Subject: OT Forse tentativo di intrusione?
Posted by Alessandro on Wed, 08 Dec 2010 12:50:17 GMT
View Forum Message <> Reply to Message

Salve, posto qui la mia domanda perchÃ© non saprei a chi altro chiedere.

Il mio firewall (firestarter) ha rilevato in rosso una intrusione (credo).
Questi i dati che rileva:
-IP Sorgente: 172.23.0.1
-Protocollo: ICMP
-Servizio: DNS

-Uso linux mint 9.
-Utilizzo un router wireless.
-Uso Opendns.

Avete idea di cosa succede? mi ha rilevato questi tentativi di accesso dalle 5
di questa mattina.

Grazie.

Subject: Re: OT Forse tentativo di intrusione?
Posted by Lorenzo Mainardi on Wed, 08 Dec 2010 13:18:42 GMT
View Forum Message <> Reply to Message

Il Wed, 08 Dec 2010 13:50:17 +0100, Alessandro scrisse:

> -IP Sorgente: 172.23.0.1
> -Protocollo: ICMP

Un ping?

--
"Never underestimate the bandwidth of a station wagon full of tapes
hurtling down the highway" - Andrew S. Tanenbaum
http://blog.mainardi.me
python -c "print 'bG9ybWF5bmFAZ21haWwuY29t'.decode('base64')"

Subject: Re: OT Forse tentativo di intrusione?
Posted by mario on Wed, 08 Dec 2010 13:57:08 GMT
View Forum Message <> Reply to Message

Il 08/12/2010 13:50, Alessandro ha scritto:
> Salve, posto qui la mia domanda perchÃ© non saprei a chi altro chiedere.
>

> Il mio firewall (firestarter) ha rilevato in rosso una intrusione (credo).
> Questi i dati che rileva:
> -IP Sorgente: 172.23.0.1
> -Protocollo: ICMP
> -Servizio: DNS
>
> -Uso linux mint 9.
> -Utilizzo un router wireless.
> -Uso Opendns.
>
> Avete idea di cosa succede? mi ha rilevato questi tentativi di accesso
> dalle 5 di questa mattina.
>
> Grazie.

Non preoccuparti per il tentativo di intrusione, Ã¨ praticamente
impossibile che un computer non ne sia oggetto durante anche pochi
minuti di connessione, puoi comunque capire da dove provengono digitando
sul programma Whois di "Strumenti di rete" il numero di IP sorgente.
Opendns Ã¨ utilizzato frequentemente dagli spammatori, quindi le tue
email potrebbero erroneamente essere considerate spam da alcuni antivirus.
Saluti Mario

Subject: Re: OT Forse tentativo di intrusione?
Posted by Lorenzo Mainardi on Wed, 08 Dec 2010 14:02:11 GMT
View Forum Message <> Reply to Message

Il Wed, 08 Dec 2010 14:57:08 +0100, mario scrisse:

> Opendns Ã¨ utilizzato frequentemente dagli spammatori, quindi le tue
> email potrebbero erroneamente essere considerate spam da alcuni
> antivirus.

Che c'entra un servizio DNS con l'invio dello spam?

--
"Never underestimate the bandwidth of a station wagon full of tapes
hurtling down the highway" - Andrew S. Tanenbaum
http://blog.mainardi.me
python -c "print 'bG9ybWF5bmFAZ21haWwuY29t'.decode('base64')"

Subject: Re: OT Forse tentativo di intrusione?
Posted by mario on Wed, 08 Dec 2010 14:23:27 GMT
View Forum Message <> Reply to Message

Il 08/12/2010 15:02, Lorenzo Mainardi ha scritto:
> Il Wed, 08 Dec 2010 14:57:08 +0100, mario scrisse:
>
>> Opendns Ã¨ utilizzato frequentemente dagli spammatori, quindi le tue
>> email potrebbero erroneamente essere considerate spam da alcuni
>> antivirus.
>
> Che c'entra un servizio DNS con l'invio dello spam?
>

Opendns svincola la connessione dal controllo del provider (e ciÃ² e
anche un vantaggio per la privacy).Tale servizio fu lanciato nel 2006
dall'hacker David Ulevitch.
Ciao Mario

Subject: Re: OT Forse tentativo di intrusione?
Posted by Davide Bianchi on Wed, 08 Dec 2010 15:05:12 GMT
View Forum Message <> Reply to Message

On 2010-12-08, Alessandro <alessandro@mail.invalid> wrote:
> Salve, posto qui la mia domanda perchÃ© non saprei a chi altro chiedere.
>
> Il mio firewall (firestarter) ha rilevato in rosso una intrusione (credo).
> Questi i dati che rileva:
> -IP Sorgente: 172.23.0.1
> -Protocollo: ICMP
> -Servizio: DNS

Quello e' un blocco "privato" e non routabile. Verifica da dove ti e'
arrivato il ping perche' se non ti e' arrivato dal tuo provider e'
arrivato dalla tua rete.

