

C. Aby uruchomić go na innej architekturze

D. Aby umożliwić mu sprawdzenie kodu źródłowego

37. Robert zdobył listę ważnych kont użytkowników, ale nie ma do nich haseł. Jeśli nie znalazł żadnych luk w zabezpieczeniach, ale uważa, że organizacja, na którą jest celem, stosuje słabe praktyki dotyczące haseł, jakiego rodzaju ataku może użyć, aby spróbować uzyskać dostęp do systemu docelowego, w którym te nazwy użytkownika są prawdopodobnie prawidłowe?

A. Rainbow tables

B. Dictionary attacks

C. Thesaurus attacks

D. Meterpreter

38. Jakie wbudowane narzędzie administracyjne serwera Windows może zezwolić na dostęp PowerShell z wiersza poleceń z innych systemów?

A. VNC

B. PowerSSHell

C. PSRemote

D. PROW

39. Robert chce zachować dostęp do systemu Linux. Która z poniższych nie jest powszechną metodą utrzymywania trwałości na serwerach z systemem Linux?

A. Zaplanowane zadania

B. Praca Crona

C. Usługi trojanów

D. Zmodyfikowane demony

40. Robert wybrał swój exploit Metasploit i ustawił swój ładunek jako cmd/unix/generic. Po próbie wykorzystania exploita otrzymuje następujące dane wyjściowe. Co poszło nie tak?

```
msf exploit(unix/misc/distcc_exec) > exploit

[-] Exploit failed: The following options failed to validate: RHOST.
[*] Exploit completed, but no session was created.
```

A. Zdalny host jest chroniony zaporą sieciową.

B. Zdalny host nie jest w trybie online.

C. Host nie jest routowalny.

D. Host zdalny nie został ustawiony.

41. Jaki rodzaj ataku bezprzewodowego skupia się na nakłanianiu klientów do korzystania z mniej bezpiecznych protokołów?

A. downfall attack

B. false negotiation attack

C. chutes and ladders attack

D. downgrade attack

42. Robert chce użyć THC Hydra do brutalnego wymuszania haseł SSH. Przygotowując się do uruchomienia polecenia, wie, że przypomina sobie flagę -t. Co powinien wziąć pod uwagę, używając tej flagi?

A. Ile celów chce zaatakować

B. Liczba zadań uruchamianych równolegle na cel

C. Limit czasu połączeń

D. Żadne z powyższych

43. Robert ustawił swoją stację roboczą do testów penetracyjnych jako człowiek pośrodku między swoim celem a serwerem FTP. Jaka jest dla niego najlepsza metoda uzyskania danych uwierzytelniających FTP?

A. Przechwytywanie ruchu za pomocą Wireshark

B. Przeprowadź atak brute-force na serwer FTP

C. Użyj exploita przeciwko serwerowi FTP

D. Użyj ataku downgrade przy następnym logowaniu

44. Robert chce wyliczyć możliwe konta użytkowników i odkrył dostępny serwer SMTP. Jakie polecenia STMP są do tego najbardziej przydatne?

A. HELO i DSN

B. EXPN i VRFY

C. VRFY i TURN

D. EXPN i ETRN

45. Jaki jest domyślny ciąg społeczności tylko do odczytu dla wielu urządzeń SNMP?

A. secret

B. readonly

C. private

D. public

46. Które z poniższych narzędzi nie pozwoli Robertowi uchwycić? Skróty NTLM v2 przez sieć do użycia w ataku typu pass-the-hash?

A. Respoder

B. Mimikatz

C. Ettercap

D. Metasplot

47. Do jakiego rodzaju działalności użyłbyś narzędzi HULK, LOIC, HOIC i SlowLoris?

A. DDoS

B. Przechwytywanie hash SMB

C. DoS

D. Brute-force SSH

48. Robert wysyła wiadomość phishingową specjalnie do Roberto, dyrektora generalnego swojej firmy docelowej. Jaki rodzaj ataku phishingowego przeprowadza?

A. nękanie CEO

B. Spear phishing

C. Podbijanie phishingu

D. Ustawienie haka

49. Podczas wykonywania fizycznego testu penetracyjnego Robert zauważa, że drzwi wyjściowe do centrum danych otwierają się automatycznie, gdy pracownik zbliża się do nich z wózkiem. Co powinien zapisać w swoich notatkach?

A. Obecność czujnika wyjścia

B. Obecność mantrapy

C. Potencjalne odblokowane drzwi

D. Nic, ponieważ to nie jest luka

50. Robert chce zebrać informacje o organizacji, ale nie chce wchodzić do budynku. Jakiej fizycznej techniki gromadzenia danych może użyć, aby potencjalnie zebrać dokumenty biznesowe bez wchodzenia do budynku?

