

Forum:[Hack Forums](#)

Thread: [Samaritans | Beginner Hacking Help Desk](#)

SysAdmin - November 5, 2018, 2:32 pm

Network Security Division Help Desk

Welcome to the official help desk of the Samaritans Network Security Division. Here, we will strive to help people that have questions and concerns regarding any and all threads that are covered by Network Security and Beginner Hacking.

Replies will primarily be from members of the Network Security Division, but others may pitch in and help aswell.

Ask away!

sh4moon - November 5, 2018, 3:02 pm

what's the best .NET windows rat?

lol just kidding. what do you think is a good way to help mitigate the APT threat? also, how do you think the west should respond to aggressive probing/attacks from Russia, China, and North Korea?

SysAdmin - November 5, 2018, 3:12 pm

(Nov 5, 2018 04:02 PM)sh4moon Wrote: [\[CITE\]](#) what's the best .NET windows rat?

lol just kidding. what do you think is a good way to help mitigate the APT threat? also, how do you think the west should respond to aggressive probing/attacks from Russia, China, and North Korea?

There really is no good way to help mitigate it unless you bring everything offline. You can't really protect everything this day and age, especially with people discovering zero-days and keeping it for their own benefits instead of reporting them.

Let's be honest, the US is doing the same to the countries you mentioned. Just look at the Stuxnet worm. Unless there are international laws in place, you can't really respond to these incidents much and try to point fingers. Those who know what they're doing will not leave any traces anyway.

sh4moon - November 5, 2018, 3:29 pm

(Nov 5, 2018 04:12 PM)SysAdmin Wrote: [\[CITE\]](#) There really is no good way to help mitigate it unless you bring everything offline. You can't really protect everything this day and age, especially with people discovering zero-days and keeping it for their own benefits instead of reporting them.

Let's be honest, the US is doing the same to the countries you mentioned. Just look at the Stuxnet worm. Unless there are international laws in place, you can't really respond to these incidents much and try to point fingers. Those who know what they're doing will not leave any traces anyway.

scenario: you've gotten access to a web server via an exploit and have a reverse shell. lets assume you have a Ubuntu running apache. you've got all the default system tools that come with a Linux install. how would you go about exploring the internal network and pivoting to other machines? keep in mind there's IDS and the network is well monitored.

phr3ak_ - November 6, 2018, 3:53 am

(Nov 5, 2018 04:29 PM)sh4moon Wrote: [\[CITE\]](#) scenario: you've gotten access to a web server via an exploit and have a reverse shell. lets assume you have a Ubuntu running apache. you've got all the default system tools that come with a Linux install. how would you go about exploring the internal network and pivoting to other machines? keep in mind there's IDS and the network is well monitored.

Hope I ain't hijacking the topic. But would like to discuss this question. I assume we have a meterpreter running in the ubuntu machine? If not then probably we can use arp-scan to reveal all the systems on the internal network. Once we get them we can use route command to route between the default gateway and victim computer.

We can now use that single compromised machine to attack all the systems on the network both within the engineering subnet and all the subnets that use the default gateway.

Finally, we can exploit each of those machines, but we will no longer have to be concerned about Intrusion Prevention Systems (IPS) and firewalls as we are now attacking from INSIDE the network!

This is just a speculation. But I guess it sort of answers your question.

@OP: Great thread. Expecting it to be helpful for many.

sh4moon - November 6, 2018, 1:05 pm

(Nov 6, 2018 04:53 AM)phr3ak_ Wrote: [\[CITE\]](#) Hope I ain't hijacking the topic. But would like to discuss this question. I assume we have a meterpreter running in the ubuntu machine? If not then probably we can use arp-scan to reveal all the systems on the internal network. Once we get them we can use route command to route between the default gateway and victim computer.

We can now use that single compromised machine to attack all the systems on the network both within the engineering subnet and all the subnets that use the default gateway.

Finally, we can exploit each of those machines, but we will no longer have to be concerned about Intrusion Prevention Systems (IPS) and firewalls as we are now attacking from INSIDE the network!

This is just a speculation. But I guess it sort of answers your question.

@OP: Great thread. Expecting it to be helpful for many.