Davide

--
Bill Gates to his broker:
"You idiot, I said $150 million on SNAPPLE!!!"

Subject: Re: OT Forse tentativo di intrusione?
Posted by Alessandro on Wed, 08 Dec 2010 17:58:57 GMT
View Forum Message <> Reply to Message

Il 08/12/2010 16:05, Davide Bianchi ha scritto:
> On 2010-12-08, Alessandro<alessandro@mail.invalid> wrote:
>> Salve, posto qui la mia domanda perchÃ© non saprei a chi altro chiedere.

>>
>> Il mio firewall (firestarter) ha rilevato in rosso una intrusione (credo).
>> Questi i dati che rileva:
>> -IP Sorgente: 172.23.0.1
>> -Protocollo: ICMP
>> -Servizio: DNS
>
> Quello e' un blocco "privato" e non routabile. Verifica da dove ti e'
> arrivato il ping perche' se non ti e' arrivato dal tuo provider e'
> arrivato dalla tua rete.
>
> Davide
>
Come faccio a verificare da dove arriva il ping ?
Ho fatto un whois ma diceva poco, e cercando su google sembra essere un servizio standard DSN, quello che mettono certi provider di default.

Subject: Re: OT Forse tentativo di intrusione?
Posted by Alessandro Selli on Thu, 09 Dec 2010 08:49:06 GMT
View Forum Message <> Reply to Message

Alessandro ha scritto:
> Il 08/12/2010 16:05, Davide Bianchi ha scritto:
>> On 2010-12-08, Alessandro<alessandro@mail.invalid> wrote:
>>> Salve, posto qui la mia domanda perchÃ© non saprei a chi altro chiedere.
>>>
>>> Il mio firewall (firestarter) ha rilevato in rosso una intrusione
>>> (credo).
>>> Questi i dati che rileva:
>>> -IP Sorgente: 172.23.0.1
>>> -Protocollo: ICMP
>>> -Servizio: DNS
>>
>> Quello e' un blocco "privato" e non routabile. Verifica da dove ti e'
>> arrivato il ping perche' se non ti e' arrivato dal tuo provider e'
>> arrivato dalla tua rete.
>>
>> Davide
>>
> Come faccio a verificare da dove arriva il ping ?

  Gl'indirizzi 172.16.0.0/12 sono indirizzi provati che non devono essere mai presenti su Internet. O il tuo provider ha dei problemi (e se si la cosa deve essergli comunicata), o il ping proviene dalla *tua* rete privata.

> Ho fatto un whois ma diceva poco,

Ti dice proprio che quel blocco di indirizzi Ã¨ privato:

Comment: This block is used as private address space.
Comment: Addresses from this block can be used by
Comment: anyone without any need to coordinate with
Comment: IANA or an Internet registry. Addresses from
Comment: this block are used in multiple, separately
Comment: operated networks.
Comment: This block was assigned by the IETF in the
Comment: Best Current Practice document, RFC 1918
Comment: which can be found at:
Comment: http://www.rfc-editor.org/rfc/rfc1918.txt

> e cercando su google sembra essere un
> servizio standard DSN, quello che mettono certi provider di default.

Il DNS standard usa pacchetti UDP o TCP, non ICMP:

ftp://ftp.rfc-editor.org/in-notes/rfc1034.txt

In the Internet, queries are carried in UDP datagrams or over
TCP connections.

ICMP non compare da nessuna parte esplicitamente nel documento. C'Ã¨, Ã¨ vero, questo servizio DNS che viaggia su ICMP:

ftp://ftp.rfc-editor.org/in-notes/rfc1788.txt

ICMP Domain Name Messages

Ã^ perÃ² un protocollo sperimentale, ed Ã¨ rimasto in questo stato senza aggiornamenti dalla sua prima versione del 1995 e usa due ICMP-type (37, Domain Name Request e 38, Domain Name Reply) che non trovo siano stati definiti in nessuna RFC (e che infatti iptables -p icmp -h non elenca); sarei sorpreso che il tuo provider lo usi. Ma in ogni caso, pacchetti dalla rete 172.16.0.0/12 in ingresso da un'interfaccia con IP pubblico non ne devono mai arrivare.

Per essere sicuro che questi paccehtti entrino dalla tua interfaccia pubblica (o da quella verso il tuo modem) puoi usare tcpdump. Ad esempio, potresti fare (da root), nell'ipotesi che la tua interfaccia di rete di cui sopra sia la eth0:

tcpdump -i eth0 'icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply'

Questo ti fa vedere tutti i pacchetti ICMP non ping che transitano sulla tua interfaccia. Oppure usi src net 172.16.0.0/12 per vedere ogni genere di pacchetto proveniente da quella rete, o tutte e due le cose.

Ciao,

--
Alessandro Selli http://alessandro.route-add.net
AVVERTENZA: i messaggi inviati a "trappola" non mi arriveranno.
WARNING: messages sent to "trappola" will never reach me.