Eksploatacija ranjivosti, detekcija, i Incident Response izveštaj

Ime studenta: Jovana Jelić **E2 138/2024**  
Datum:11/12/2024

Pregled Ranljivosti

Za svaku eksploatisanu ranljivost:

* 1. **Informacije o ranljivosti**ID ranljivosti (CVE): CVE-2012-0002  
     Pogođen servis: Remote Desktop Protocol (RDP)  
     CVSS ocena: 7.1 (High)  
     Opis ranljivosti:  
     (Uključite kratak opis ranljivosti, pogođeni servis i severity)

MS12-020 predstavlja ranjivost u Microsoftovom RDP servisu koja omogućava napadaču da izazove rušenje sistema korišćenjem posebno oblikovanih paketa. Ovo je DoS (Denial of Service) -gde je glavni cilj napada učiniti RDP servis nedostupnim (prekid rada ili restart sistema), a ne dobijanje daljinskog pristupa sistemu -napad koji može da isključi uslugu ili čitavu mašinu.

Remote Desktop Protocol

**Omogućavanje daljinske kontrole:**

* Korisnici mogu da upravljaju udaljenim računarom, kao da sede ispred njega.
* GUI udaljenog računara se prenosi korisniku.

**Komunikacioni protokol:**

* Koristi **TCP port 3389** po defaultu za komunikaciju.
* Podržava šifrovanje kako bi se obezbedila sigurnost podataka u komunikaciji.

**Multifunkcionalnost:**

* Korisnici mogu da otvaraju fajlove, pokreću aplikacije i obavljaju administrativne zadatke na udaljenim sistemima.
* Podržava funkcionalnosti kao što su prenosi fajlova, deljenje štampača i međusobno deljenje radne površine.
  1. **Opis eksploita**Izvor eksploita:   
     (Link ka public available eksploitu ili naziv metasploit modula)

Metasploit modul: auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids

Metod eksploatacije:  
(kratak opis principa kako exploit radi)

Napad funkcioniše tako što se na ranjivu mašinu šalje posebno oblikovan RDP zahtev koji preoptereti resurse sistema i izaziva pad servisa.

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)

Operativni sistem: Windows Server 2008 R2 SP1

Servis: Remote Desktop Protocol (RDP)

Port: TCP/3389

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

Metasploit Framework

Modul: auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids

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

**1. Pokretanje Metasploit Framework-a:**  
Pokrenuli smo msfconsole na našem sistemu. **msfconsole -komanda pokreće Metasploit Framework konzolu, glavnu alatku za eksploataciju ranjivosti.**

1. **Izbor modula:**  
   Koristili smo use auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids za odabir specifičnog Metasploit modula.

use bira specifičan modul iz Metasploit Framework-a.

Modul auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids je namenjen za eksploataciju ranjivosti u RDP protokolu na Windows mašinama.



1. **Podešavanje opcija:**  
   Postavili smo ciljne IP adrese i port:

* Komanda set postavlja parametre za ciljne adrese.

RHOSTS definiše IP adresu ranjive mašine (ovde: 192.168.8.121).

* RPORT definiše port na kojem se ciljni servis izvršava.

RDP servis koristi port 3389 prema podrazumevanim postavkama.

* run -Pokreće odabrani modul koristeći prethodno definisane parametre (RHOSTS i RPORT).

Modul šalje posebno oblikovane pakete prema cilju kako bi izazvao prekid rada servisa.



1. **Pokretanje eksploita:**  
   Modul je pokrenut komandom run.

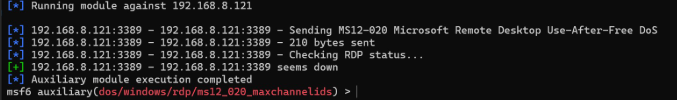
**Metasploit šalje pakete cilju:**  
Eksploit modul koristi RDP protokol da šalje posebno oblikovane pakete, koje Windows Server 2008 ne može pravilno da obradi. Ovo izaziva "use-after-free" grešku.