I was thinking just a regular command shell. but you could get a meterpreter pretty easily even with just a shell. fyi I know what I would do, just curious what answers I would get.

phr3ak_ - November 6, 2018, 7:50 pm

(Nov 6, 2018 02:05 PM)sh4moon Wrote: [\[CITE\]](#) I was thinking just a regular command shell. but you could get a meterpreter pretty easily even with just a shell. fyi I know what I would do, just curious what answers I would get.

Yeah, I know mate. Though not much activity around here. So, thought of sharing my views.

sh4moon - November 6, 2018, 8:06 pm

(Nov 6, 2018 08:50 PM)phr3ak_ Wrote: [\[CITE\]](#) Yeah, I know mate. Though not much activity around here. So, thought of sharing my views.

nobody asks questions when you want them to lol. I might advertise this thread in my signature.

I do have a question though. if you're a pentester by some chance, how often do you come across honeypots or just general traps during pentests?

phr3ak_ - November 6, 2018, 11:13 pm

(Nov 6, 2018 09:06 PM)sh4moon Wrote: [\[CITE\]](#) nobody asks questions when you want them to lol. I might advertise this thread in my signature.

I do have a question though. if you're a pentester by some chance, how often do you come across honeypots or just general traps during pentests?

I don't have a lot of experience but I haven't yet encountered any such yet. But our team claims that almost 2-3 out of 5 networks have a good chance that they are tripped very well. So, we always try to be cautious. We have a set of protocols that we are asked to follow before diving in.

EDIT: Can someone share some good exploit development books or resources. Just looking forward to gain some insights to a problem.

?Criminal - November 6, 2018, 11:51 pm

(Nov 5, 2018 04:12 PM)SysAdmin Wrote: [\[CITE\]](#) There really is no good way to help mitigate it unless you bring everything offline. You can't really protect everything this day and age, especially with people discovering zero-days and keeping it for their own benefits instead of reporting them.

Let's be honest, the US is doing the same to the countries you mentioned. Just look at the Stuxnet worm. Unless there are international laws in place, you can't really respond to these incidents much and try to point fingers. Those who know what they're doing will not leave any traces anyway.

Best mitigation is air gapping the network, only the most dedicated of attackers will get around an air gap and exfiltrate their data back to a C&C somewhere, really ups the ante.

(Nov 6, 2018 04:53 AM)phr3ak_ Wrote: [\[CITE\]](#) Hope I ain't hijacking the topic. But would like to discuss this question. I assume we have a meterpreter running in the ubuntu machine? If not then probably we can use arp-scan to reveal all the systems on the internal network. Once we get them we can use route command to route between the default gateway and victim computer.

We can now use that single compromised machine to attack all the systems on the network both within the engineering subnet and all the subnets that use the default gateway.

Finally, we can exploit each of those machines, but we will no longer have to be concerned about Intrusion Prevention Systems (IPS) and firewalls as we are now attacking from INSIDE the network!

This is just a speculation. But I guess it sort of answers your question.

@OP: Great thread. Expecting it to be helpful for many.

I have a question for you that always made me curious, say I have a website we'll say it's the internet service provider comcast, say on the subdomain hacktheplanet.comcast.net theres an install of coldfusion that is vulnerable to a coldfusion RCE and I pop the box, however I realize that the interesting data is on accounts.comcast.net because that box has the customer tables in the DBMS NOT the box located at 88.73.21.45 the box at 88.73.21.46 which is pointed to accounts.comcast.net does have the interesting data though so if I use the shell on the hacktheplanet.comcast.net is it possible to pivot to the other server(the accounts.comcast.net one)through the shell since ill be on the internal network at that point or no.

SysAdmin - November 7, 2018, 2:57 am

(Nov 7, 2018 12:51 AM)?Criminal Wrote: [\[CITE\]](#) Best mitigation is air gapping the network, only the most dedicated of attackers will get around an air gap and exfiltrate their data back to a C&C somewhere, really ups the ante.

