



REALIZATION OF A TCP SYN FLOOD ATTACK USING KALI LINUX

Dejan V. Vuletić^a, Nemanja D. Nojković^b

^a University of Defence in Belgrade, Strategic Research Institute,
Belgrade, Republic of Serbia,
e-mail: dejan.vuletic@mod.gov.rs,
ORCID iD:  <http://orcid.org/0000-0001-9496-2259>

^b Serbian Armed Forces, General Staff,
Department for Telecommunication and Informatics (J-6),
Command Information Systems and IT Support Centre,
Belgrade, Republic of Serbia,
e-mail: nemanjanojko@gmail.com,
ORCID iD:  <https://orcid.org/0000-0002-3216-1891>

DOI: 10.5937/vojtehg66-16419; <https://doi.org/10.5937/vojtehg66-16419>

FIELD: Computer Sciences

ARTICLE TYPE: Professional Paper

ARTICLE LANGUAGE: English

Summary:

Denial-of-Service (DoS) is a type of attack that attempts to prevent legitimate users from accessing network services. This is accomplished by overloading network services or by excessive connectivity, causing a drop in a connection or a service. DoS tools are designed to send large numbers of requests to the targeted server (usually web, FTP, e-mail server), in order to overwhelm server resources and make it unusable. There are various ways in which attackers achieve this. One of the usual ways is simply overwhelming the server by sending too many requests. This will disable the normal functioning of the server (and the web pages will open more slowly), and in some cases it can lead to a situation that the server ceases to operate. This paper shows some effects of TCP Syn Flood Attacks (using Kali Linux) through the change of processor utilization and the unavailability of the target computer (executing ping command).

Key words: DoS attack, Kali Linux, ping, processor utilization.

Introduction

The Transmission Control Protocol (TCP), unlike the User Datagram Protocol (UDP), is based on a connection, which means that the sending packet must establish a complete connection with its recipient or its intended recipient before sending any packets. This protocol relies on a three-way handshake mechanism (SYN, SYN-ACK, ACK) where each request forms a semi-open connection (SYN), a response request (SYN-ACK), and a confirmation to the response (ACK). Any attack attempting

to abuse the TCP/IP protocol would usually do this by sending the TCP packet in the wrong order, causing the target server to run out of resources. One of the examples of this type of attacks is TCP SYN Flood (Lawrence, 2012).

In the TCP handshake mechanism, there must be an arrangement between each side in order for the connection to be established. If a TCP client does not exist or it is a client with a fake IP address, such an arrangement is not possible. In a TCP SYN or SYN flood attack, attackers set the situation for the server to believe that they require a legitimate connection through a number of TCP requests that come from a fake IP address. In a situation when the client's IP address is fake or the client is unable to respond, the certificate (ACK packet) is never sent back from the server. The server is forced to maintain an open connection and buffer for each request for the original connection, attempting to resend the SYN-ACK packet request before the request expires. Having in mind the fact that server resources are limited and SYN flood often includes a huge number of connection requests, the server is unable to process existing requests before new requests arrive and this results in service termination.

Figure 1 shows the TCP SYN Flood attack pattern with corresponding messages sent between the server and a legitimate user, as well as the server and an attacker. As can be seen in the Figure, the connection confirmation does not arrive to the attacker as it does in the case with the legitimate user (Radware, 2013).

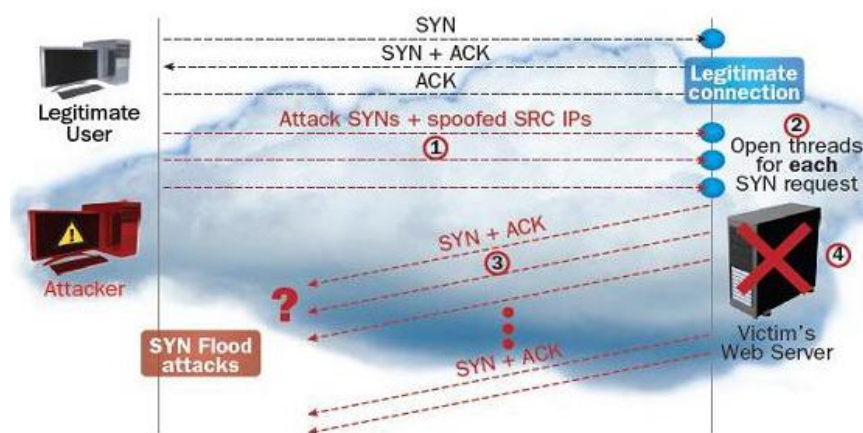


Figure 1 – TCP SYN Flood (Radware, 2013)

