N-Partner solution

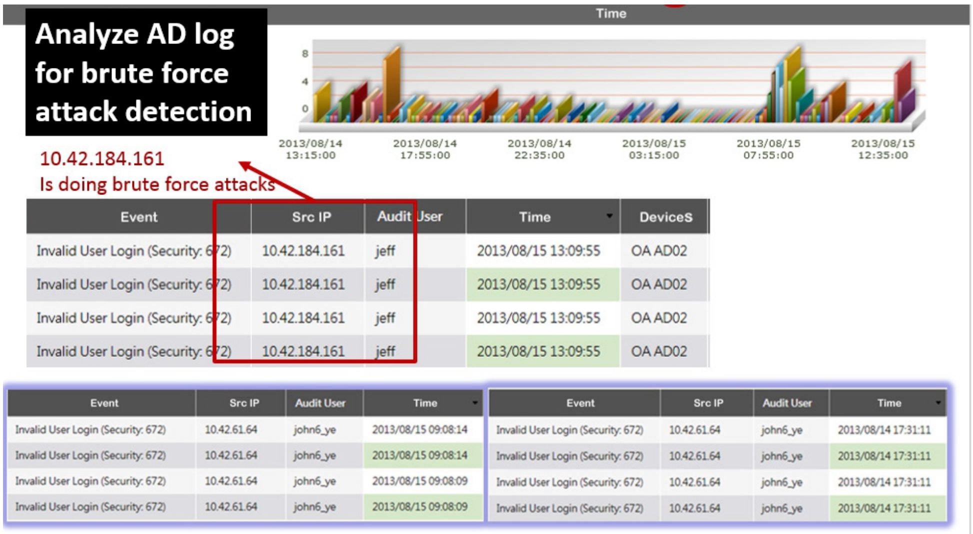
To protect password from brute-force attacks is the most important thing to ensure network safety

There will be huge loss if the staffs cannot access IT resources or the password is decoded

Now IT systems are widely used and it is common to use Windows domain for authentication and authorization. However there is a risk that anyone having the account and password can use the system freely. Brute-force attack is one of the most common ways to attack. Hackers run the brute-force program in the intranet trying to log in. IT administrators tend to limit the numbers of login errors for password protection and once going beyond the limit the accounts will be locked for some time. That seems what has to be done however after brute-force attacks lots of accounts will be locked and the staffs cannot log in their own accounts. That can lead to negative effects for enterprise operation. To prevent the damage IT departments must give up the old way and set up a new one for operation that can do intelligent analysis. As soon as a Brute-force attack happens the IP and location of the attacker will be identified and warnings will be sent out to help IT departments separate the attacker in minimum time.

Automatic learning and analysis technology develop intelligent network operations

N-Partner uses big data analysis for automatic learning based on Windows AD log. If there is abnormal amount of log-in failure IT departments will receive real-time alerts including source IP address and the accounts used to log in. Besides through the analysis technology another type of alerts will be sent out when someone log in successfully after several failures that will be seen as the password is decoded by brute-force method. Especially when the cracked account has high authority IT departments must get real-time warnings so that they can set new passwords to prevent enterprises from suffering enormous loss.



Analyze AD log for brute force attack detection

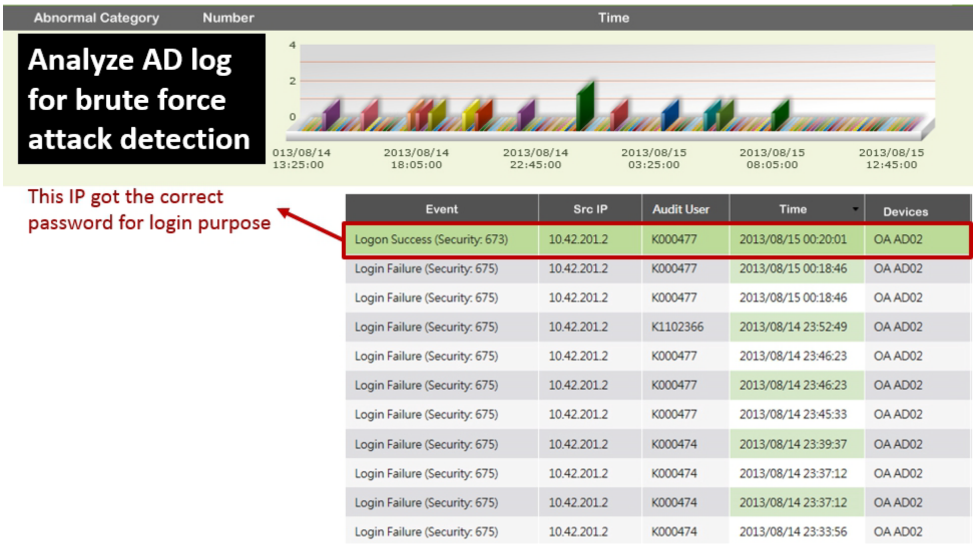
10.42.184.161
Is doing brute force attacks

Event	Src IP	Audit User	Time	DeviceS
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02

Event	Src IP	Audit User	Time
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:14
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:14
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:09
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:09

Event	Src IP	Audit User	Time
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11

N-Partner's intelligent brute-force attack analysis helps IT administrators catch malicious sources in real time without any manual configuration.