I have a question for you that always made me curious, say I have a website we'll say it's the internet service provider comcast, say on the subdomain hacktheplanet.comcast.net theres an install of coldfusion that is vulnerable to a coldfusion RCE and I pop the box, however I realize that the interesting data is on accounts.comcast.net because that box has the customer tables in the DBMS NOT the box located at 88.73.21.45 the box at 88.73.21.46 which is pointed to accounts.comcast.net does have the interesting data though so if I use the shell on the

hacktheplanet.comcast.net is it possible to pivot to the other server(the accounts.comcast.net one)through the shell since ill be on the internal network at that point or no.

I could have sworn that I've read that air-gapping networks have been exploited before. Again, if you wanted to be safe, you shouldn't even run an OS, let alone be connected to the internet. Thus, you are never safe.

sh4moon - November 7, 2018, 7:06 am

(Nov 7, 2018 12:51 AM)?Criminal Wrote: [\[CITE\]](#) Best mitigation is air gapping the network, only the most dedicated of attackers will get around an air gap and exfiltrate their data back to a C&C somewhere, really ups the ante.

I have a question for you that always made me curious, say I have a website we'll say it's the internet service provider comcast, say on the subdomain hacktheplanet.comcast.net theres an install of coldfusion that is vulnerable to a coldfusion RCE and I pop the box, however I realize that the interesting data is on accounts.comcast.net because that box has the customer tables in the DBMS NOT the box located at 88.73.21.45 the box at 88.73.21.46 which is pointed to accounts.comcast.net does have the interesting data though so if I use the shell on the hacktheplanet.comcast.net is it possible to pivot to the other server(the accounts.comcast.net one)through the shell since ill be on the internal network at that point or no.

whether or not you can pivot to it depends on the network. in this example they seem to be on the same network. it would be a simple compromise of the original server then pivot straight to your target. it's not always that easy though. you may have to go to a different subnet in this example because it's just a small /24 network. but if the subdomain's server is on the same network as the one you got into it's just a matter of pivoting.

as for airgapping, that's not an option for a lot of companies these days. internet connectivity is a major part of business.

phr3ak_ - November 8, 2018, 5:03 pm

(Nov 7, 2018 12:51 AM)?Criminal Wrote: [\[CITE\]](#) Best mitigation is air gapping the network, only the most dedicated of attackers will get around an air gap and exfiltrate their data back to a C&C somewhere, really ups the ante.

I have a question for you that always made me curious, say I have a website we'll say it's the internet service provider comcast, say on the subdomain hacktheplanet.comcast.net theres an install of coldfusion that is vulnerable to a coldfusion RCE and I pop the box, however I realize that the interesting data is on accounts.comcast.net because that box has the customer tables in the DBMS NOT the box located at 88.73.21.45 the box at 88.73.21.46 which is pointed to accounts.comcast.net does have the interesting data though so if I use the shell on the hacktheplanet.comcast.net is it possible to pivot to the other server(the accounts.comcast.net one)through the shell since ill be on the internal network at that point or no.

Didn't reply since I was working on a similar problem (Not entirely same but was somewhat similar). Since you mentioned hacktheplanet.comcat.com is already vulnerable and exploited. So, you can shell into it. And then you can try pivoting inside the network. The only problem which you might face is with permission elevation. Other than that you can easily attack other systems that are within the primary network.

sh4moon - November 8, 2018, 9:26 pm

(Nov 8, 2018 06:03 PM)phr3ak_ Wrote: [\[CITE\]](#) Didn't reply since I was working on a similar problem (Not entirely same but was somewhat similar). Since you mentioned hacktheplanet.comcat.com is already vulnerable and exploited. So, you can shell into it. And then you can try pivoting inside the network. The only problem which you might face is with permission elevation. Other than that you can easily attack other systems that are within the primary network.

granted, you don't necessarily have to escalate privileges depending on what's accessible from that shelled server. getting root never hurt anything though :)

shelled - November 11, 2018, 8:54 pm

With powershell being caught more and more commonly now even with obfuscation methods, what are your recommendations on making payloads that are less likely to be caught for red team engagements?

sh4moon - November 11, 2018, 9:07 pm

(Nov 11, 2018 09:54 PM)shelled Wrote: [\[CITE\]](#) With powershell being caught more and more commonly now even with obfuscation methods, what are your recommendations on making payloads that are less likely to be caught for red team engagements?

just because powershell is detected more than it was doesn't mean it isn't a factor. you could use veil evasion or make your own custom payloads/payload templates.