Рис. 1 – TCP SYN Flood (Radware, 2013)

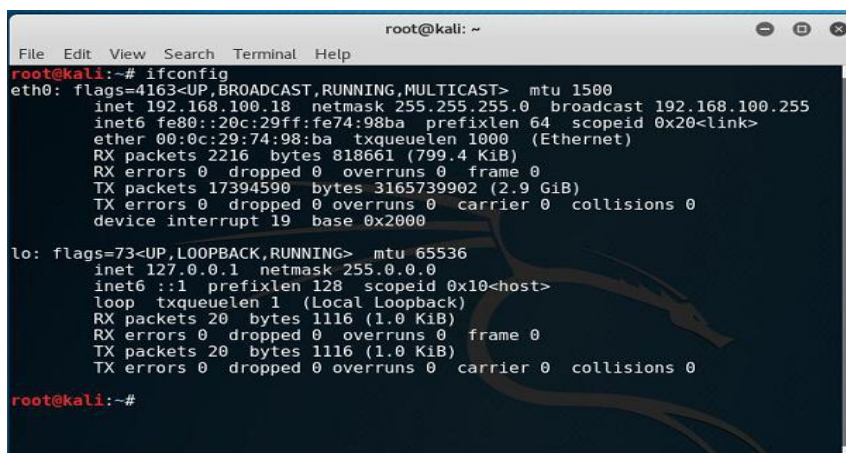
Слика 1 – TCP SYN Flood (Radware, 2013)

Practical realization of TCP Syn Flood Attacks

To display the effects of TCP Syn Flood Attacks, we will use two computers that are connected to the same network. Kali Linux was installed on the attacking computer, as a virtual machine on Windows 10 using VMware Workstation 12 Player. The Windows 10 operating system is installed on the computer that will be attacked (Allen et al, 2014).

A computer that launches the attacks (the attacking computer). Kali Linux based on the Debian distribution is installed on this computer (Hertzog et al, 2017). It contains the hping3 tool, which is a free generator and package analyzer for the TCP/IP protocol. Hping3 is produced by Salvatore Sanfilippo. A newer version of hping3 is a script version which uses Tcl language (a simple language for creating a program) (Beggs, 2014), (Ansari, 2015).

Figure 2 shows the basic network virtual machine data obtained by typing the ifconfig command in the terminal on Kali Linux. The Figure shows that there is IP address information, subnet masks and other network card information.



```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.18 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe74:98ba prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:74:98:ba txqueuelen 1000 (Ethernet)
    RX packets 2216 bytes 818661 (799.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17394590 bytes 3165739902 (2.9 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
  
```

Figure 2 – Basic network virtual machine data
 Рис. 2 – Базовые данные на виртуальной машине
 Слика 2 – Основни подаци на виртуелној машини

The attack is implemented through the terminal by typing the command hping3 with certain parameters (Figure 3):

- The name of the used tool (hping3)
- Number of packets to send (-c 1000)
- Size of each packet that will be sent (-d 128)

- The type of packages to be sent (-s represents the SYN packets)
- TCP Window Size (-w 64)
- The attacking port (-p 8000)
- Type of Attack (- - flood). Flood mode – sending packet as fast as possible.
- Using random source IP addresses (- rand-source)
- Address of the attacked computer (destination IP address)

