SocioBrains
ISSN 2367-5721, JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
INTERNATIONAL SCIENTIFIC REFEREED ONLINE JOURNAL WITH IMPACT FACTOR
ISSUE 42, FEBRUARY 2018

IMPLEMENTATION OF NETWORK ENUMERATION CYBER-ATTACKS AND DEFENSE THE COMPUTER RESOURCES OF THE LOCAL AND WIDE AREA NETWORKS

Abstract: In this paper a summarized implementation of network enumeration cyber-attack and defense the computer resources of the local and wide area networks is made. Most of the network system administrators, security professionals, network architects and IT specialists must create security defense mechanisms against all types of network enumeration cyber-attacks in the computer networks of government agencies and private organizations.

Keywords: Cyber-attacks, Computer and network administrators, Computer resources, Enumeration, Defense, LAN, Protocols, Security, Vulnerability, WAN.

Authors information:

Petar Boyanov
Chief Assistant Professor, PhD,
Lecturer in Department
"Communication and Computer Technologies"
at Konstantin Preslavsky University of Shumen
✉ peshoaikido@abv.bg
Bulgaria

Hristo Hristov
Associate Professor, PhD,
Lecturer in Department
"Management of Security Systems"
at Konstantin Preslavsky University of Shumen
✉ hristov63@abv.bg
Bulgaria

1. Въведение

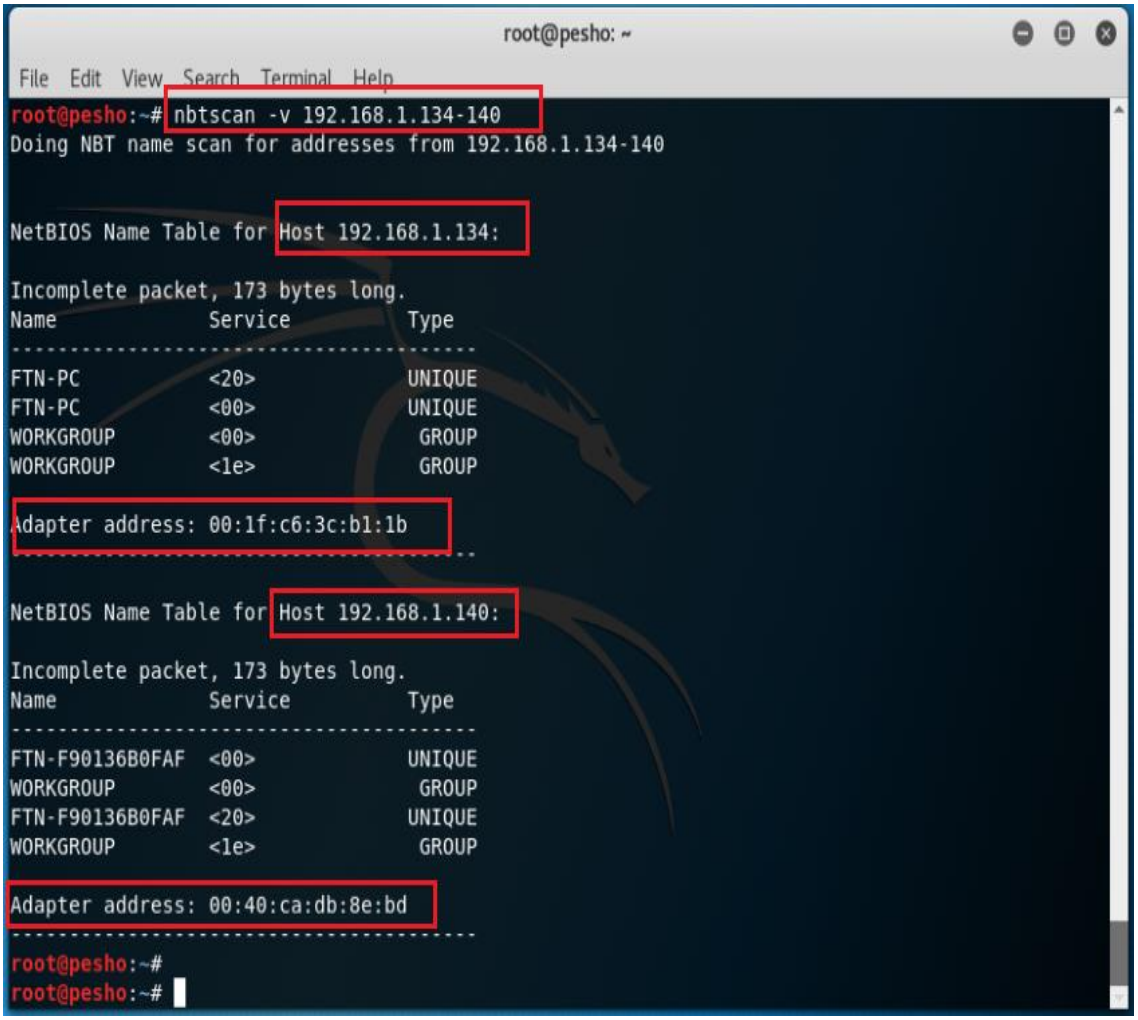
Кибератаките чрез изброяване на системните ресурси на дадена организация намират приложение при разкриването на информация за нулевата сесия (Null Session), именната NetBIOS таблица, типът на работната станция, потребители, групи, политики на акаунтите, споделени папки, домейни, отдалечено време, системни твърди дялове, услуги, процеси, регистри и сесии на логване само в локалните компютърни мрежи [20]. Атаките чрез изброяване включват следните подтипове [1], [2], [3]. [4], [6], [8], [10], [11], [12], [13]:

- Кибератаки към протокола LDAP (Lightweight Directory Access Protocol);
- Кибератаки към таблицата NetBIOS (Network Basic Input/Output System);
- Кибератаки към електронната поща SMTP (Simple Mail Transfer Protocol);
- Кибератаки към протокола SNMP (Simple Network Management Protocol);
- Кибератаки към протокола NTP (Network Time Protocol);
- Кибератаки към услугата DNS (Domain Name System). [3], [4], [5], [6], [9], [11], [13], [16].

2. Изложение

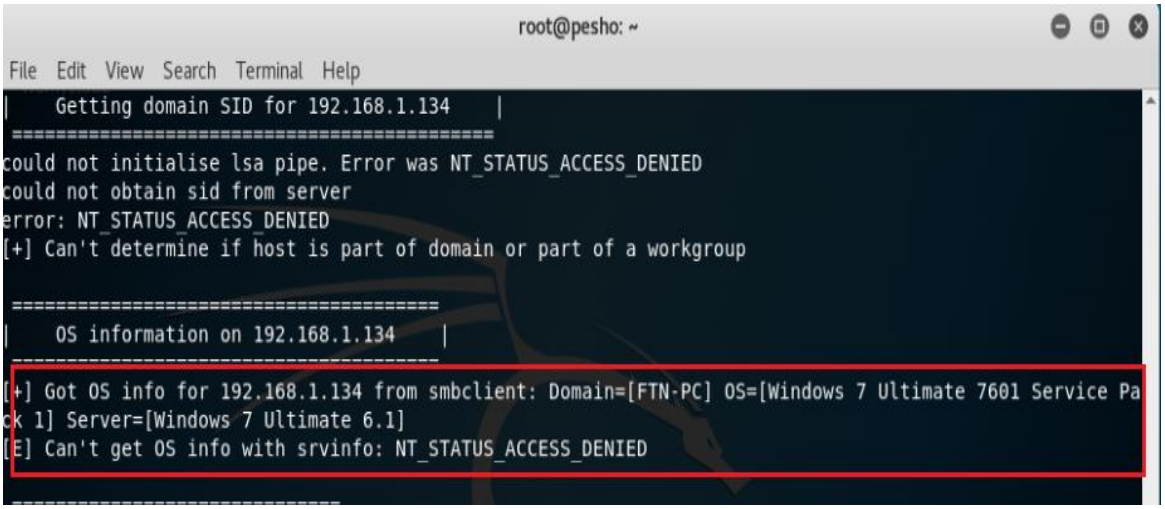
Кибератаката към таблицата NetBIOS (Network Basic Input/Output System)