A. Piggybacking

B. Surfowanie po plikach

C. Krople USB

D. Nurkowanie w śmietniku

51. Robert przygotowuje się do podróży do innego stanu w celu wykonania fizycznego testu penetracyjnego. Jaki sprzęt do testów penetracyjnych powinien sprawdzić pod kątem legalności przed wyjazdem do tego stanu?

A. Metasplot

B. Wytrychy

C. Narzędzia szyfrujące

D. SET

52. Która technika motywacji socjotechnicznej polega na przekonywaniu celu, że inni ludzie zachowywali się podobnie, a zatem, że oni też mogą?

A. Podobieństwo

B. Strach

C. Dowód społeczny

D. Wzajemność

53. Jaki jest domyślny ciąg społeczności tylko do odczytu dla wielu urządzeń SNMP?

A. secret

B. readonly

C. private

D. public

54. Robert chce uzyskać dostęp do siedziby firmy docelowej, ale odkrywa, że jego pierwotny pomysł na przeskoczenie ogrodzenia prawdopodobnie nie jest praktyczny. Który czynnik najmniej przeszkodzi mu w próbie przeskoczenia płotu?

A. Drut kolczasty

B. Brama

C. Wysokość ogrodzenia

D. Ochroniarze

55. Robert obawia się, że aplikacja internetowa w jego organizacji obsługuje niesprawdzone przekierowania. Które z poniższych podejść zminimalizuje ryzyko tego ataku?

A. Wymaganie HTTPS

B. Szyfrowanie sesyjnych plików cookie

C. Implementacja uwierzytelniania wieloskładnikowego

D. Ograniczanie przekierowań do swojej domeny

56. Robert sprawdza swoje logi serwera WWW i widzi, że ktoś wysłał następujący ciąg zapytania do aplikacji działającej na serwerze:

http://www.mycompany.com/servicestatus.php?serviceID=892&serviceID=892' ; UPUŚĆ TABELĘ

Usługi;--

Jaki rodzaj ataku został najprawdopodobniej podjęty?

A. Skrypty między witrynami

B. Przejmowanie sesji

C. Zanieczyszczenie parametru

D. Man-in-the-middle

57. Po dalszej inspekcji Joe znajduje serię tysięcy żądań do tego samego adresu URL pochodzących z jednego adresu IP. Oto kilka przykładów:

http://www.mycompany.com/servicestatus.php?serviceID=1

http://www.mycompany.com/servicestatus.php?serviceID=2

http://www.mycompany.com/servicestatus.php?serviceID=3

http://www.mycompany.com/servicestatus.php?serviceID=4

http://www.mycompany.com/servicestatus.php?serviceID=5

http://www.mycompany.com/servicestatus.php?serviceID=6

Jaki typ luki prawdopodobnie próbował wykorzystać atakujący?

A. Niepewne bezpośrednie odniesienie do obiektu

B. Przesyłanie plików

C. Niezweryfikowane przekierowanie

D. Przejęcie sesji

58. Przygody Roberta w analizie logów serwera WWW nie są jeszcze zakończone. Kontynuując przeglądanie dzienników, znajduje żądanie http://www.mycompany.com/../../../etc/passwd

Jaki rodzaj ataku został najprawdopodobniej podjęty?

A. Wstrzyknięcie SQL

B. Przejmowanie sesji

C. Przeglądanie katalogów

D. Przesyłanie plików

59. Jaki rodzaj ataku zależy od tego, że użytkownicy często logują się do wielu witryn jednocześnie w tej samej przeglądarce?

A. Wstrzyknięcie SQL

B. Skrypty między witrynami

C. Fałszerstwo żądań między witrynami

D. Włączenie pliku

60. Jaki rodzaj ataku cross-site scripting nie byłby widoczny dla specjalisty ds. bezpieczeństwa sprawdzającego kod źródłowy HTML w przeglądarce?

A. Odbity XSS

B. Przechowywane XSS

C. Trwałe XSS

D. XSS oparty na DOM

61. Gdzie są przechowywane klucze LSA Secrets w systemie Windows?

A. Folder $System

B. Rejestr

C. Folder System32

D. Są przechowywane tylko na kontrolerze Active Directory.

62. Jaka technika jest wymagana do korzystania z usługi LSASS w celu złamania poświadczeń w nowoczesnym systemie Windows?

A. Ustaw magazyn na „nieszyfrowany”.

B. Włącz obsługę starszej wersji LSASS.

C. Włącz WDigest.

D. Wyłącz LSASS 2.0.

Użyj poniższego scenariusza do pytań 63-65. Robert otrzymał zadanie kontynuowania procesu eksploatacji serwera Windows 2012, dla którego inny tester penetracyjny uzyskał poświadczenia na poziomie użytkownika. Wie, że serwer jest w pełni załatany i nie ma ujawnionych podatnych na ataki usług. Jego celem jest uzyskanie dostępu administracyjnego do serwera.