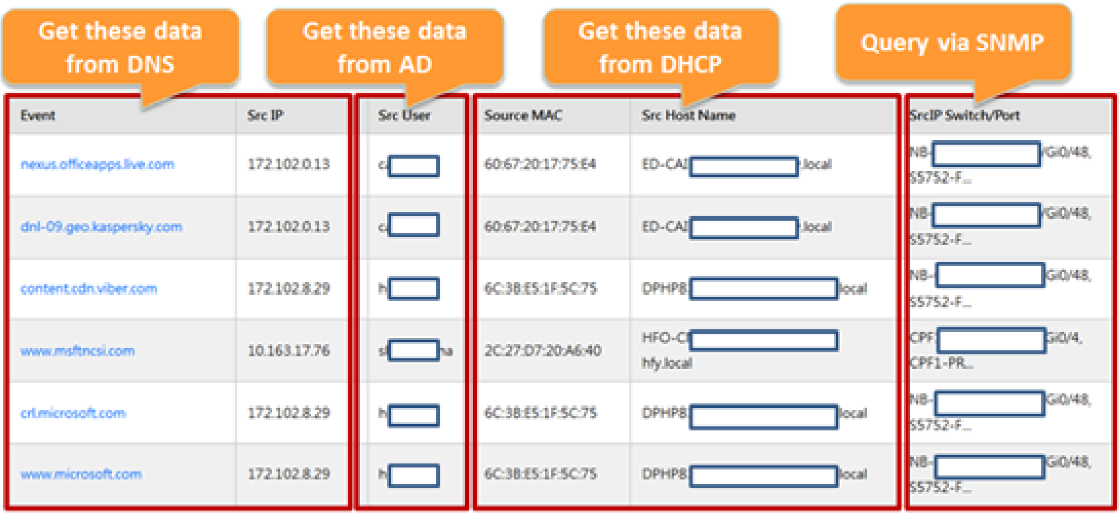


Event	Src IP	Audit User	Time	Devices
Logon Success (Security: 673)	10.42.201.2	K000477	2013/08/15 00:20:01	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/15 00:18:46	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/15 00:18:46	OA AD02
Login Failure (Security: 675)	10.42.201.2	K1102366	2013/08/14 23:52:49	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:46:23	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:46:23	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:45:33	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:39:37	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:37:12	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:37:12	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:33:56	OA AD02

A successful login after several failures should be noted

Correlate AD and SNMP with the analysis result to get the user name and location info

N-Partner s core technology can integrate SNMP the surveillance system Flow the flow analysis system and Syslog the log store and searching or SIEM for the IT departments to keep tabs on the network usage. Also with the user name provided by Windows AD log N-Partner s core technology can correlate it with other logs and SNMP MIB data. Through N-Reporter/N-Cloud system which produce by N-Partner IT departments will know which IP address correlate to user name has abnormal network traffic or is attacking the enterprises. SNMP is used to find out the IP address s location that is the switch and interface it belongs in.



Event	Src IP	Src User	Source MAC	Src Host Name	SrcIP Switch/Port
nexus.officeapps.live.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CA[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
dnl-09.geo.kaspersky.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CA[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
content.cdn.viber.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.msftncsi.com	10.163.17.76	s[redacted]ha	2C:27:D7:20:A6:40	HFO-C[redacted] hfy.local	CPF[redacted]Gi0/4, CPF1-PR...
crl.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...

Use Flow/Syslog/SNMP correlation to find the IP address and location with behavior anomaly

N-Partner introduction

N-Partner Technology Ltd. Co. founded in 2011 specializes in Big Data and AI and Abnormal Analysis. The headquarters is set in Taichung Taiwan. All of our core members have over 15 years of experience in Network Operations and software development. We have professional experts in various fields including internet information security operation system Kernel hardware and virtual machine C language PHP/Java database big data processing and Cloud computing architecture artistic designing etc. N-Reporter and N-Cloud developed by N-Partner are the only IT operating systems that can integrate SNMP Flow and Syslog and that make IT administrators debug more easily. We use the leading technology including Any-to-Any analysis which establishes Dynamic Benchmarks based on each event log and history to detect abnormal activities and to send out real-time alerts. What is more Cloud computing architecture is used in N-Cloud for high processing efficiency high expandability and the ability for lots of people to use simultaneously it is the first SaaS Service with both NOC and SOC and it has been used by many educational networks multinational corporation and telecommunications for operation. By 2015 N-Partner has expanded the business scale to China and gradually to Southeast Asia.

N-Partner contact information

Address: Rm. B1 14F. No.497 Zhongming S. Rd. West Dist. Taichung City 403 Taiwan R.O.C.
Website address: www.npartnertech.com
Telephone number: 886-4-2375-2865
E-mail address: sales@npartnertech.com
Support service: support@npartnertech.com

N-Partner