**Provera stanja RDP servisa:**  
Nakon što su paketi poslati, modul proverava da li je RDP servis dostupan. Log poruka 192.168.8.121:3389 seems down ukazuje da je ciljna mašina izgubila funkcionalnost RDP servisa.

1. **Rezultat:**  
   Eksploatacija je bila uspešna; RDP servis na ciljnoj mašini prestao je sa radom.

Eksploit je iskoristio grešku u upravljanju memorijom u RDP protokolu (CVE-2012-0002), što je dovelo do rušenja servisa.

Uspešan rezultat (seems down) znači da ciljni servis više nije funkcionalan, što je krajnji cilj ovog DoS napada.



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

RDP servis na ciljnom sistemu je postao nedostupan, što ukazuje na uspešno izvršen Denial of Service napad.

A computer screen shot of a blue screen

Description automatically generated

Detekcija Korišćenjem Wazuh SIEM-a

Za svaku eksploatisanu ranljivost:

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)

**Pravila korišćena za detekciju**:

Wazuh je koristio pravila povezana sa RDP aktivnostima i Windows događajima za detekciju anomalija koje se odnose na MS12-020 eksploataciju.

**ID pravila**:

1. 60106 – Windows Logon Success

* Detektuje uspešno prijavljivanje na sistem, što može ukazivati na neovlašćen pristup nakon eksploatacije.
* **MITRE ID**: T1078
* **Taktike**: Defense Evasion, Persistence, Privilege Escalation, Initial Access

1. 60122 – Logon Failure - Unknown user or bad password

* Detektuje neuspešne pokušaje prijavljivanja koji mogu prethoditi eksploataciji.
* **MITRE ID**: T1531
* **Taktike**: Impact

1. 506 – Wazuh agent stopped

* Signalizira gašenje Wazuh agenta, što može biti pokušaj napadača da izbegne detekciju.
* **MITRE ID**: T1562.001
* **Taktika**: Defense Evasion

1. 67018 – System shutdown initiated

* Detektuje restartovanje ili gašenje sistema, što može biti deo aktivnosti napadača nakon eksploatacije.
* **MITRE ID**: T1529
* **Taktika**: Impact

1. 67028 – Special privileges assigned to new logon

* Ukazuje na eskalaciju privilegija nakon uspešne eksploatacije.
* **MITRE ID**: T1484
* **Taktike**: Defense Evasion, Privilege Escalation

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)

Wazuh agent je instaliran na ciljanom Windows Server 2008 R2 sistemu.

**Konfiguracija**:

Agent je povezan sa Wazuh Managerom koristeći definisan ossec.conf fajl na sledeci nacin

Omogućeno prikupljanje događaja iz:

* **Windows Event Logs** (Application, Security, System)

Sinhronizovani pomoću unikatnih ključeva.

A computer screen with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

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

Wazuh SIEM je uspešno detektovao napad putem MS12-020 ranjivosti:

Pravila kao što su 67018, 506, i 60106 omogućila su korelaciju događaja.

Prikupljeni logovi su ukazali na restart sistema i eskalaciju privilegija.

**Napad MS12-020 na RDP port (3389)**:

* Eksploatacija je inicirana putem MS12-020 modula.
* RDP servis je postao nedostupan, što je ukazano kroz logove sistema.

A screenshot of a computer

Description automatically generated

A close-up of a graph

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Prikupljeni logovi**:

* Aktivirana su sledeća pravila:
  + **67018**: Gašenje sistema nakon napada (restart je posledica eksploatacije).
  + **506**: Wazuh agent prestao da radi tokom napada.
  + **60106**: Prijava na sistem sa eskaliranim privilegijama.
  + **67028**: Pridodeljene specijalne privilegije.

**Detekcija putem Wazuh Dashboard-a**:

* Na Wazuh Dashboardu, pregledani su incidenti filtrirani prema:
  + **Host name**: winsrv.
  + **Rule ID**: 67018, 506, 60106.
* Ovim potvrfjujrmo događaje:
  + Logovi ukazuju na restart sistema nakon eksploatacije.
  + Evidentirani su pokušaji prijavljivanja i dodeljivanje privilegija.

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)