Тази кибератака помага на киберпрестъпника да получи информация за физическия MAC адрес и компютърното име на машината жертва на служителя от държавното учреждение или частната организация от мрежовата таблица с имена - NetBIOS чрез използването на командата "nbtscan" за Linux базирана операционна система. На фиг. 1 са сканирани два хоста с IPv4 адреси - 192.168.1.134 и 192.168.1.140 и след изпълнение на командата са показани и получените резултати [18], [19].



Фиг. 1. Получени резултати след изпълнение на командата "nbtscan -v 192.168.1.134-140"

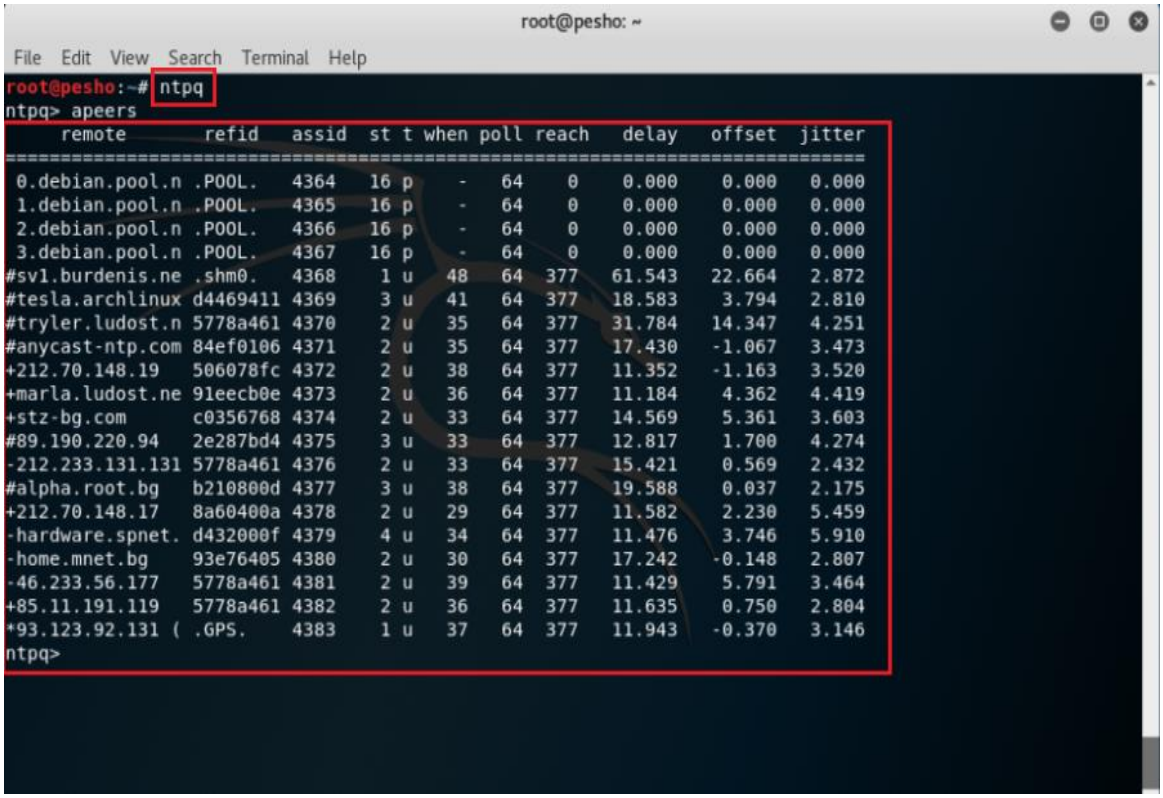
Другата команда, която може да се използва за получаване на информация за версията на операционната система за избрана машина жертва на служител от дадена организация е "enum4linux". Това е илюстрирано на фиг. 2.