?Criminal - November 12, 2018, 11:55 am

(Nov 11, 2018 10:07 PM)sh4moon Wrote: [\[CITE\]](#) just because powershell is detected more than it was doesn't mean it isn't a factor. you could use veil evasion or make your own custom payloads/payload templates.

Powershells just another living off the land technique, it's been heavily replaced by abusing the binaries that come with java there was one you can pass code to and various other ones. The most advanced malware combines pre and post exploitation into one as iv'e seen malware that basically just launches shit like powershell or some other LOTL technique and either downloads and passes in commands from a txt file or it's built into the malware it self.

sh4moon - November 12, 2018, 2:14 pm

(Nov 12, 2018 12:55 PM)?Criminal Wrote: [\[CITE\]](#) Powershells just another living off the land technique, it's been heavily replaced by abusing the binaries that come with java there was one you can pass code to and various other ones. The most advanced malware combines pre and post exploitation into one as iv'e seen malware that basically just launches shit like powershell or some other LOTL technique and either downloads and passes in commands from a txt file or it's built into the malware it self.

I agree. my opinion is that you should use what's already on system when possible. there was a backdoor technique that used a combo of a .bat, powershell, and something else. I'll have to see if I can find it.

SysAdmin - November 18, 2018, 5:41 am

Bumping this up a bit, we're still taking in questions!

Legion - November 18, 2018, 7:08 am

Where's the best place for me to freshen up on website exploitation? Preferably a reading source?

SysAdmin - November 18, 2018, 7:13 am

(Nov 18, 2018 08:08 AM)NET. Wrote: [\[CITE\]](#) Where's the best place for me to freshen up on website exploitation? Preferably a reading source?

<http://www.valencynetworks.com/articles/cyber-security-attacks-web-exploitation.html>

There's also places like Cybrary and Udemy (warez disallowed) that have courses on Web Exploitation.

Legion - November 18, 2018, 7:23 am

(Nov 18, 2018 08:13 AM)SysAdmin Wrote: [\[CITE\]](#)

<http://www.valencynetworks.com/articles/cyber-security-attacks-web-exploitation.html>

There's also places like Cybrary and Udemy (warez disallowed) (warez disallowed) that have courses on Web Exploitation.

Thanks man I'll take a look. I didn't know cybrary specifically did web exploitation. I've done the security+ course they offer.

SysAdmin - November 18, 2018, 7:24 am

(Nov 18, 2018 08:23 AM)NET. Wrote: [\[CITE\]](#) Thanks man I'll take a look. I didn't know cybrary specifically did web exploitation. I've done the security+ course they offer.

Getting the All-In-One Security+ Book from Amazon would also help, I have the Network+ one and it goes very in-depth.

I imagine Security+ would be the same as it is from the same publisher and writer.

passwords - November 19, 2018, 8:22 am

Packet Manipulation

I recently developed my own proxy server.

So far I've only tested in on Terraria, where I can receive and send the packets from the client.

My question is.. What are the limits for packet manipulation?

What games can you do it with, without having to crack some serious encryption?

Also, what more is there to do besides game packet manipulation?

sh4moon - November 19, 2018, 8:52 am

(Nov 19, 2018 09:22 AM)NETGuard Wrote: [\[CITE\]](#) Packet Manipulation

I recently developed my own proxy server.

So far I've only tested in on Terraria, where I can receive and send the packets from the client.

My question is.. What are the limits for packet manipulation?

What games can you do it with, without having to crack some serious encryption?

Also, what more is there to do besides game packet manipulation?

you could use it to bypass firewall restrictions. this is a bit of a side note because it's not really packet manipulation. you could put it on a hacked system and use the system as a proxy.

?Criminal - November 19, 2018, 7:17 pm

(Nov 19, 2018 09:22 AM)NETGuard Wrote: [\[CITE\]](#) Packet Manipulation

I recently developed my own proxy server.

So far I've only tested in on Terraria, where I can receive and send the packets from the client.

My question is.. What are the limits for packet manipulation?

What games can you do it with, without having to crack some serious encryption?