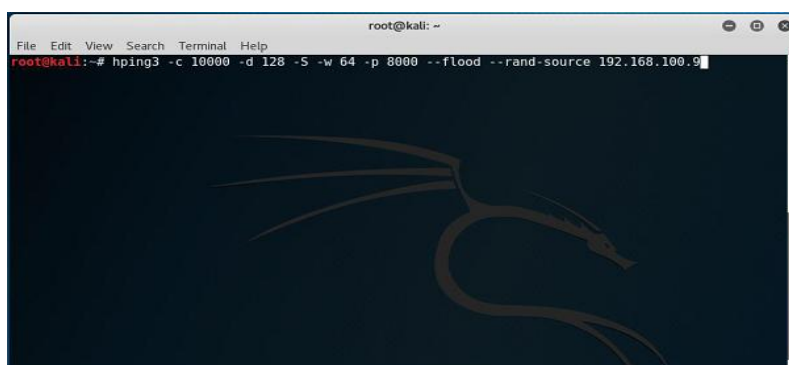


Figure 3 – Entering parameters on the attacking computer
 Рис. 3 – Ввод параметров в компьютер, с которого производится атака
 Слика 3 – Уношење параметара у рачунар којим се напада

Before the attack begins, we are checking the availability of the computer we are planning to attack in the Command Prompt on Windows 10, using the ping command.

Figure 4 shows that there is no problem in the connection and that the ping on the targeted computer was executed.

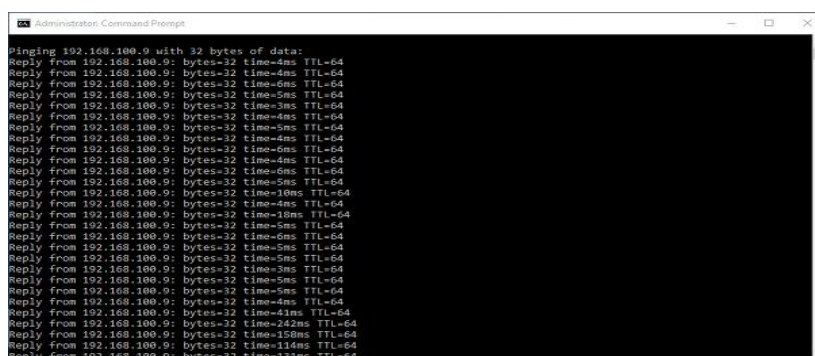


Figure 4 – Checking the availability of the targeted computer using the ping command
 Рис. 4 – Проверка доступности целевого компьютера с помощью команды ping
 Слика 4 – Провера доступности циљаног рачунара употребом ping команде

To increase the intensity of the attack, the command can be started from multiple terminals as shown in Figure 5.

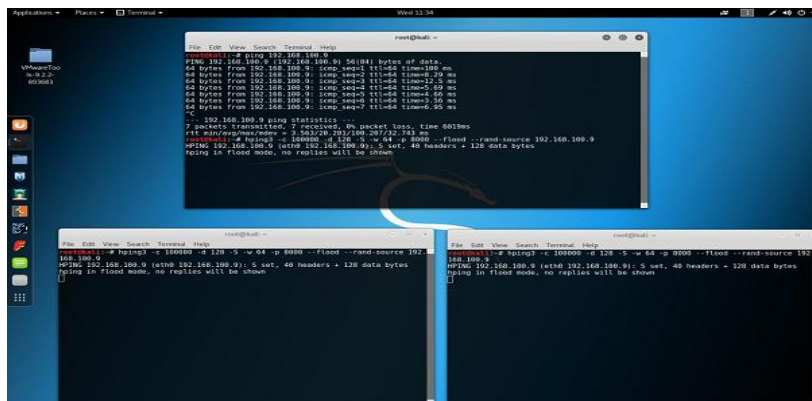


Figure 5 – Starting attacks from multiple terminals

Рис. 5 – Начало атак, нацеленных на несколько терминалов

Слика 5 – Покретања напада на више терминала

After executing the command (realization of the attack) we again use the ping command to check the availability of the attacked computer. Figure 6 shows that the computer partially responds to this command (not always available).