Фиг. 2. Получени резултати след изпълнение на командата за хост с IP адрес - 192.168.1.134 "enum4linux -U -M -S -P -G -d -o -i -r 192.168.1.134"

Кибератаката към протокола NTP (Network Time Protocol)

Тази кибератака се използва с цел откриване на всички сървъри за синхронизиране на времето и датата на всички компютри в света с използването на специални команди като "ntpq", "ntpdc" и "ntptrace". На фиг. 3 са показани всички намерени сървъри за синхронизация за мрежовото време с командата "ntpq" [10], [11], [12], [16], [17], [19], [20], [21].

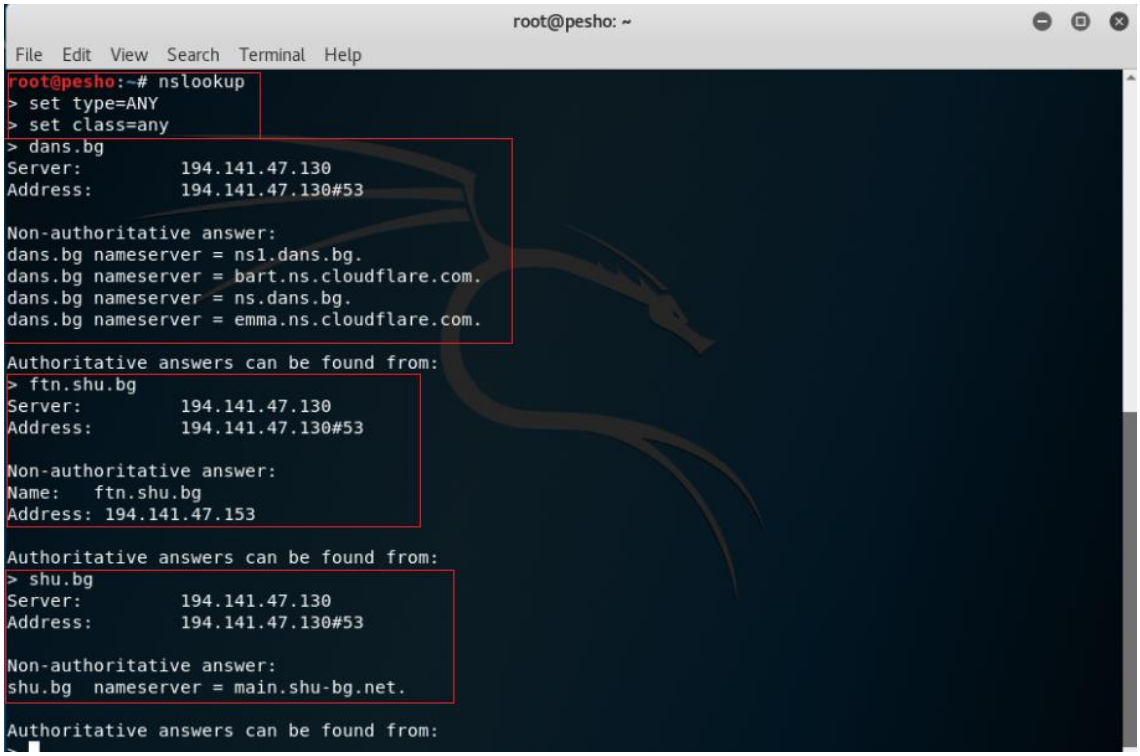


Фиг. 3. Получени резултати след изпълнение на командата "ntpq"

Кибератаки към услугата DNS (Domain Name System)

Приложението Nslookup представлява софтуерна програма, която изпраща интерактивно заявки към сървърите на имената на домейните. Чрез този процес на изпращане на заявки киберпрестъпникът ще получи важна информация относно имената на DNS сървърите, имената на хостовете, потребителски имена, IP адреси на хостовете и др [11], [13], [15].