63. Robert chce przeprowadzić atak wykorzystujący nienotowane ścieżki usług. Który z poniższych użytkowników jest najbardziej pożądany do wyświetlenia w sekcji „Zaloguj się jako” w panelu sterowania Usługi?

A. Konto usługi serwisu

B. system

C. root

D. poweruser

64. Robert chce spróbować ataku typu kerberoasting. Jaki powinien być jego pierwszy krok do wykonania tego ataku?

A. Zidentyfikuj adres IP serwera Kerberos domeny.

B. Pobierz wartości SPN.

C. Przechwytuj skróty NTLM z przewodu.

D. Wyodrębnij bilety serwisowe z pamięci.

65. Robert przechwycił hasze NTLM i chce przeprowadzić atak typu pass-the-hash. Niestety nie wie, które systemy w sieci mogą akceptować hash. Jakiego narzędzia mógł użyć, aby pomóc mu przeprowadzić ten test?

A. Hashcat

B. smbklient

C. Hydra

D. Żadne z powyższych

66. Robert wdrożył fizyczne keyloggery do systemów docelowych. Jaki problem najczęściej kojarzy się z fizycznymi keyloggerami?

A. Awaria sprzętu

B. Odkrycie

C. Wykrywanie oparte na oprogramowaniu

D. Wyczerpanie magazynu

67. Dlaczego dostęp JTAG jest szczególnie przydatny dla testerów penetracyjnych, którzy mają fizyczny dostęp do systemów?

A. Zapewnia nieuwierzytelniony dostęp zdalny.

B. JTAG oferuje dostęp debugowania bezpośrednio do pamięci.

C. JTAG jest automatycznie logowany jako root.

D. JTAG zapewnia szczegółowe logowanie systemu.

68. Jaki operator porównania testuje równość w Rubim?

A. –eq

B.-ne

C. ==

D. !=

69. Jaka wartość zostałaby użyta do zakodowania spacji w ciągu URL?

A. %20

B. %21

C. %22

D. %23

70. Sprawdź poniższy fragment kodu. W jakim języku jest napisany ten kod?

begin

system 'nmap ' + ip

rescue

puts 'An error occurred.'

end

A. Pythona

B. PowerShell

C. Rubin

D. Bash

71. Które z poniższych par języków pozwalają na bezpośrednie połączenie łańcucha i liczby całkowitej?

A. Python i Bash

B. Bash i PowerShell

C. Python i Ruby

D. Ruby i PowerShell

72. Jaki jest limit liczby klauzul elsif w skrypcie Ruby?

A. 1

B. 2

C. 10

D. Bez limitu

73. Rozważmy następujący kod Pythona:

jeśli 1 == 1:

print("cześć")

```
elif 3 == 3:
print("cześć")
jeszcze:
print("cześć")
```

Ile razy ten kod wydrukuje słowo „cześć”?

A. 0

B. 1

C. 2

D. 3

74. Organizacja Roberta używa obecnie uwierzytelniania opartego na hasłach i chciałaby przejść na uwierzytelnianie wieloskładnikowe. Który z poniższych jest akceptowalnym drugim czynnikiem?

A. Pytanie zabezpieczające

B. PIN

C. Aplikacja na smartfona

D. Hasło

75. Który z poniższych elementów nie nadaje się do podsumowania raportu z testów penetracyjnych?

A. Opis ustaleń

B. Oświadczenie o ryzyku

C. Zwykły język

D. Szczegóły techniczne

76. Która z poniższych czynności nie jest często wykonywana podczas fazy porządkowania po zaangażowaniu?

A. Naprawa podatności

B. Usuwanie muszli

C. Usunięcie danych uwierzytelniających utworzonych przez testera

D. Usuwanie narzędzi

77. Kto najskuteczniej ułatwia przeprowadzenie sesji wyciągniętych wniosków po teście penetracyjnym?

A. Lider zespołu

B. CIO

C. Strona trzecia

D. Klient

78. Podczas procesu modelowania zagrożeń organizacja stwierdza, że najbardziej martwi ją uporczywa grupa podmiotów o wyrafinowanych zdolnościach. Jakim typem cyberprzestępcy jest najbardziej zainteresowana ta organizacja?

A.Pentester

B. Haktywista

C. Zagrożenie wewnętrzne

D. APT

79. Użyj poniższego scenariusza, aby odpowiedzieć na dwa następne pytania. Grupa bezpieczeństwa określa ilościowo ryzyko związane z określonym zagrożeniem w organizacji. Prawdopodobieństwo zagrożenia wynosi 6, a potencjalna szkoda 5. Stosując odpowiednią formułę do oceny ryzyka zagrożenia, jaki jest poziom ryzyka dla tego typu zagrożenia?

A. 11

B. 33

C. 30

D. 45

80. Ryzyko to będzie prawdopodobnie traktowane priorytetowo jako priorytet _____.

Średni

B. Niski

C. Wysoki

D. Pilne