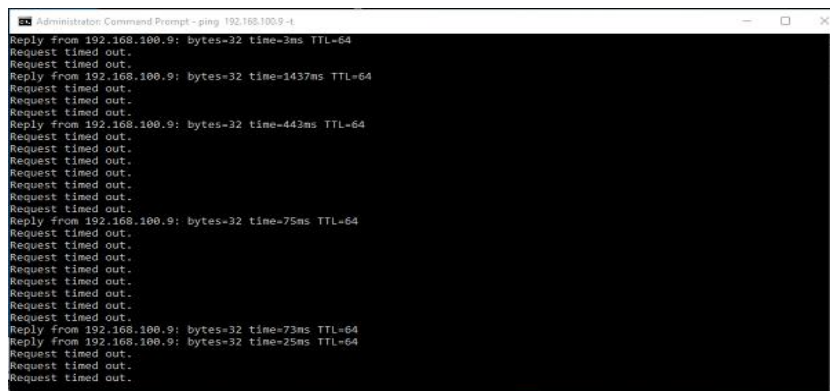


Figure 6 – Checking the availability of the targeted computer after the attack using the ping command

Рис. 6 – Проверка доступности целевого компьютера после атаки, с помощью команды ping

Слика 6 – Провера доступности циљаног рачунара, након напада, употребом ping команде

A computer that will be attacked. We are watching events on this computer before and after the attack against it. Figure 7 shows the basic information about this computer using the ipconfig command in Windows Power Shell. In the Figure, we can see the IP address information, subnet masks, and other features of the network card.

```

Administrator: Windows PowerShell

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::5df2:4708:3758:32a6%12
    IPv4 Address. . . . . : 192.168.255.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8574:5e31:80d:2961%19
    IPv4 Address. . . . . : 192.168.100.9
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 13:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:9d38:953c:38ce:647:a2a9:cb7b
    Link-local IPv6 Address . . . . . : fe80::38ce:647:a2a9:cb7b%11
    Default Gateway . . . . . : 

PS C:\WINDOWS\system32> ping 192.168.100.5

Pinging 192.168.100.5 with 32 bytes of data:
Request timed out.
Reply from 192.168.100.9: Destination host unreachable.
Reply from 192.168.100.9: Destination host unreachable.

Ping statistics for 192.168.100.5:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
PS C:\WINDOWS\system32>
  
```

Figure 7 – Data on the attacked computer
 Рис. 7 – Данные на взломанном компьютере
 Слика 7 – Подаци на нападнутом рачунару

After executing the command on Kali Linux, the performance of the attacked computer has changed, as shown in Figure 8. By comparing images, it can be noted that processor utilization has increased. In addition to the performance changes, the attack made the computer unable to respond to connection requests, as shown by the ping command Request timed out. Due to the attacks, the computer could not connect and communicate with another computer on the network.

The interruption of the attack on the terminals is accomplished by pressing the Ctrl + C key. In addition to the performance changing, after stopping the attack, the ping command begins to work normally (it shows that the computer is available). This is shown in Figure 9.

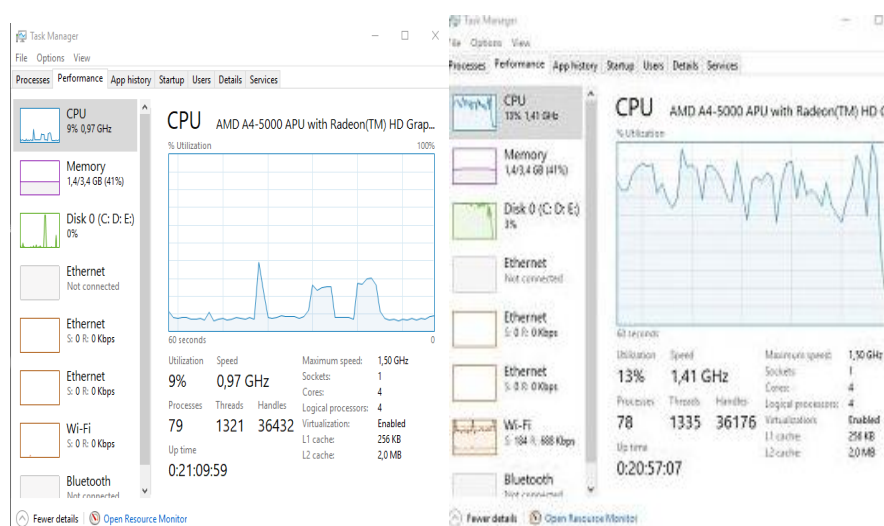


Figure 8 – CPU utilization before and during the attack
 Рис. 8 – Загруженность процессора до и после атаки
 Слика 8 – Искоришћеност процесора пре и током напада