В операционната система Kali Linux е използвана командата “nslookup” с допълнителни конфигурирани настройки за показване на всички типове и класове на имената на DNS сървърите. Уеб сървърите, към които са отправени заявки, са: "dans.bg", "ftn.shu.bg" и "shu.bg". Това е показано на фиг. 4.



Фиг. 4. Получени резултати след изпълнение на командата "nslookup" в Linux базирана операционна система

Софтуерните средства, които се използват за осъществяване на кибератаки от изброяване, са [1], [2], [3], [4], [7], [8]:

- Hyena за NetBIOS изброяване.
- NetBIOS Enumerator за NetBIOS изброяване.
- Winfingerprint за NetBIOS изброяване.
- LDAP Account Manager за протокола LDAP.
- LDAP Administration Tool.
- Active Directory Domain Services Management Pack.
- LEX - The LDAP Explorer.
- LDAP Administration Tool.
- JXplorer.
- LDAP Browser Editor.
- LDAP Search и др.

ЗАБЕЛЕЖКА: Всичките експерименти и изследвания в тази статия са направени в специализирана компютърна лаборатория във Факултета по технически науки при Шуменския университет „Епископ Константин Преславски“, състояща се от няколко хоста и в домашна частна локална компютърна мрежа, състояща се от четири хоста. Всичко илюстрирано и обяснено в тази статия е с научно-изследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.

Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.” // Наказателен кодекс - Чл. 319а. (Нов - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.).

3. Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва да предприемат и направят следните защитни действия като [4], [5], [6], [9], [10], [11], [12], [14], [18], [20]:

• Прилагане на по-стриктни специални настройки на пощенския сървър за пренасяне електронни писма - SMTP като блокиране или отхвърляне на електронни съобщения към непознати получатели.

• Да не допуска да има съдържание относно информация локалната компютърна машина на служителя в отговорите на неговите електронни писма.

• Да се използват специални политики на сигурност чрез базова автентификация до точно определен кръг от потребители.

• Да се използва протокола SSL с цел пренасяният мрежов трафик да бъде криптиран.

• Задължително правило на служителите е компютърното име на машината да бъде напълно различно с тяхната електронна поща.

• Задължително условие на всеки служител е да излиза локално от компютърния си акаунт. Това се прави с цел, ако служителят отиде да обядва и го няма на работното му място, но в същото време си е оставил компютърът да работи, да няма друг достъп до неговите ресурси.

References:

1. Vasileva R, „Analiz na sastoyanieto na zashtita pri bedstvia v Bulgaria“, NS s mezhdunarodno uchastie "Kursantite i studentite na morskoto uchilishte i naukata", VVMU “N. Y. Vaptsarov", Varna, 26-27 mart 2015 g.
2. Dosev N. Y., Sazdavane na sklad ot danni za opredelyane na riska za informatsionnata sigurnost na korporatsiyata", Nauchna konferentsia s mezhdunarodno uchastie na tema „Kibersigurnostta v informatsionnoto obshtestvo”, Fakultet "A, PVO i KIS", Shumen 2017 g.
3. Dosev N. Y., Nepravitelstveniyat sektor i natsionalnata sigurnost“, Treta mezhdunarodna nauchna konferentsia –„Nauka, obrazovanie, inovatsii“, posvetena na 145 godishninata na BAN i 35 godishninata ot kosmicheskia polet na Georgi Ivanov, 21-23-05. 2014g., Shumen.
4. Tasheva Zh. N., R. A. Bogdanov, Tehnologichni reshenia za informatsionna sigurnost, Izdatelstvo na NVU „Vasil Levski, ISBN 978-954-753-130-7, 2013, 110 s.
5. Tasheva Zh. N., Harduerni i softuerni sredstva za informatsionna sigurnost, Izdatelstvo na NVU „Vasil Levski, ISBN 978-954-753-188-8, 2014, 136 s.
6. Tasheva Zh. N., Informatsionni tehnologii za sigurnost, Izdatelstvo na NVU „Vasil Levski, ISBN 978-954-753-190-1, 2014, 176 s.
7. Tasheva Zh. N., Boyanov P. Kr., "Sravnitelen analiz na zlonamereni ueb-bazirani ataki", Nauchna konferentsia na tema „Zashtitata na lichnite danni v konteksta na informatsionnata sigurnost”, Fakultet "Artileria, PVO i KIS" pri Natsionalniyat voenen universitet „Vasil Levski”, gr. Shumen, Balgraia, ISBN 978-954-9681-49-9, 6 - 7 Yuni 2013, str. 178 – 183.Barry B. I., Chan H. A., Intrusion detection systems, Handbook of Information and Communication Security, Springer Berlin Heidelberg, ISBN: 978-3-642-04117-4, pp. 193 – 205.
8. Beale J., Foster J. C., Snort 2.0 Intrusion Detection, Syngress Publishing, 2003, ISBN: 1-931836-74-4, pp. 650.
9. Bejtlich R., The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013, ISBN-13: 978-1593275099, pp.376.
10. Berenjkoub, Mehdi S. H. F. H., A Taxonomy for Network Vulnerabilities, International Journal of Information & Communication Technology, May 2010, Vol.2, №1, pp. 29-44.
11. Boyanov P., Analysis and assessment of several security vulnerability databases, Third International Scientific Conference Science, Education, Innovation, Dedicated To The 145th Anniversary Of Bulgarian Academy Of Sciences And To The 35th Anniversary Of Georgi Ivanov’s Flightissn, ISBN 978-954-577-969-5, vol. II, Shumen, Bulgaria, 21-23 May 2014, pp. 118 – 122.

12. Dimanova D. "Risk management of critical infrastructure sites and facilities". International Scientific Refereed Online Journal With Impact Factor, 2017, ISSN 2367-5721.
13. Dimanova D, Kuzmanov Z, "Measuring and assessing risk". International Scientific Refereed Online Journal With Impact Factor, Issue 32, april 2017, ISSN 2367-5721. www.sociobrains.com.
14. Fry C., Nystrom M., Security Monitoring, O'Reilly Media, 2009, ISBN: 978-0-596-51816-5, pp. 248.
15. Hekmat S, "Communication Networks", "PragSoft Corporation", USA, 2005 г.
16. Helmer, Guy, et al. "A software fault tree approach to requirements analysis of an intrusion detection system", Requirements Engineering 7.4 (2002): 207-220.
17. Nachev, A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. Informatsionnыe tehnologii i bezopasnosty, Zhurnal Akad. nauk Ukrainы., Spets. vыpusk, Kiev, 2013, Str. 79-86
18. Ogletree, Terry William, ed. Upgrading and repairing networks. Que Publishing, 2004.
19. Stanev St., Szczypiorski Krzysztof., Steganography Training: a Case Study from University of Shumen in Bulgaria, Intl Journal Of Electronics And Telecommunications, 2016, Vol. 62, No. 3, Pp. 315-318, Manuscript received September 7, 2016; revised September, 2016, DOI: 10.1515/eletel-2016-0043.
20. Tasheva, Z. N., Tasheva, A. T. Combining cryptography and steganography in software system for hiding confidential information, International Journal of Science, Education and Innovation, Volume 1, 2013. ISSN 1314-9784, Association Scientific and Applied Research, pp. 84-92.