Also, what more is there to do besides game packet manipulation?

every single game is vulnerable to it, even encrypted ones you just have to know how to hook packet sends before the encryption occurs, thats usually how people do it, all games by design suffer from packet manipulation, other then packet manipulation you can't really do much in an online game, theres client side code injection which sometimes can also lead into packet manipulation but usually it's just for stuff like ESP and etc some of the more major server side exploits usually stem from packet manipulation.

HFuserLv19001 - November 19, 2018, 10:09 pm

I figure this is a decent place to ask. Lets say theoretically someone wanted to evaluate the security of some websites/systems. How can they best maintain their anonymity? I read the guide

suggestion and it provides some good information, but I didn't see anything about VPS', or utilizing proxychains or the tor service. When going active, whats the best way forward?

sh4moon - November 20, 2018, 8:21 am

(Nov 19, 2018 11:09 PM)HFuserLvI9001 Wrote: [\[CITE\]](#) I figure this is a decent place to ask. Lets say theoretically someone wanted to evaluate the security of some websites/systems. How can they best maintain their anonymity? I read the guide suggestion and it provides some good information, but I didn't see anything about VPS', or utilizing proxychains or the tor service. When going active, whats the best way forward?

if by moving forward you mean actually breaking into stuff...

I'd use a Kali usb for your os, and never actually install it on your computer's hard drive. use a Wi-Fi network other than yours. use a vpn which is really important if you use public Wi-Fi. buy yourself a nice bulletproof server and install hacking tools on that (we'll call it device B). then compromise a server or some system and use that as a proxy (device C).

so how it'll work is you head to your coffee shop and connect to the Wi-Fi. you use your vpn and tor (with the proxychains tool) to connect to server B with all your tools on it (probably using ssh to control the server). from server B you conduct your hacking through device C as your proxy.

if you want to be less black/grey hat then cut out device C. if you want more anonymity then just add a lot more device C's. or if you don't want to bother with device B then just use tor and vpn.

Armada - November 20, 2018, 10:57 am

(Nov 19, 2018 09:22 AM)NETGuard Wrote: [\[CITE\]](#) Packet Manipulation

I recently developed my own proxy server.

So far I've only tested in on Terraria, where I can receive and send the packets from the client.

My question is.. What are the limits for packet manipulation?

What games can you do it with, without having to crack some serious encryption?

Also, what more is there to do besides game packet manipulation?

Packet manipulation is extremely effive in phishing, network breaches, application manipulation (games, etc) and much more.

Consider the following. Packets are the networks form of communication right?

When you manipulate packets, you are basically playing the game Broken telephone.

The idea is the end packet will not be the same as the originally sent packet, allowing the MITM attack to basically manipulate the communication stream to tell the systems to do whatever the hell the attacker wants it to do. (Within limitations of course)

HFuserLvI9001 - November 20, 2018, 3:44 pm

(Nov 20, 2018 09:21 AM)sh4moon Wrote: [\[CITE\]](#) if by moving forward you mean actually breaking into stuff...

I'd use a Kali usb for your os, and never actually install it on your computer's hard drive. use a Wi-Fi network other than yours. use a vpn which is really important if you use public Wi-Fi. buy yourself a nice bulletproof server and install hacking tools on that (we'll call it device B). then compromise a server or some system and use that as a proxy (device C).

so how it'll work is you head to your coffee shop and connect to the Wi-Fi. you use your vpn and tor (with the proxychains tool) to connect to server B with all your tools on it (probably using ssh to control the server). from server B you conduct your hacking through device C as your proxy.

if you want to be less black/grey hat then cut out device C. if you want more anonymity then just add a lot more device C's. or if you don't want to bother with device B then just use tor and vpn.

I would never break into anything without authorization, but thanks for the info. It's always good to learn something new.

sh4moon - November 20, 2018, 3:53 pm

(Nov 20, 2018 04:44 PM)HFuserLvl9001 Wrote: [\[CITE\]](#) I would never break into anything without authorization, but thanks for the info. It's always good to learn something new.
oh good. good luck with that then.

cliterous - November 20, 2018, 6:53 pm

Glad I found this, I want to learn to hack into snapchat accounts of people who are nobodies (aka not celebrity types), brute force four digit passwords w/ attempt limit, and how to potentially bypass 2auth and hack a discord account but I have no clue where to start.
for educational purposes, of course