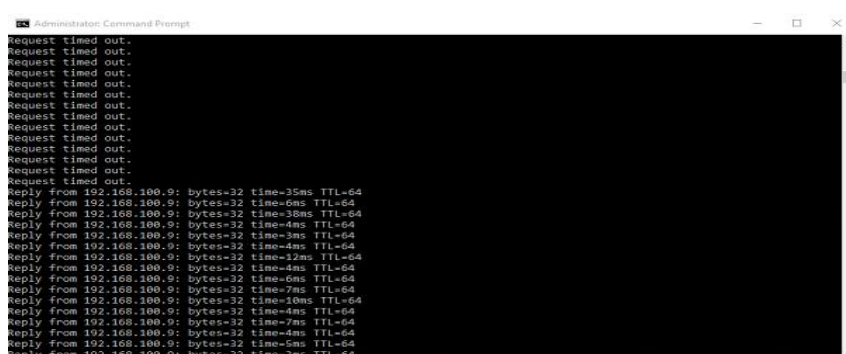


Figure 9 – Appearance of the screen when the attack is completed and the ping command is given

Рис. 9 – Экран после завершения атаки и после команды ping
 Слика 9 – Изглед екрана када је напад завршен и задата ping команда

Conclusion

Every system that is connected to the Internet and equipped with TCP-based network services is a potential victim of an attack. The earliest form of DoS attack was SYN flood, which originated in 1996 and exploits weaknesses in the TCP. Other attacks exploit weaknesses in

operating systems and applications, leading to the inaccessibility of network services or even cessation of server operation.

Classic DoS attacks are one-on-one attacks in which a powerful host generates traffic that "overwhelms" the target host's connection, which hinders authorized clients from accessing network services. Distributed Denial of Service (DDoS) is a type of DoS attack that is used by multiple users. DDoS attacks have gone a step further, which is multiplying, resulting in the fact that servers or parts of the network can be totally unusable for clients.

There are several ways to execute DoS attacks such as TCP SYN Flood attack which can be done with different tools, such as Kali Linux.

References

Allen, L., Heriyanto, T. & Ali, S. 2014. *Kali Linux – Assuring Security by Penetration Testing*. Birmingham, UK: Packt Publishing, pp.14-28.

Ansari, A.J. 2015. *Web Penetration Testing with Kali Linux*. Birmingham, UK: Packt Publishing, p.4.

Beggs, R.W. 2014. *Mastering Kali Linux for Advanced Penetration Testing*. Birmingham, UK: Packt Publishing, pp.315-316.

Hertzog, R., Aharoni, M., & O'Gorman, J. 2017. *Kali Linux Revealed: Mastering the Penetration Testing Distribution*. Offsec Press.

Lawrence, C.M. 2012. *DDoS For Dummies, Corero Network Security Edition*. [e-book]. Hoboken, New Jersey: John Wiley & Sons. Available at: <http://crezer.net/Newsletter/archivos/DDoS.pdf>. Accessed: 10.02.2018.

-Radware. 2013. *DDoS Survival Handbook*. [e-book]. Radware, Ltd. Available at: https://security.radware.com/uploadedfiles/resources_and_content/ddos_handbook/ddos_handbook.pdf. Accessed: 10.02.2018.

РЕАЛИЗАЦИЯ TCP SYN FLOOD АТАК С ИСПОЛЬЗОВАНИЕМ KALI LINUX

Деян В. Вулетић^а, Немања Д. Нойкович^б

^а Университет обороны в г. Белград, Институт стратегических исследований, г. Белград, Республика Сербия

^б Вооружённые Силы Республики Сербия, Генеральный штаб, Управление информатики и телекоммуникаций (J-6), Центр командно-информационных систем, г. Белград, Республика Сербия

ОБЛАСТЬ: компьютерные науки

ВИД СТАТЬИ: профессиональная статья

ЯЗЫК СТАТЬИ: английский

Резюме:

Хакерская атака «отказ в обслуживании» (*Denial-of-Service - DoS*) – это вид взлома вычислительной системы с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ становится значительно затруднённым. DoS инструменты отсылают большое количество запросов целевому серверу (как правило web, FTP, электронная почта), перезагружая его ресурсы, что в итоге приводит к отказу в обслуживании. Хакерами разработано несколько методов для достижения своей цели. Один из них – это чрезмерная перезагрузка сервера огромным количеством запросов. Данные действия мешают нормальной работе сервера (вследствие чего web-страницы намного медленнее открываются), а в некоторых случаях это может привести к полному отказу в обслуживании. В данной статье были представлены отдельные эффекты TCP Syn Flood Attacks (с использованием Kali Linux), отражаемые в изменениях загруженности процессора и недоступности целевого компьютера (для ping команды).

Ключевые слова: DoS атака, Kali Linux, ping, загруженность процессора.

РЕАЛИЗАЦИЈА TCP SYN FLOOD НАПАДА УПОТРЕБОМ КАЛИ ЛИНУКСА

Дејан В. Вулетић^а, Немања Д. Нојковић^б

^а Универзитет одбране у Београду, Институт за стратегијска истраживања, Београд, Република Србија

^б Војска Србије, Генералштаб, Управа за телекомуникације и информатику (Ј-6), Центар за командно-информационе системе и подршку, Београд, Република Србија

ОБЛАСТ: рачунарске науке

ВРСТА ЧЛАНКА: стручни чланак

ЈЕЗИК ЧЛАНКА: енглески

Сажетак:

Напад одбијања услуга (*Denial-of-Service – DoS*) врста је напада којим се спречава да овлашћени корисници приступе одговарајућим мрежним услугама. То се постиже преоптерећењем мрежних услуга или прекобројним конекцијама, што доводи до прекида (отежане) конекције или услуге. DoS алати шаљу велики број захтева циљаном серверу (обично web, FTP, e-mail сервер) ради преоптерећења његових ресурса, чинећи га на тај начин неупотребљивим. Један од честих начина на које нападачи то

постигну јесте преоптерећење сервера слањем великог броја захтева. Таква активност онемогућиће нормално функционисање сервера (и web странице ће се отварати много спорије), па ће у неким случајевима престати и да функционише. У чланку су приказани одређени ефекти TCP Syn Flood Attacks (употребом Kali Linux-а) кроз промену искоришћености процесора и недоступности циљаног рачунара (извршавањем ping команде).

Кључне речи: DoS напад, Kali Linux, ping, искоришћеност процесора.

Paper received on / Дата получения работы / Датум пријема чланка: 02.02.2018.
Manuscript corrections submitted on / Дата получения исправленной версии работы /
Датум достављања исправки рукописа: 13.04.2018.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум
коначног прихватања чланка за објављивање: 15.04.2018.

© 2018 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). This article is an open access article distributed under the
terms and conditions of the Creative Commons Attribution license
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2018 Авторы. Опубликовано в «Военно-технический вестник / Vojnotehnički glasnik / Military
Technical Courier» (www.vtg.mod.gov.rs, втг.мо.упр.срб). Данная статья в открытом доступе и
распространяется в соответствии с лицензией «Creative Commons»
(<http://creativecommons.org/licenses/by/3.0/rs/>).

© 2018 Аутори. Објавио Војнотехнички гласник / Vojnotehnički glasnik / Military Technical Courier
(www.vtg.mod.gov.rs, втг.мо.упр.срб). Ово је чланак отвореног приступа и дистрибуира се у
складу са Creative Commons licencom (<http://creativecommons.org/licenses/by/3.0/rs/>).

